UNIVERSIDADE FEDERAL DE ALAGOAS – UFAL

Faculdade de Direito de Alagoas – FDA

NATHALIA MARIA CARDOSO ACIOLE

O DIREITO À PRIVACIDADE E A LEI GERAL DE PROTEÇÃO DE DADOS NO ORDENAMENTO JURÍDICO BRASILEIRO

Maceió/AL

Janeiro/2020

UNIVERSIDADE FEDERAL DE ALAGOAS – UFAL

Faculdade de Direito de Alagoas – FDA

NATHALIA MARIA CARDOSO ACIOLE

O DIREITO À PRIVACIDADE E A LEI GERAL DE PROTEÇÃO DE DADOS NO ORDENAMENTO JURÍDICO BRASILEIRO

Monografia de conclusão de curso, apresentado à Faculdade de Direito de Alagoas (FDA/UFAL) como requisito parcial para obtenção de grau de Bacharel em Direito.

Orientadora: Prof. Dra. Juliana de Oliveira Jota Dantas

_____

Assinatura da Orientadora

Maceió/AL

Janeiro/2020

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico
Bibliotecário: Marcelino de Carvalho Freitas Neto – CRB-4 – 1767

A181d Aciole, Nathalia Maria Cardoso.
O direto à privacidade e a Lei Geral de Proteção de Dados no ordenamento jurídico brasileiro / Nathalia Maria Cardoso Aciole. – 2020.
59f.

Orientadora: Juliana de Oliveira Jota Dantas.
Monografia (Trabalho de Conclusão de Curso em Direito) – Universidade Federal de Alagoas. Faculdade de Direito de Alagoas. Maceió, 2020.

Bibliografia: f. 55-59.

1. Brasil. Lei geral de proteção de dados pessoais (2018). 2. União Europeia. Regulamento Geral sobre a Proteção de Dados (2016). 3. Direito à privacidade. 4. Dados pessoais. 5. Proteção de dados. 6. Internet. 7. Vigilância. 8. Modernidade líquida. I. Título.

CDU: 343.45:004.738.5(81)

UNIVERSIDADE FEDERAL DE ALAGOAS - UFAL
FACULDADE DE DIREITO DE ALAGOAS – FDA

FORMULÁRIO DE AVALIAÇÃO DO TCC

Orientador: PROFª Drª JULIANA DE OLIVEIRA JOTA DANTAS

Discente: NATHALIA MARIA CARDOSO ACIOLE

Nº de matrícula: 15112418

Título do trabalho:
O DIREITO À PRIVACIDADE E A LEI GERAL DE PROTEÇÃO DE DADOS NO ORDENAMENTO JURÍDICO BRASILEIRO

	ESPECIFICAÇÃO	FAIXA DE PONTUAÇÃO	NOTAS 1AV	NOTAS 2AV	MÉDIA
A	**RELEVÂNCIA DO TEMA** (análise da importância do tema tratado, sua atualidade e possível impacto perante a comunidade acadêmica – articulação correta entre a teoria e a realidade estudada).	0,0 a 2,0	2,0	2,0	2,0
B	**QUALIDADE DA ABORDAGEM** (Fundamentação teórica consistente, bem definida e corretamente desenvolvida; fundamentação legal; equilíbrio e inter-relação entre as partes. Nível de aprofundamento e argumentação. Alcance dos objetivos propostos).	0,0 a 4,0	3,5	3,5	3,5
C	**QUALIDADE DO TEXTO** (análise da redação empregada pelo autor, em termos de clareza, coerência e coesão).	0,0 a 2,0	2,0	2,0	2,0
D	**QUALIDADE DA PESQUISA** (análise do método empregado, seguindo os padrões e as normas técnicas para trabalhos científicos, conforme ABNT mais recente e, especialmente, verificação das fontes/referências: se foram pertinentes, satisfatórias e/ou suficientes).	0,0 a 2,0	1,5	1,5	1,5
NOTA FINAL					9,0 (NOVE)

Observação e/ou Recomendação:

Maceió-AL, 14 de fevereiro de 2020

BANCA EXAMINADORA:

1º Avaliador (1AV) _____ **Matrícula** 1121340

2º Avaliador (2AV) _____ **Matrícula** 1991433

(Assinatura legível com carimbo, se professor)

RESUMO

O presente trabalho apresenta como tema central a análise das questões relativa ao direitoda privacidade, além de reflexões sobre seus desdobramentos na modernidade líquida e na sociedade da informação. A novel e crescente preocupação em tutelar esses direitos é resultante da informatização dos meios de comunicação, e consequentemente das relações sociais, em que o usuário passa a ser sujeito de direito de uma relação virtual e efêmera. Essa pesquisa é dedicada ao estudo crítico dos eventos resultantes da sociedade pós-moderna, como o surgimento do instituto da sociedade da vigilância e da superexposição nas redes sociais, além dos avanços tecnológicos que justificam a existência desses institutos. No ínterim, buscou-se realizar o exame dos marcos regulatórios para solução de conflitos originários de relações jurídicas virtuais, com o foco na Lei Geral de Proteção de Dados e do *General Data Protection Regulation*, com a análise dos principais artigos, nas simetrias entre os textos legais e dos efeitos produzidos em sociedade.

Palavras-chave: direito à privacidade; Lei Geral de Proteção de Dados; dados pessoais; *General Data Protection Regulation*; proteção de dados pessoais; Internet; vigilância; superexposição; modernidade líquida.

ABSTRACT

This present term paper aims the analysis about issues related with the right of privacy, and furthermore reflections about its development inside liquid modernity and information society. The new and the growing concern in protect these rights arises from the informatization of comunication means, and as consequence of social relationships, the user becomes the main person under the Law inside of a virtual and ephemeral relationship. This survey is dedicated to the critical study of the resulting events from postmodern society, as the rising of Surveillance Society e over exposition in social mídia, and besides the technological advances that justifies the existence of these institutes. In the meantime, it was sought the study of normative regulations to solve the consequent issues related with digital and legal relations, with a main focus in the analysis of the articles, symmetry between the acts and the efects amog the societyof the *Lei Geral de Proteção de Dados* and General Data Protection Regulation.

Key-words: *the right of privacy;* Lei Geral de Proteção de dados*; personal data; General Data Protection Regulation; protection of personal data; Internet; Surveillance; over exposition; liquid modernity.*

SUMÁRIO

1. INTRODUÇÃO

O ser humano, desde sua origem, desenvolve atividades e habilidades que permitam sua integração no corpo social; hodiernamente essa integração se dá no âmbito digital, em razão dos inúmeros avanços alcançados nessa seara que surgiram com o intuito de facilitar a comunicação interpessoal com as famosas Tecnologias da Informação, além de permitir o aperfeiçoamento dos meios de consumo, do desenvolvimento tecnológico, entre outros.

Entretanto, com a virtualização dos meios, principalmente da comunicação, novos tipos de relações jurídicas são originados. Nesse contexto, as relações humanas passam a ser dotadas de aspectos da liquidez decorrentes da pós-modernidade, o que implica em uma dissipação dos indivíduos membros desse corpo social assemelhando-se ao estado físico da matéria, diluindo o contexto primitivo de sociedade que pressupõe uma união tangível em um determinado território.

Diante do exposto, os indivíduos buscam formas alternativas de voltarem a integrar a coletividade, um exemplo disso é o crescimento exponencial de redes sociais que permitem a comunicação imediata entre os usuários, além de possibilitar amizades, relacionamentos amorosos, relações de emprego, conectados apenas por uma rede sem fios e ilimitada.

Contudo, tudo isso culmina em infinitas situações que o legislador não está preparado para lidar, como a superexposição do ser nas redes sociais que surge como exercício das liberdades a eles conferidas, além de questões referentes ao direito ao esquecimento, ou fenômenos ainda mais complexos como a criação de mecanismos de vigilância ou de manipulação de dados como forma de criar ambientes hostis de polarização e discurso de ódio.

Esse tipo de tecnologia é desenvolvido tanto por entidades governamentais, como a China que realiza o monitoramento ininterrupto de seus cidadãos, ou por entidades privadas como ocorreu com o escândalo que culminou no vazamento de dados de 87 (oitenta e sete) milhões de usuários do *Facebook,* valendo-se da coleta de dados psicológicos dos usuários a fim de manipular resultados das eleições norte-americanas.

Os titulares constantemente inserem dados pessoais em diversos sítios da internet, como nas compras *online*, ou na inscrição em mídias sociais, todavia, constata-se uma vulnerabilidade na tecnologia desenvolvida para proteger esses dados, permitindo ataques diretos feitos por *hackers*, que realizam a coleta desses dados que poderão ser utilizados para

fins alheios aos de sua criação, sendo, dessa maneira, um tema contemporâneo à sociedade da informação.

Por se tratar de uma temática ainda pouco explorada, porém de grande relevância no contexto atual, a pesquisa em comento se propõe a considerar os principais aspectos do *General Data Protection Regulation,* analisando os marcos normativos que o antecederam, bem como suas principais disposições, o contexto em que está inserida, entre outros.

Além disso, o estudo objetiva elucidar questionamentos decorrentes da Lei nº 13.709, a Lei Geral de Proteção de Dados, que entrará em vigor no ano corrente, em especial, com o recorte no direito à privacidade e na proteção dos dados pessoais.

A análise inicialmente será pautada no estudo dos impactos resultantes do Marco Civil da Internet, como marco regulatório inicial na proteção de dados pessoais, com o apoio da legislação, doutrina e jurisprudência. Ato contínuo, a pesquisa explorará questões referentes a nova legislação de proteção de dados, como seu processo legislativo e principais artigos.

2. DO DIREITO À PRIVACIDADE E SUA INFLUÊNCIA NA SOCIEDADE PÓS-MODERNA

2.1. BREVE HISTÓRICO DO DIREITO À PRIVACIDADE

A privacidade é um direito subjetivo fundamental de primeira geração, estando localizado no âmbito dos direitos individuais. Esse direito pode ser entendido como o direito a ter o controle do acesso a informações de caráter exclusivo e pessoal, possuindo como peculiaridades o direito de estar só (*the right to be alone*), o segredo e sigilo, bem como a autonomia da vontade (MIRANDA, 2018).

Discussões acerca de seu surgimento remontam a Antiguidade, como nas culturas grega, chinesa e hebraica, em que a vida em grande parte acontecia publicamente, fazendo-se necessária a proteção da intimidade (MIRANDA, 2018). Também é possível constatar seus desdobramentos na Idade Média com a premissa do "*a man's house is his castle*", em que há separação do público e privado, definido a casa como um castelo, possuindo barreiras intransponíveis separando o espaço de intimidade da vida pública do homem.

Em 1890 foi publicado na *Havard Law Review* o artigo intitulado "*The right of privacy*", escrito por Samuel D. Warren e Louis D. Brandeis, podendo ser considerado o primeiro documento que tratou diretamente do *right to privacy* no *Common Law*. O documento foi escrito como forma de represália a notícias sensacionalistas publicadas pela imprensa sobre o casamento da filha do autor Samuel Warren. O texto invoca o *right to enjoy your life* e o *right to let be alone,* relacionados com a ideia intangível da propriedade como forma de posse, assim como a premissa de que o indivíduo tem o poder de autodeterminação sem sofrer ingerência realizadas por terceiros sendo essas indevidas e/ou não autorizadas por lei (WARREN; BRANDEIS, 1890).

Porém, com o fim da Segunda Guerra Mundial, a Declaração Internacional dos Direitos Humanos fomentou a proteção dos direitos à personalidade, e o direito à privacidade restou consagrado em seu art. 12, *in verbis*:

> Ninguém será sujeito à **interferência em sua vida privada**, **em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação**. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. **(grifou-se)**

Diante da leitura do referido artigo, verifica-se que esse direito se estende além da vida privada do indivíduo, atingindo aspectos como a inviolabilidade do domicílio,

correspondência, assim como ataques a sua reputação e honra. Assim corrobora a Constituição Federal brasileira de 1988, no capítulo Dos Direitos e Garantias Fundamentais, localizados no art. 5º, incisos X, XI e XII.

> X - são invioláveis a **intimidade, a vida privada, a honra e a imagem das pessoas**, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> XI - a **casa é asilo inviolável do indivíduo**, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
>
> XII - é inviolável o **sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas,** salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; **(grifou-se)**

O inciso X traz a inviolabilidade tanto da intimidade quanto da vida privada, como forma de diferenciar esses dois institutos. Segundo Paulo Lôbo (2019) a intimidade tem relação com "fatos, situações que a pessoa deseja ver sob seu domínio exclusivo, sem compartilhar com qualquer outra", afirma ainda que esse conceito é variável, dependendo da época, cultura e localidade. No que concerne à vida privada, o supracitado autor aduz que "diz respeito ao ambiente familiar, cuja lesão resvala em outros membros do grupo", como gosto pessoal, locais que frequenta, sexualidade, aspectos que não devem sofrer intromissão de terceiros.

É usual a confusão que resulta na utilização desses conceitos como sinônimos, entretanto, eles podem ser considerados complementares. Todavia, é possível constatar que o tratamento doutrinário e jurisprudencial no direito brasileiro não faz essa diferenciação, justamente por existir uma linha tênue que separa esses dois âmbitos, o que pode implicar em um tratamento superficial que não prioriza as particularidades desses direitos.

Outro ponto importante a ser destacado é a necessidade de adequação do texto constitucional à realidade social vigente. A Constituição Federal do Brasil foi promulgada em 1988, logo após o fim de uma longa ditadura militar, possuindo o enfoque de garantir à população direitos fundamentais, políticos, sociais.

O projeto de implantação da Sociedade da Informação no Brasil aconteceu em 1996 pelo Conselho Nacional de Ciência e Tecnologia, com a finalidade de em âmbito nacional promover a integração e coordenação do "desenvolvimento e a utilização de serviços avançados de computação, comunicação e informação e de suas aplicações na sociedade", o que permitiria aperfeiçoar a pesquisa e a educação, estabelecendo uma alfabetização digital

dos usuários, além de interferir em aspectos econômicos, dando ao Brasil a chance de competir no mercado mundial[1].

Com a justificativa de que o avanço tecnológico acontecia rapidamente e que o Brasil para integrar a sociedade em rede deveria se adequar a esses avanços, tendo como consequência o crescimento exponencial da economia, padrão de consumo e comportamento da sociedade, além de alavancar o processo de minimização da desigualdade econômica. Esse processo de informatização da sociedade brasileira viabilizou a necessidade de adequação da legislação existente, principalmente a Constitucional, no que se refere à virtualização das relações jurídicas hodiernas.

Em razão disso, podem ser estabelecidas diferentes formas de interpretação da norma constitucional, para que a mesma consiga se adequar a realidade hodierna. Tem-se como exemplo a corrente doutrinária norte-americana do Originalismo (*Originalism*), este prevê uma nova interpretação da norma constitucional diante das vicissitudes da sociedade moderna, todavia essa interpretação da norma deverá seguir seu significado semântico original *(original meaning),* considerando a intenção do Constituinte no momento de sua criação. Segundo Jack M. Balkin (2011) "*Fidelity to original meaning as original semantic content does not require that we must apply the equal protection clause the same way that people at the time of enactment would be applied*", ou seja, em síntese o conteúdo semântico da norma será preservado, entretanto sua aplicação será realizada após a análise do caso concreto. [2]

Em contraponto à teoria do Originalismo, a premissa do *Living Constitution* ou Constituição viva, pressupõe que a Constituição é um documento vivo que acompanha a sociedade e as questões de direito contemporâneas, não sendo necessárias emendas formais à Constituição para a adequação da norma no caso concreto. Esse tipo de interpretação pode abrir margens para um maior ativismo judicial, que pode ser entendido como um método de

---

[1]Disponível em: http://livroaberto.ibict.br/bitstream/1/434/1/Livro%20Verde.pdf

[2]Tradução nossa: "Fidelidade ao significado original como conteúdo semântico original não significa que devemos aplicar a mesma cláusula de proteção da mesma forma que seria aplicada no momento da promulgação."

interpretação amplo das leis em geral, como explica David A. Strauss (2011), sendo essa a maior crítica imposta a esse tipo de interpretação.

Conduzindo a noção do *Living Constitution* para conjuntura brasileira da pós-modernidade, composta por uma sociedade informatizada e fluída, vislumbra-se a importância de uma interpretação extensiva da norma constitucional, de forma que a própria Constituição Federal seja considerada um documento vivo, amoldando-se às constantes modificações sociais.

A doutrina alemã estabelece que o direito à privacidade é dividido em três esferas, teoria criada por Heinrich Hubmann (*apud* MIRANDA, 2018) com a finalidade de separar o "núcleo essencial insuscetível de limitação e o que poderia ser objeto de autolimitação" (LÔBO, 2019).

Essa teoria pode ser denominada como "teoria dos círculos concêntricos", sendo levado em consideração que as camadas desse círculo abrangem a esfera mais íntima à esfera mais "pública" do sujeito, ou seja, parte de uma camada que diz respeito apenas ao titular das informações até a esfera de conhecimento geral, na qual o sujeito não possui o direito de limitação.

A esfera íntima/interna (*Geheimsphäre*) possui estreita ligação com o princípio da dignidade, isso ocorre diante da impossibilidade de ingerências do Estado no âmbito privado do indivíduo (LÔBO, 2019). Nessa esfera estão localizadas as questões do âmago pessoal, fazendo parte do segredo e sigilo individual, como a orientação sexual, religião, entre outros (MIRANDA, 2018).

No que concerne a esfera intermediária, a privada (*Vertrauensphäre*), o sujeito pode exercer livremente aspectos de sua personalidade, entretanto podem sofrer formas de controle por meio do Estado na prevalência dos direitos coletivos face os individuais (LÔBO, 2019). Nesse âmbito as informações são compartilhadas com pessoas determinadas, como familiares, amigos.

Por fim, tem-se a esfera pública/social, essa não possui relação com os progressos dos direitos da personalidade individuais (LÔBO, 2019), justamente porque a pessoa decide expor acontecimentos, fatos de sua vida, ou seja, as informações estão em domínio público e são utilizadas como forma de integração no corpo social.

Em contrapartida a concepção da estrutura tridimensional da privacidade é dividida em: dimensão decisional da privacidade, dimensão espacial da privacidade e dimensão informacional da privacidade.

Na dimensão decisional a privacidade é tratada como forma de proteção ao indivíduo, no que se refere ao seu modo de vida e suas escolhas pessoais. Essa dimensão está ligada diretamente ao direito norte-americano, fundamentando-se na ideia de liberdades reprodutivas (EHRHARDT; PEIXOTO, 2019).

No que concerne a dimensão espacial da privacidade, têm-se como escopo a premissa da privacidade como espaço físico em que não é possível a intervenção de terceiros, como o lar, por exemplo. Esse direito está presente na Constituição Federal no art. 5º, XI, o qual determina que "a residência é asilo inviolável do indivíduo", de forma a indicar o direito à privacidade no âmbito físico do indivíduo (EHRHARDT; PEIXOTO, 2019). Por fim, a dimensão informacional da privacidade diz respeito ao tratamento dos dados pessoais e suas consequentes implicações, levando-se em consideração a velocidade da informação e o uso de mecanismos disseminadores.

Nessa senda, verifica-se que as teorias em comento buscam estabelecer que a privacidade não possua uma única incidência ou delimitação. A privacidade é um direito que se adequa a situação do seu titular, abrangendo a proteção desde a esfera mais íntima até a mais externa, além de estar em constante aperfeiçoamento garantindo a tutela jurídica de seus titulares.

2.2. PRIVACIDADE: RAMIFICAÇÕES E IMPLICAÇÕES NA SOCIEDADE DA INFORMAÇÃO

O advento da Internet permite a disseminação de informações de forma veloz e ampla, fato esse que interfere diretamente na privacidade, culminando na ressignificação desse direito, que passa a ter nuances contemporâneas diante das vicissitudes das relações sociais. Urge ao Direito o dever de criar institutos que possam salvaguardar os interesses dos sujeitos da relação, estes em constante evolução. Um exemplo disso é o direito ao esquecimento, que

pode ser explicado como o direito que o indivíduo possui de não ter expostos fatos de sua vida íntima/privada para toda a coletividade *ad aeternum.*

A noção do *droit à l'oubli* (HEYLLIARD, 2012) surgiu em um apontamento feito por Gerard-Lyon Caen referente ao *Affaire Landru*[3] em 1965, em que o professor invocou o argumento do direito ao esquecimento como fundamento jurídico no caso de uma das ex-amantes do *serial killer Landru*, que ingressou com uma ação de indenização por danos causados diante da exibição de filme que retratava fatos de sua vida pregressa, a ação foi intentada com o fito de fazer que com que aqueles fatos expostos no filme fossem esquecidos (SARMENTO, 2015). Contudo, a ação interposta foi considerada improcedente, o juiz argumentou se valendo da *"prescription du silence"*, tendo em vista que a autora havia publicado suas memórias sobre o caso, e essas, dessa maneira, possuíam caráter público e judiciário.

O reconhecimento jurisprudencial desse direito aconteceu em 1983 no caso *Madame M. v. Filipachi et Congedipress*[4], proferida pelo *Tribunal de Grand Instance de Paris,* em razão de um texto jornalístico publicado tratando de um crime que praticado 15 anos antes (SARMENTO, 2015), sendo aplicada, nesse caso, uma nova liberdade pública como forma de responsabilização civil (HEYLLIARD, 2012).

O direito ao esquecimento ingressa ao ordenamento jurídico brasileiro paulatinamente. Na VI Jornada de Direito Civil foi editado o Enunciado nº 531, que dispõe que "a tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento"[5], com a justificativa que

> Os danos provocados pelas novas tecnologias de informação vêm-se acumulando nos dias atuais. O direito ao esquecimento tem sua origem histórica no campo das condenações criminais. Surge como parcela importante do direito do ex-detento à ressocialização. **Não atribui a ninguém o direito de apagar fatos ou reescrever a própria história, mas apenas assegura a possibilidade de discutir o uso que é dado aos fatos pretéritos, mais especificamente o modo e a finalidade com que são lembrados. (grifou-se)**

[3]TGI Seine, 14/10/1965
[4] TGI Paris, 20/04/1983
[5] Disponível em: https://www.cjf.jus.br/enunciados/enunciado/142. Acesso em: 03/09/2019

O Superior Tribunal de Justiça utilizou-se do direito ao esquecimento como fundamento em dois casos notórios, o da Chacina da Candelária (RESP. nº 1.334.097) e o caso Aída Curi (RESP. nº 1.335.153). Dois recursos foram ajuizados contra a Rede de Televisão Globo, um recurso interposto por um dos acusados, e posteriormente absolvido, da Chacina da Candelária, tendo em vista a veiculação do caso em rede nacional no programa Linha Direta, com a exposição da imagem e nome do autor, causando danos a ele e seus familiares, o que resultou na condenação Rede Globo ao pagamento de indenização. Em seu voto[6], o Ministro Relator Luis Felipe Salomão ressalta a controvérsia entre a liberdade de informação face aos direitos da personalidade, quer estes sejam a privacidade e intimidade, afirma ainda que

> A assertiva de que uma notícia lícita não se transforma em ilícita com o simples passar do tempo não tem nenhuma base jurídica. O ordenamento é repleto de previsões em que a significação conferida pelo Direito à passagem do tempo é exatamente o esquecimento e a estabilização do passado, mostrando-se ilícito sim reagitar o que a lei pretende sepultar.

O outro recurso fora ajuizado pelos irmãos de Aida Curi, com o mesmo fundamento da apresentação do caso no programa televisivo Linha Direta, com a alegação de que a lembrança que ocasionou mais uma vez sofrimento aos familiares. O Ministro Relator aduziu que o caso está em domínio público, e que seria impossível a retratação do caso "Aída Curi sem Aída Curi" [7].

Extrai-se da análise dos casos que o direito ao esquecimento entra em confronto com outros direitos fundamentais constitucionalmente garantidos, como o direito à informação, por exemplo. Esse direito está consagrado na Constituição no art. 5º, inciso XIV e no artigo 220, § 1º, *in verbis*:

> Art. 5º, inciso XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;
>
> Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.

---

[6] Disponível em: https://www.conjur.com.br/dl/direito-esquecimento-acordao-stj.pdf. Acesso em 03/09/2019.
[7] Disponível em: https://www.conjur.com.br/dl/direito-esquecimento-acordao-stj-aida.pdf. Acesso em: 09/09/2019.

> § 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.

Esse direito está aliado à preservação da história, desdobrando-se em três dimensões: o direito de informar, referente às liberdadesde expressão e de imprensa; o direito de se informar, o acessoà informaçãoe o direito de ser informado, referente a questões de interesse público (EHRHARDT; NUNES; PORTO, 2016 *apud* CANOTILHO, 2007).

Parte-se da premissa que o povo tem o direito de saber de sua história, e que essa história é complementar ao direito de informação, tendo em vista que sem esse direito não seria possível a disseminação de fatos importantes ao interesse público, e em especial nas de ações penais públicas em que o interesse geral é intensificado, como na Chacina da Candelária e no assassinato de Aída Curi. Nas palavras do Min. Relator Luis Felipe Salomão[8]

> a recordação de crimes passados pode significar uma análise de como a sociedade - e o próprio ser humano - evolui ou regride, especialmente no que concerne ao respeito por valores éticos e humanitários, assim também qual foi a resposta dos aparelhos judiciais ao fato, revelando, de certo modo, para onde está caminhando a humanidade e a criminologia.

Portanto, é necessária a ponderação no caso concreto para definir qual direito irá sobrepor o outro, partindo análise principiológica, jurisprudencial e da doutrina, como forma de garantir ora o direito à privacidade em detrimento do interesse público, ora o interesse público face o direito individual.

Entretanto, diante da conjectura da pós-modernidade o direito ao esquecimento passa por uma atualização fundamental, tendo em vista que a informação trafega rapidamente na Internet e nela permanece por um lapso temporal indeterminado. A partir disso, surgem direitos decorrentes ao esquecimento passíveis de tutela jurídica.

É costume na doutrina nacional e estrangeira acreditar que o direito ao esquecimento possui uma forma e conteúdo únicos (ACIOLI; EHRHARDT, 2019). De acordo com os estudos taxonômicos de Gregory Voss e Céline Castets-Renard (2016), analisando as normas de convergência desse direito. Apontam que existem cinco tipos de direito ao esquecimento:

---

[8]Ibidem.

> a) *Right to rehabilitation* (direito à reabilitação): *the right to oblivion of the judicial past* (direito ao esquecimento do passado judicial);
>
> b) *Right to deletion/erasure* (direito ao apagamento): *the right to oblivion established by data protection legislation* (direito ao esquecimento estabelecido em legislação de dados)
>
> c) *Right to delisting/delinking/de-indexing* (direito à desindexação);
>
> d) *Right to obscurity* (direito à obscuridade);
>
> e) *Right to digital oblivion of data collected by information society services*(direito ao esquecimento digital de dados coletados por serviços secretos).

O direito à reabilitação garante ao indivíduo o direito à reintegração social após condenação judicial (CASTETS-RENARD; VOSS, 2016). Muito utilizado no âmbito penal ao "apagar" as informações concernentes ao cadastro penal do indivíduo após o cometimento de infrações penais. Os autores explicam que existem condições para a concessão desse direito, como o bom comportamento, por exemplo.

O direito ao apagamento está pautado na possibilidade do sujeito em recuperar o exercício de suas informações que estão sendo controladas pelo Poder Público ou por outras entidades, podendo ser considerado um direito à autodeterminação informativa, existindo, dessa forma, disposições legais que garantem esse direito, como a *General Data Protection Regulation* na União Europeia (ACIOLI; EHRHARDT, 2019).

No quadro atual de proteção do usuário no ciberespaço o direito a desindexação surge como forma de garantir que as informações dos sujeitos não se perpetuem na esfera da Internet. Esse direito tem como marco teórico o *caseGoogle Spain v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*[9]. A ação foi interposta por Mario Costeja González em face do *Google Spain*, com o fundamento de que sempre que um usuário do site digitasse o nome do autor no buscador os resultados direcionados seriam as páginas do jornal da *La Vanguardia* datadas de 19 de janeiro e 9 de março de 1998, constando um anúncio de uma venda de imóveis em hasta pública, em que figurava o nome de Mario Costeja González como devedor da Segurança Social, tendo em vista que estava sendo executado em razão desse fato.

---

[9] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN. Acesso em 09/09/2019.

O pedido principal da ação era que o Jornal *La Vanguardia* retirasse ou alterasse as páginas em que o nome do autor figurava, com o escopo de suprimir essas informações ou que criassem um mecanismo de proteção para que no momento da busca os dados pessoais do autor fossem protegidos. Já o que concerne ao *Google Spain* foi pedida a supressão ou a ocultação dos dados pessoais do autor, para que no momento da busca no site os *hiperlinks* não direcionassem o nome do autor às publicações do *La Vanguardia*.

O Acórdão proferido pelo Tribunal de Justiça Europeu se valeu da análise de artigos constantes na Diretiva 95/46/CE, além da natureza de tratamento de dados que o buscador do site *Google* realiza, com o argumento[10] de que

> não se discute que entre os dados encontrados, indexados e armazenados pelos motores de busca e postos à disposição dos seus utilizadores figuram também informações sobre pessoas singulares identificadas ou identificáveis e, portanto, **«dados pessoais»** na aceção do artigo 2. o, alínea a), da referida diretiva.
>
> Por conseguinte, há que declarar que, ao explorar a Internet de forma automatizada, constante e sistemática, na busca das informações nela publicadas, **o operador de um motor de busca «recolhe» esses dados, que «recupera», «registra» e «organiza» posteriormente no âmbito dos seus programas de indexação, «conserva» nos seus servidores e, se for caso disso, «comunica» e «coloca à disposição» dos seus utilizadores, sob a forma de listas de resultados das suas pesquisas.**

Referente ao direito de apagar dados pessoais, o Tribunal decidiu que diante do tempo do fato (16 anos) não existia mais razão para justificar a permanência dos dados na rede, conferindo ao autor o direito de "exigir a supressão das referidas ligações dessa lista de resultados".[11]

No direito à obscuridade as informações pessoais não estão disponíveis para todos, possuindo um difícil acesso em razão de fatores específicos. Já o direito ao esquecimento digital de dados coletados por serviços secretos refere-se ao direito que o indivíduo tem de requerer que as redes sociais, *browsers,* e servidores de suprimir ou cancelar informações constantes nas suas bases de dados, sendo necessário provar a irrelevância das informações que serão potencialmente apagadas (CASTETS-RENARD; VOSS, 2016).

---

[10]Idem.
[11]Idem.

Além do direito ao esquecimento, outros direitos se aperfeiçoam diante da pós-modernidade, como o direito à imagem, sigilo de correspondência e as relações de consumo, por exemplo. Tecnologias são constantemente criadas com o intuito de obter informações referentes ao comportamento, hábitos financeiros e lazer dos usuários, como aplicativos que permitem a manipulação de fotografias, as redes sociais e os sites de compras *online*. Entretanto, o uso reiterado dessas tecnologias pode culminar na permissão de acesso às informações bancárias, como senhas e dados financeiros, assim como outros dados importantes do usuário, isso ocorre em razão dos contratos eletrônicos de adesão que impõem termos e condições de uso como forma condicionada de viabilizar esse acesso.

Nesse ponto, em particular, questiona-se o respeito ao princípio da boa-fé objetiva e de seus desdobramentos do proprietário, hospedeiro ou provedor do *site* no momento de criação do contrato de adesão. É imperioso o cumprimento desse princípio, tendo em vista que os usuários, em sua maioria, não são capazes de discernir as cláusulas presentes no contrato e prever os possíveis efeitos em seu âmbito privado.

Segundo Paulo Lôbo (2019) o direito à privacidade no contexto atual da virtualização abrange o "autogoverno dos dados pessoais" por se tratar de um direito da personalidade, ou seja, os titulares desse direito devem possuir autonomia para poder resguardar seus dados com o objetivo de proteção de sua esfera privada, além desses dados possuírem um grande valor de mercado que implica em um enriquecimento por parte das entidades privadas se valendo da quebra dos parâmetros da privacidade.

Observa-se da análise das ramificações do direito à privacidade que as relações humanas no ciberespaço necessitam de uma regulação que se adeque constantemente aos avanços tecnológicos e sociais, e que os ordenamentos jurídicos acompanhem essa evolução como forma de garantir o aspecto individual desse direito.

2.3. OS DESAFIOS DA MODERNIDADE LÍQUIDA: A INFORMAÇÃO, A EXPOSIÇÃO E A VIGILÂNCIA

A modernidade líquida faz analogia ao estado físico da matéria, quer este seja o estado líquido. Esse período é assim definido por Zygmunt Bauman em razão da fluidez presente no estado líquido, que implica na dificuldade da união de moléculas na manutenção de uma forma específica, isso ocorre justamente por não haver uma tensão particular, diferentemente

do estado sólido da matéria, em razão das partículas estarem tensionadas, elas conseguem permanecer estáveis em um formato estabelecido (BAUMAN, 2001).

Toda essa explicação verte na sociedade pós-moderna atual, na qual as relações são fluidas/líquidas, e consequentemente impossíveis de serem definidas em um formato específico. Na modernidade líquida "indivíduos" passam por um processo de emancipação, no qual a noção inicial de comunidade como coletividade é superada, ou seja, a comunidade antes possuía aspectos referentes ao estado sólido da matéria com comunidades de formatos específicos e imutáveis é superada, na modernidade líquida não existe mais uma tensão que delimita as relações entre os sujeitos, o que implica em uma multiplicidade de relacionamentos sem formatação prévia.

Todavia, mesmo diante da emancipação individual surge necessidade de integração em um corpo social, como a rede mundial de computadores, que pode ser considerado o modelo moderno e mais comum de comunidade. Nesse contexto, Bauman (2001) afirma que

> O que foi separado não pode ser colado novamente. Abandonai toda esperança de totalidade, tanto futura como passada, vós que entrais no mundo da modernidade fluida. Chegou o tempo de anunciar, como fez recentemente Alain Touraine, "o fim da definição do ser humano como ser social, definido por seu lugar na sociedade, que determina seu comportamento e ações". Em seu lugar, o princípio da combinação da "definição estratégia da ação social que não é orientada por normas sociais" e a "defesa, por todos os atores sociais, de sua especificidade cultural e psicológica" "pode ser encontrado dentro do indivíduo, e não mais em instituições sociais ou em princípios universais

A modernidade líquida possui como esteio a rede mundial de computadores, que funciona como forma de integração e comunicação dos atores sociais. Seu surgimento pode ser datado na década de 1960, em que os responsáveis pela Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos (DARPA), criaram a internet como forma de proteção ao sistema de comunicação norte-americano pelos soviéticos no caso de uma possível guerra nuclear, o que resultou em uma arquitetura em rede que não possui um único núcleo, mas vários núcleos autônomos com diversas conexões que contornam barreiras eletrônicas. Após o fim da Guerra Fria, a ARPANET foi utilizada para outros fins por milhares de usuários do mundo inteiro, criando extensas redes de comunicação derrubando as paredes fictícias da territorialidade (CASTELLS, 1999).

Nos Estados Unidos na década de 1970 que surge um "novo paradigma tecnológico, organizado com base na tecnologia da informação", tendo em vista que diante do contexto geopolítico e econômico mundial houve a concretização de "um novo estilo de produção,

comunicação, gerenciamento e vida". Os avanços nessa época decorrem da cultura da liberdade, da inovação individual e do espírito empreendedor norte-americano, já que a criação de mecanismos tecnológicos de formação de rede, da incessante busca por avanços tecnológicos e a interação social personalizada não faziam parte da tradição de uma cultura corporativista (CASTELLS, 1999).

Nas palavras de Manuel Castells (2001) "os primeiros estágios do uso da Internet, na década de 1980, foram anunciados como a chegada de uma era de comunicação livre e realização pessoal nas comunidades virtuais formadas em torno da comunicação medida pelo computador". Ou seja, a grande promessa da Internet era permitir a conexão de diversos grupos de pessoas transgredindo as barreiras territoriais antes existentes utilizando-se apenas dos computadores como meio de comunicação.

Diante do contexto tecnológico e social atual, constata-se que a promessa foi cumprida e que ampliou ainda mais seu objetivo inicial, tendo em vista que a comunicação é universal e continua a ser realizada por computadores, estes cada vez mais sofisticados como os famosos *gadgets*. Entretanto, a Internet não é apenas um meio de comunicação, passando a integrar os meios de trabalho, difusão de informações e a interferir na economia, lazer e modo de comportamento dos indivíduos.

Na sociedade pós-moderna as mídias sociais cumprem o papel de integrar em forma de comunidade os indivíduos, que agora podem ser identificados como "usuários". O momento de integração acontece com apenas um *click* e perdura pelo tempo escolhido, configurando, portanto, na fluidez presente na modernidade líquida.

O autor Byung-Chul Han (2012), em seu livro Sociedade da Transparência, discorre que a sociedade atual passa por um processo de exposição, tendo em vista que:

> A negatividade do apartar *(secret, secretus)*, delimitação, reclusão é constitutiva para o valor cultural. Na sociedade positiva, na qual as coisas, agora transformadas em mercadorias, têm que ser expostas para *ser*, seu valor cultural desaparece em favor de seu valor positivo. Em vista desse valor expositivo, sua existência perde a importância. Pois, tudo que repousa em si mesmo, que se demora em si mesmo a não ter mais valor, só adquirindo algum valor se for *visto*.

O autor afirma também que há a substituição do caráter privado em detrimento da publicização da pessoa, em que o público é transformado em exposição, afastando-se por completo do "agir comum". Em suma, o que se percebe é que os indivíduos, principalmente os que estão integrados nas comunidades por meio de mídias sociais, consentem em ter seu

âmbito privado publicizado, gerando uma constante exposição, o que desemboca na deturpação de direitos fundamentais, com ênfase no direito à privacidade.

Assim coaduna Zygmunt Bauman (2013), sustentando que

> A área da privacidade transforma-se num lugar de encarceramento, sendo o dono do espaço privado condenado e sentenciado a padecer expiando os próprios erros; forçado a uma condição marcada pela ausência de ouvintes ávidos por extrair e remover os segredos que se ocultam por trás das trincheiras da privacidade, por exibi-los publicamente e torná-los propriedade comum de todos, que todos desejam compartilhar.

Percebe-se diante da narrativa de Zygmunt Bauman, que o usuário das redes se submete a uma matança de seus direitos da privacidade espontaneamente. Isso ocorre justamente porque estamos diante de uma sociedade informacional, e como forma de autoafirmação do sujeito como indivíduo pertencente àquela rede. Em alusão a essa autoafirmação, a necessidade de ter segredos se esvai, em que os usuários passam a ser felizes quando compartilham suas informações mais íntimas, a exposição passa a ser o aspecto central da existência na sociedade da informação (BAUMAN; LYON, 2013).

Isso desemboca no paradigma da vigilância contemporânea, que tem como base o modelo proposto por Jeremy Bentham e seu Panóptico, um tipo ideal de prisão vigiada por uma única pessoa em razão de sua arquitetura circular, sem que os prisioneiros saibam se estão sendo vigiados ou não. Assim como a distopia moderna proposta por George Orwell, em seu livro 1984, em que os sujeitos submetidos a um governo autoritário imposto pelo Grande Irmão, tendo suas ações vigiadas por teletelas – uma espécie de televisão que além de repassar informações, entretenimento, funciona como uma câmera de vigilância – e qualquer ação suspeita é notada e imediatamente investigada.

De acordo com Byung-Chul Han (2017) que o " panóptico digital do século XXI é aperspectivístico na medida em que não é mais vigiado de um centro, não é mais supervisionado pela onipotência do olhar do panóptico", diferenciando-se do modelo do Panóptico proposto por Bentham, já que o modelo por ele proposto partia do fenômeno de uma sociedade disciplinar, sendo utilizado principalmente em presídios, de forma a possuir uma natureza unilateral de transparência. Contudo, no modelo atual de panóptico digital os indivíduos - ao contrário dos presos que não podiam se comunicar - estão conectados em uma rede, comunicando-se a todo momento, configurando o isolamento atual. Nesse contexto, os usuários abrem mão de sua esfera privada e íntima como forma de integração no sistema do panóptico digital.

Eventos como o vazamento de dados confidenciais no *Wikileaks* por Edward Snowden e o atentado às Torres Gêmeas nos Estados Unidos, além de diversos acontecimentos atuais que envolvem o processamento de dados pessoais impulsionaram a necessidade de criar mecanismos de proteção e de vigilância.

A sociedade da vigilância é toda aquela que possui dependência de comunicação e de tecnologias da informação para processos de controle e administração. O chamado *Surveillance*é a coleta e processamento de dados pessoais, estes sendo identificáveis ou não, com o propósito de influenciar e gerenciar os dados coletados. Contudo, apesar de ser uma tecnologia necessária que impulsiona o futuro, permitindo a descoberta de desvios legais praticados pelos usuários da rede ou como meio de facilitar transações e interações dos indivíduos (LYON, 2011), esse tipo de tecnologia pode permitir que todo o complexo de informações do usuário estejam à disposição dos controladores de dados e informações, não garantindo, portanto, que haverá a proteção da privacidade dos sujeitos de direito.

Todavia, apesar da vigilância constante não existem consequências danosas para os usuários, segundo Manuel Castells (2003) o

> O aspecto mais atemorizante é, de fato, a ausência de regras explícitas de comportamento, de previsibilidade das consequências do nosso comportamento exposto, segundo os contextos de interpretação, e de acordo com critérios usados para julgar nosso comportamento por uma variedade de autores atrás da tela de nossa casa de vidro. Não é o *Big Brother*, mas uma multidão de irmãzinhas, agências de vigilância e processamento de informações que registram nosso comportamento para sempre, enquanto bancos de dados nos rodeiam ao longo de toda nossa vida. (...)

No cenário atual, esse processo de vigilância não pode mais ser considerado como um atentado à liberdade, já que o há a livre exposição ao panóptico, para Byung-Chul Han (2018) o "presidiário do panóptico digital é ao mesmo tempo agressor e vítima, e nisso que reside a dialética da liberdade, que se apresenta como controle".

Os dispositivos eletrônicos possuem tecnologia de controle refinada na coleta de dados, que atualmente incluem o uso de senhas, quer estas sejam numéricas ou biométricas, os *cookies* dos sites que utilizamos, e os procedimentos de autenticação. Os *cookies* servem como um tipo de marcador digital automático inseridos pelos sítios da Internet, fazendo alterações no disco rígido, a partir disso ele passa a monitorar toda movimentação realizada on-line pelo servidor que fez a instalação. A utilização de autenticação por assinaturas digitais

é outro exemplo, esse tipo de ação permite que outros computadores verifiquem qual a origem e características dos seus correspondentes (CASTELLS, 2003).

Além da vigilância que os próprios usuários realizam reciprocamente, já que o novo modelo de entretenimento é o de observar a vida alheia, agindo como mero expectador, com a decorrente exposição como forma de integração ao *loop* infinito de exposição *versus* monitoramento.

Outro exemplo da sociedade de vigilância é da tecnologia de reconhecimento facial implantada na China, em que a inteligência artificial se utiliza de um banco de dados como forma de monitoramentos dos cidadãos, o que facilita na investigação ou coibição da prática de delitos, além de sistematizar os serviços de emergência e ajudar na fiscalização dos habitantes do país. Isso influencia no sistema de "crédito social"[12] idealizado pelo governo Chinês, em que os cidadãos ganham pontos por diversas ações como voluntariado ou por atrair investimentos para cidade, o *score* de cada cidadão implica no acesso dos programas de bem-estar, em que os *high scores* possuem acesso a *checkups* médicos gratuitos, enquanto os *low scores* são barrados de empregos públicos, por exemplo.[13]

Todavia, esse tipo de tecnologia permite ao Estado manter-se em um status de *Big Brother*, todas as ações dos indivíduos são monitoradas 24h permitindo um controle estatal onipresente, isso pode desembocar em atitudes abusivas e totalitárias por parte do Estado.

De forma semelhante segue o Estado Brasileiro com os Decretos nº 10.046 e 10.047 de 09 de outubro de 2019, ambos aprovados pelo atual Presidente da República, os quais permitem a criação dão origem ao Cadastro Base do Cidadão e o Comitê Central de Governança de Dados, uma megabase de dados pessoais dos cidadãos, dados esses que estão elencados no art. 2º[14] do Decreto nº 10.046, que vão desde atributos biográficos, genéticos, laborais até biometria.

---

[12] Disponível em: https://revistasegurancaeletronica.com.br/china-utiliza-reconhecimento-facial-para-conseguir-vigilancia-total-no-pais/. Acesso em: 12/10/2019.

[13] Disponível em: https://www.technologyreview.com/f/613027/chinas-social-credit-system-isnt-as-orwellian-as-it-sounds. Acesso em: 12/10/2019.

[14] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 12/10/2019.

Esse decreto vai de encontro a Lei Geral de Proteção de Dados, que regula o tratamento de dados pessoais, limitando o uso e tratamento desses por entidades privadas. Nesse momento, o vigilante da sociedade brasileira passa a ser o próprio Estado, o qual deterá uma quantidade infinita de dados pessoais dos brasileiros.

Nas palavras de Bauman (2013)

> A arquitetura das tecnologias eletrônicas pelas quais o poder se afirma nas mutáveis e móveis organizações atuais torna a arquitetura de paredes e janelas amplamente redundante (não obstante firewalls e windows). E ela permite formas de controle que apresentam diferentes faces, que não têm uma conexão óbvia com o aprisionamento e, além disso, amiúde compartilham as características da flexibilidade e da diversão encontradas no entretenimento e no consumo.

Outros tipos de tecnologia, como a Internet das Coisas, que permite o uso de vários aparelhos conectados por uma rede *wireless* (sem fios), coordenando diversas atividades simultâneas, como no monitoramento de câmeras, ou nas *smart TVs* e nos *smart cars,* por exemplo, realizando a coleta e tratamento de dados ao concomitantemente. Entretanto, apesar de ser uma tecnologia valida e importante no desenvolvimento de softwares, por possuir essa conexão sem fios é extremamente vulnerável a ataques de *hackers*, o que implica em uma potencial invasão à privacidade do seu titular.

Esses são exemplos de implicações modernas e habituais que os sujeitos da pós-modernidade/modernidade líquida se deparam, isso demanda um cuidado máximo na proteção da privacidade do usuário, buscando ainda formas de respeitar, também, suas liberdades individuais.

3. ESTUDOS REFERENTES À PROTEÇÃO DE DADOS PESSOAIS NA UNIÃO EUROPEIA

3.1. EVOLUÇÃO LEGAL DA REGULAÇÃO DE DADOS NO CONTEXTO EUROPEU

A Europa, diante de seu desenvolvimento econômico e social, encontra-se na vanguarda da proteção de direitos como a privacidade, intimidade, liberdades e como consequência a proteção de todos os dados de natureza pessoal dos atores das relações sociais digitais. Pode-se afirmar que um dos primeiros marcos reguladores criados sobre o tema adveio da Organização para Cooperação e Desenvolvimento Econômico (OCDE), com as denominadas Diretrizes da OCDE, denominada como "Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais", a qual entrou em vigor em 23 de setembro de 1980 (MIRANDA, 2018).

Essas Diretrizes foram adotadas no formato de recomendação, baseando-se em três princípios basilares que se estendem a todos os países membros da Organização, são eles: democracia pluralista, respeito aos direitos humanos e economias de mercado aberto. Afirmam que as referidas diretrizes fazem parte de um "consenso internacional sobre a orientação geral a respeito da coleta e do gerenciamento da informação pessoal"[15]. Aduzem ainda que os princípios presentes nas Diretrizes são dotados de clareza e flexibilidade na formulação e aplicação, o que permite acompanhar os avanços tecnológicos e sociais. Segundo o documento[16]

> Esses princípios abrangem todos os meios utilizados para o processamento automatizado de dados referentes a indivíduos (do computador local à rede de complexas ramificações nacionais e internacionais), todos os tipos de processamento de dados pessoais (da administração do pessoal ao levantamento de perfis de consumidores) e todas as categorias de dados (da circulação de dados ao seu conteúdo, dos mais comuns ao mais sensíveis). Os princípios aplicam-se a ambos os níveis nacional e internacional.

Extrai-se que o principal objetivo das Diretrizes é o de oferecer uma maior segurança no que se refere ao processamento e trânsito de dados, o que implica consequentemente na proteção à Privacidade, em razão do processo ser dotado de segurança e confiabilidade.

---

[15]Disponível em: http://www.oecd.org/sti/ieconomy/15590254.pdf
[16] Idem.

Outro instrumento regulatório importante foi a Convenção para a proteção de indivíduos no que diz respeito ao processamento automático de dados pessoais (Convenção 108[17]), também conhecida como Convenção de Estrasburgo. Seu principal objetivo era o de proteger os indivíduos de abusos provenientes da coleta e tratamento de dados pessoais, com a proibição ao tratamento de dados pessoais sensíveis referentes à raça, política, religião, vida sexual e antecedentes criminais, assim como a salvaguarda do direito do individuo saber quais informações são armazenadas na rede e, caso necessário, corrigi-las. Essa Convenção integra o direito à proteção de dados e o acesso à informação como partes inerentes aos direitos humanos, passíveis, portanto, de proteção. Sua importância se justifica na possibilidade de adesão de países não membros da União Europeia, dada a relevância dos direitos postos em discussão pela Convenção.

Contudo, é em 1995 com a elaboração da moderna Diretiva 95/46/CE, que a União Europeia inicia um movimento vanguardista no que se refere ao direito à privacidade na era da informação. A Diretiva trata de assuntos como o trânsito seguro de dados pessoais, respeitando os direitos fundamentais e liberdades dos indivíduos, não importando a nacionalidade ou residência e principalmente a vida privada, de forma a contribuir para o progresso econômico e social, bem como o desenvolvimento do comércio e o bem-estar dos indivíduos[18].

3.1.1 Questões relativas à Diretiva 94/46/CE e sua importância na proteção de dados

A Diretiva 95/46/CE veio a ser complementada pela Diretiva 2002/58/CE, que evidencia nas considerações 2 e 319 as perspectivas adotadas pelo instrumento, a primeira diz respeito ao caráter protetivo da Diretiva, já que seu principal objetivo era o de manter asegurança durante a coleta, transmissão e tratamento de dados dos indivíduos; já a segunda é

---

[17] Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37

[18] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT

[19] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=PT

de que barreiras não fossem criadas exageradamente de forma a impedir os progressos de natureza científica e econômica (MIRANDA, 2018).

Essa Diretiva surge com o escopo de harmonizar a legislação em matéria de proteção dos dados pessoais, da privacidade e dos interesses legítimos das pessoas coletivas no setor das comunicações eletrônicas, no que se refere aos países membros do bloco Europeu. Sua natureza vinculativa, no entanto, estabelece apenas uma referência a ser seguida pelos países membros do bloco, já que se buscava que esses adotassem legislações próprias no que se refere aos direitos supracitados.

Conceitos importantes são encontrados no art. 2º, como o conceito de dados pessoais, tratamento de dados, ficheiro de dados pessoais, responsável pelo tratamento, subcontratante, terceiro, destinatário e o consentimento da pessoa em causa. Por dados pessoais tem-se que

> qualquer informação relativa a uma pessoa singular identificada ou identificável (« pessoa em causa »); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica,psíquica,econômica, cultural ou social.

Constata-se que o consentimento é fator importante nas regulações de dados já que parte do pressuposto da proteção às liberdades dos sujeitos, a diretiva em seu art. 2º, define-o como "qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento".

A Diretiva dispõe em seu art. 2º, alínea b, que o tratamento de dados é

> qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição.

Além de estabelecer princípios que regem a qualidade dos dados, a categoria dos dados, princípios que legitimam o tratamento, além dos tipos de tratamento. Outros princípios importantes são elencados na Diretiva, são eles:

a) publicidade, que impede a criação de bancos de dados secretos, conforme a consideração 48;

b) finalidade, que dita que as informações apenas serão coletadas, armazenadas, tratadas e divulgadas para o fim que foram emitidas, de forma a obstruir qualquer tipo de desvio de finalidade, conforme o art. 6º, alínea b;
c) boa-fé, a qual determina o dever de lealdade entre o banco de dados e o cadastrado, estando diretamente ligada à finalidade, já que há a garantia de que a coleta de informações não será corrompida. A previsão da boa-fé se escora nos considerandos 25, 28 e 38, e no art. 6º, I, alínea a;
d) necessidade, que limita a coleta de dados de maneira proporcional à finalidade destinada, está presente no art. 6º, I, alínea c;
e) exatidão, que traz a imposição de que a coleta dos dados aconteça de forma exata e completa, mantendo-se atualizados. Está presente nos arts. 6º, I, alínea d e 12, diante da existência desse princípio extrai-se o direito do cadastrado de apagar, corrigir ou atualizar dados;
f) temporalidade, esse principio prevê que os dados não podem permanecer mantidos na base de dados *ad aeternum* em razão dos dados já terem cumprido sua finalidade, conforme o art. 6º, I, alínea e. Direitos correlatos surgem desse princípio, como o direito ao esquecimento, apagamento e desindexação de dados;
g) informação, o cadastrado possui o direito de saber que seus dados foram armazenados, além do acesso irrestrito aos cadastros realizados, com informações completas e precisas, com previsão nos considerandos 25, 39, 40 e arts. 10 e 11;
h) confidencialidade, esse principio determina que o dado somente poderá ser acessado para cumprir a finalidade a qual foi coletado, não sendo permitido o acesso a terceiros ou divulgação, buscando a manutenção da relação de confidencialidade estabelecida entre o cadastrado e o banco de dados, estando presente no art. 16;
i) segurança, determina que deverão ser criados mecanismos de proteção de dados, priorizando a confidencialidade das informações ao criar óbices que impeçam a divulgação, perda, alteração ou acesso indevido, com o fito de manter a finalidade que esse dado foi coletado, está presente no considerando 46 e no art. 17;
j) reparação integral, haverá a responsabilização integral do agente que der causa à invasão de privacidade ou que não cumpra as diretrizes normativas, por todos os danos causados por meio de indenização cabível, conforme exemplifica o art. 23;

Ademais, outras inovações relevantes foram objeto da Diretiva, como a impossibilidade de decisões individuais automatizadas, ou seja, uma pessoa física ou jurídica não poderia ficar sujeita a receber uma decisão que atinja significativamente sua esfera jurídica ou econômica, sendo essa tomada apenas com base no tratamento de dados que fossem destinados a avaliar questões referentes à personalidade, como questões referentes ao crédito, por exemplo. O mesmo artigo ainda prevê as exceções que permitem a aplicação da decisão acima descrita, com a clara necessidade de previsão legal anterior.

A criação de uma autoridade exclusiva e independente, responsável pela fiscalização, elaboração de pareceres, aplicação de sanções e de intervenção de infratores, foi uma das principais evoluções legais da Diretiva, conforme os considerandos 62 a 64, o que garantiu transparência e autonomia na fiscalização efetuada com o fito de proteger os direitos em tela.

Todavia, não se pode comparar o contexto de criação da Diretiva na Década de 90 com a época atual, já que esta é dominada por constantes avanços tecnológicos, aperfeiçoamento dos métodos de comunicação e evolução social. Diante disso, demonstrou-se a necessidade de criação de uma ampla e moderna legislação que pudesse abranger as novas relações sociais e os avanços na seara da tecnologia.

3.1.2. O caso *Cambridge Analytica* como marco na proteção de dados

Em 2018 o mundo presenciou o maior escândalo relacionado ao vazamento de dados, o *Cambridge Analytica/Facebook. Cambridge Analyitica* (CA) era uma sociedade fundada em 2013, funcionava como uma filial do *SLC Group (Strategic Communication Laboratories Group)* situado na Grã-Bretanha.

A *Cambridge Analytica* era uma empresa especializada em realizar um apanhado estratégico de informações que definiam questões comportamentais dos usuários como forma de influenciar o jogo político e atividades militares. O estopim do escândalo aconteceu com a publicação em março de 2018 pelo *New York Times*[20] e *The Guardian*[21], no texto das noticias

[20] Mais informações em: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Acesso em: 13/01/2020.

é possível constatar que a *Cambridge Analytica* era comandada por um dos consultores de Donald Trump, Stephen K. Bannon e financiada pelo republicano Robert Mercer. A empresa coletou os dados de mais de 50 (cinqüenta) milhões de usuários do site *Facebook*, traçando a partir de seu aspecto comportamental na rede o perfil político do usuário, sem a anuência implícita para utilização desses dados, o que impactou nas eleições norte-americanas de 2016 que elegeram o então presidente Donald Trump.

As notícias ainda mencionam a participação do político Ted Cruz, tendo em vista que ele foi um dos principais beneficiados nesse esquema, já que contratou a *Cambridge Analytica*para garantir vantagem sobre seus concorrentes nas eleições presidenciais norte-americanas a partir dessa coleta irregular de dados psicológicos de eleitores.

Entretanto, esse não foi o único evento em que a *Cambridge Analytica* se utilizou de dados pessoais dos usuários para influenciar no jogo político, já existem informações que evidenciam o tratamento de dados no referendo que retirou o Reino Unido da União Europeia, até as eleições presidenciais do Brasil, por exemplo. Posteriormente, foi descoberto que a empresa possuía acesso aos dados de 87 (oitenta e sete) milhões de usuários, bem como informações sigilosas pertencentes ao Tesouro.

Essa atitude implicou em uma polarização por manipulação, que se perfaz com a utilização de três métodos: o primeiro método acontece diante da abundancia de usuários as empresas se utilizam de campanhas e anúncios como forma de criar micro-alvos e perfis psicográficos. O segundo diz respeito à manipulação nas redes sociais a partir de algoritmos que direcionam o usuário a questões referentes a ganhos políticos, sociais e econômicos. O terceiro método utilizado para manipulação é o dos *bots* automáticos e algoritmos de redes sociais que disparam continuamente *fake news,* discurso de ódio e conspirações que distorcem o processo político.[22]

---

[21] Mais informações em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 13/01/2020.

[22] Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf. P. 22. Acesso em: 13/01/2020.

O *Information Commissioner's Office (ICO[23])* é o responsável pela investigação das ações da *Cambridge Analytica*, e em julho de 2011 publicou o documento que trata sobre a investigação realizada no processo *Cambridge Analytica/Facebook,* denominado de "Investigação sobre o uso de dados analíticos em campanhas políticas"[24]. Nesse documento o *IOC* demonstra a intenção de multar o *Facebook* por falta de transparência e segurança na coleta de dados, se valendo do *Data Protection Act 1998* que estava em vigor no Reino Unido à época.

Com o advento do *General Data Protection Regulation* o ente adquiriu novos poderes que permitem uma investigação mais aprofundada, já que os dados coletados de forma irregular são pessoais, ou seja, possuem um vinculo com um individuo identificado ou identificável, por estarem presentes em uma rede social amplamente utilizada e que para ingressá-la o usuário deposita seus dados pessoais.

Essa nova Regulação surge com o escopo de proteger os dados pessoais de situações como a exposta, implicando em uma maior responsabilização dos detentores dos meios de tratamento e coleta. Diante disso, o usuário possuíra uma maior segurança jurídica e dificilmente passará pela manipulação política ora explicada.

3.2. *GENERAL DATA PROTECTION REGULATION*: QUESTÕES REFERENTES AO SEU DESENVOLVIMENTO LEGISLATIVO, APLICAÇÃO E SEUS EFEITOS NO SISTEMA NORMATIVO EUROPEU E BRASILEIRO

Em exercício desde 25 de maio de 2018, a *General Data Protection Regulation (GDPR)* surgiu com o escopo de dirimir questões referentes á legislação de dados na União Europeia, harmonizando o sistema normativo europeu como forma de garantir uma proteção devida aos direitos decorrentes do uso das tecnologias da informação.

---

[23] Mais informações em: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/ico-statement-investigation-into-data-analytics-for-political-purposes/. Acesso em 13/01/2020.

[24] *Investigation into use of the data analytics in political campaigns.* Disponível em: https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf. Acesso em: 13/01/2020.

A *GDPR* foi promulgada em 27 de abril de 2016 pelo Regulamento 2016/679[25], revogando a Diretiva 95/46/CE e sua publicação aconteceu em 27 de abril de 2016, contudo, por se tratar de uma legislação complexa, ficou estabelecido o período de transição de dois anos para adaptação de todas as pessoas físicas e jurídicas. Nesse ponto, observa-se que o Brasil seguiu a mesma orientação para o período de adequação, determinando um *vacatio legis*diferenciado com a duração idêntica a estabelecida na *GDPR*.

A maior modificação estabelecida da Regulação em relação a Diretiva diz respeito a sua força vinculante, tendo em vista que a Diretiva como já explicado, possuía como principal função o direcionamento dos países-membros no momento de criação de legislações próprias, permitindo uma maior discricionariedade dos membros, diferentemente da Regulação que possui natureza vinculativa com a aplicação de todos os seus artigos nos países-membros, não sendo necessária a criação de outro instrumento legislativo que legitime sua aplicação. A harmonização do sistema normativo dos países-membros da UE foi um dos objetivos que guiou a criação dessa Regulação.

O legislador no momento de elaboração da Regulação, teve o cuidado de criar uma norma que protegesse os usuários da melhor maneira, mas que também não impedisse o desenvolvimento econômico resultante das tecnologias, conforme expõe o considerando nº 2

> Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais **deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais**. O presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, **para o progresso econômico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares**.

Esse considerando se respalda na existência de diversas transações econômicas realizadas digitalmente por grandes e pequenos empresários, além de empresas que se utilizam do tratamento de dados como forma de renda, de forma que impede a criação de óbices que possam de algum modo a interferir no desenvolvimento de negócios.

---

[25]Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Acesso em: 13/01/2020.

Em razão disso, buscou-se gerar a confiança tanto dos agentes que se utilizam para obter ganhos econômicos, quanto dos usuários, que muitas vezes são a parte hipossuficiente dessa relação jurídica, além da constante evolução tecnológica. Nesse sentido, a Regulação cria uma segurança jurídica que permite que os empresários realizem investimentos e transações econômicas, gerando o desenvolvimento econômico, o que permite também a salvaguarda dos direitos dos usuários, conforme a expõem os considerandos 6 e 7.

3.2.1. Âmbitos de aplicação da GDPR: material e territorial.

Outrossim, a *GDPR* estabelece os âmbitos de sua aplicação material em seu art. 2º, de forma que a Regulação "aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados", ou seja, o tratamento de dados deve ser realizado de forma neutra, independentemente do uso de tecnologia, com a aplicação de tratamento de dados automatizados ou manuais, caso esses dados estejam contidos em sistemas de arquivo (LIMA, 2018).

Já no que se refere ao âmbito territorial, o art. 3º enuncia que

> 1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado 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.

Em outras palavras, a *GDPR* é aplicada às empresas que realizam o tratamento de dados que possuem sedes físicas no território dos países membros da União Europeia, independe se o armazenamento desses dados seja em seu território, já que o Regulamento é aplicável a todos os titulares de dados que estejam presentes no território da EU, não importando a cidadania.

Já a segunda parte do art. 3º afirma que o regulamento será aplicado para o tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União quando as atividades de tratamento estejam relacionadas com a oferta de bens ou serviços a esses titulares de dados na União, não sendo exigido o pagamento, assim como o controle de comportamento, devendo esse ter lugar na União.

Em relação às questões referentes ao controle de comportamento, o considerando 24 elucida que

> O tratamento de dados pessoais de titulares de dados que se encontrem na União por um responsável ou subcontratante que não esteja estabelecido na União deverá ser também abrangido pelo presente regulamento quando esteja relacionado com o controle do comportamento dos referidos titulares de dados, na medida em que o seu comportamento tenha lugar na União. **A fim de determinar se uma atividade de tratamento pode ser considerada «controle do comportamento» de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes. (grifou-se)**

A Regulação também será aplicada ao "tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público", o considerando 25 traz exemplos dessa aplicação extraterritorial por força do direito internacional, como as missões diplomáticas ou postos consulares.

3.2.2. Análise sobre temas relevantes elencados no regulamento: dados pessoais, tratamento, responsabilidade e sanções na *GDPR*

Por dados pessoais, o regulamento entende, em seu art. 4º, 1, que são informações relativas a uma pessoa natural identificada ou identificável, tendo como pessoa identificável uma "pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular"[26].

A Lei Geral de Proteção de Dados[27] brasileira se vale do mesmo conceito de dados pessoais, determinando em seu art. 5º, I, que esses dados seriam relativos a uma pessoa identificada ou identificável. Isso acontece porque o legislador brasileiro tomou como base a *GDPR* no momento da feitura da lei, justamente em razão da vanguarda legislativa europeia que permitiu a criação de uma lei moderna, clara e ampla.

---

[26] Ibidem.

[27] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

A Regulação ainda traz conceitos como dados genéticos, dados biométricos e dados relativos à saúde, diferentemente do que acontece na legislação brasileira. Já no que se refere aos dados sensíveis, o regulamento separa um capítulo especial no art. 9º, separando-o em uma categoria especial de dados, conforme o exposto a seguir

> 1. É proibido o tratamento de dados pessoais que revelem **a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.**

Insta destacar que a lei sempre menciona "dados pessoais", isso implica na proteção de dados que estejam vinculados a uma pessoa identificada ou que seja identificável. Nesse sentido, também é necessário diferençar o dado pessoal de informação, segundo Danilo Doneda (2011) o dado pode ser considerado como uma pré-informação, ou seja, é uma informação em potencial antes de sua transmissão, o que requer uma prévia interpretação antes de adquirir sentido (*apud* WACKS, 1989). Já a informação pessoal deve possuir um vinculo que realize a ligação com a pessoa em questão, como suas características ou ações, nome civil ou domicílio, ou informações provenientes de seus atos, como os dados referentes ao seu consumo, opiniões, entre outras (DONEDA, 2011). A menção expressa de dados pessoais ocorre em razão de se fazer proteger dados que estejam vinculados a uma pessoa singular, resguardando seu direito à privacidade.

A regulação não faz menção expressa aos dados anonimizados, tem-se por dados anônimos todos aqueles que não possuem informações que permitam identificá-los, de forma que se torna inviável a identificação de seu titular até mesmo pelo responsável do tratamento.

A *Opinion 5/2014* sobre o *Article 29 Working Party*[28] dispõe sobre as questões referentes às técnicas de anonimização de dados pessoais, bem como os possíveis riscos decorrentes. Essas técnicas são divididas em níveis de robustez que devem ser baseados em três critérios: se é possível que esse dado possa individualizar o titular, se é possível ter ligações com esse individuo e por fim se é possível inferir informações sobre o individuo.

[28]Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Contudo, a *opinion* enuncia que a anonimização ideal é muito difícil de ser alcançada, criando riscos de reidentificação do dado que ora foi objeto de tratamento.

Contudo, o procedimento de pseudoanonimização dos dados é objeto de proteção da *GDPR* por estarem inseridos no contexto dos dados pessoais, o que implica em uma minimização de riscos para os titulares dos dados, além de servir como um tipo de ajuda para os responsáveis pelo tratamento e subcontratantes a cumprir as obrigações resultantes desse tratamento, conforme a disciplina do considerando 28. Por pseudoanonimização, a regulação entende que é o tratamento de dados pessoais que não podem ser atribuídos a "um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável", de acordo com o art. 4º, 5.

A pseudoanonimização ainda está presente da *GDPR* relacionada com o conceito de *Data Protection by Design* e *by default,* conforme o expresso em seu art. 25, 1,

> 1. **Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização**, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados. (grifou-se)

Da mesma maneira, o art. 32 se vale da pseudoanonimização como técnica de segurança na encriptação de dados pessoais. No que concerne o tratamento de dados, alguns requisitos deverão ser analisados para manter a licitude desse processo, conforme o art. 6º, requisitos como o consentimento do titular, ou quando for utilizado para execução de um contrato no qual o titular dos dados é parte, para o cumprimento de obrigações jurídicas, para defesa dos interesses vitais do titular, ou quando esse tratamento for objeto de interesse público, e por fim quando o tratamento for necessário para interesses legítimos pelo responsável ou por terceiros, excetuando-se os casos em que haja supremacia de interesses ou direitos do titular que justifiquem a proteção dos dados, principalmente se esse titular for menor.

Quando esse tratamento for realizado com base no consentimento, faz-se imprescindível que seja demonstrado o consentimento do titular, podendo esse consentimento ser retirado a qualquer momento, de forma que deve ser igualmente fácil dar e retirar esse consentimento (art. 7º).

Sobre responsabilidade pelo tratamento de dados, é obrigado ao responsável pelo tratamento que sejam implementadas medidas técnicas e organizacionais adequadas para que demonstrem que esse tratamento segue o disposto na regulação (art. 25).

Outro ponto importante é a criação de uma autoridade supervisora da aplicação da regulação, todavia, cada Estado-membro é responsável por essa supervisão (art. 51). A autoridade deverá agir com independência no desempenho de suas atividades, em que seus membros deverão estar livres de qualquer tipo de influência direta ou indireta, externa ou interna, da mesma forma esses membros deverão abster-se de ações incompatíveis com sua função. Possui poderes investigativos, corretivos, de autorização e consultoria (art. 58) e deve enviar um relatório anual sobre as atividades desempenhadas.

É direito dos titulares de dados, sem prejuízos ao processo administrativo ou judicial, de apresentar uma queixa perante a autoridade supervisora de dados, essa será responsável por informar os avanços do processo (art. 77), e da mesma forma poderá interpor um recurso administrativo ou judicial em face de uma decisão vinculativa emitida pela autoridade supervisora (art. 78).

Insta mencionar que a legislação brasileira de dados também criou uma autoridade competente de supervisão, contudo a autoridade brasileira possui caráter transitório, o que implica em uma mudança futura, e não possui o mesmo tipo de independência que a autoridade supervisora europeia.

No que concerne a indenização, a regulação assegura que toda pessoa que sofrer algum tipo de dano que viole alguma previsão ora estabelecida terá o direito de receber uma indenização pelo tratamento ou pelo processador do dado (art. 82). Por fim, o responsável por definir as sanções aplicadas é o Estado-membro, especialmente as que não são objetos de sanções administrativas previstas no art. 83, as sanções devem ser efetivas, proporcionais e dissuasivas.

Diante do exposto, verifica-se que a Lei Geral de Proteção de Dados brasileira, em muitos pontos, como será demonstrado no próximo capítulo, reproduziu partesdo texto do

regulamento europeu. Essa atitude do legislador brasileiro se justifica no refinamento que a *GDPR* trouxe na proteção efetiva de dados, com uma maior responsabilização no tratamento e com sanções e compensações que efetivam o sentimento de segurança jurídica.

4. LEGISLAÇÃO BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS

4.1. O MARCO CIVILDA INTERNET: O PRIMEIRO MARCO REGULADOR DE PROTEÇÃO DE DADOS PESSOAIS

O processo de integração do Brasil na sociedade da informação acontece paulatinamente desde a criação do projeto de mesmo nome em 1996. Diante disso, observa-se a crescente modernização dos campos da comunicação e tecnologia no território brasileiro, com a consequente informatização da sociedade que passa a integrar o contexto mundial da digitalização no ciberespaço.

Nessa senda, em 2014 foi sancionado o Marco Civil da Internet (Lei nº 12.965/14), que tinha como principal objetivo a regulamentação as relações advindas do ciberespaço, normatizando a utilização da Internet através de princípios e diretrizes norteadoras. A Lei nº 12.965/14 foi elaborada diante da necessidade de adequação do ordenamento jurídico pátrio ao contexto da virtualização das relações jurídicas, justamente em razão da lacuna legislativa existente, o que dificultava a efetiva tutela dos direitos decorrentes dessas novas relações jurídicas.

Um das principais escolhas da lei foi a priorização da liberdade de expressão e da privacidade como *conditio sine qua non,* conforme o disposto no caput no art. 2º, além de outros como o reconhecimento da escala mundial da rede, os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais, a pluralidade e a diversidade, a abertura e a colaboração, a livre iniciativa, a livre concorrência e a defesa do consumidor, assim como a finalidade social da rede.[29]

A própria lei traz conceitos importantes em seu art. 5º, que enuncia

> 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;

[29]Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

> 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.

Tratando-se do direito à privacidade, esse aparece como um dos princípios basilares que disciplinam o uso da internet, bem como o tratamento dos dados pessoais (art. 3º). Já no art. 7º, observa-se a ratificação de direitos previstos constitucionalmente, como a inviolabilidade da intimidade e vida privada, com a consequente sanção pecuniária revestida pelo dano moral nos casos de violações, além da inviolabilidade do sigilo das correspondências eletrônicas. A lei inova quando trata nos incisos VI, VII e VIII estabelecendo regulamentação sobre o tratamento de dados, exigindo transparência nos contratos de prestação de serviço, no fornecimento condicionado de dados pessoais a terceiros, além da exigência de informações claras sobre coleta, uso, tratamento e proteção de dados. O consentimento do titular dos dados passa a figurar como ponto principal no tratamento de dados, o que confere em uma segurança jurídica ao indivíduo na escolha de fornecimento de dados para o tratamento.

Outro ponto importante é o da neutralidade da internet, prevista no art. 9º, que determina que os responsáveis pelo tratamento de dados devem "tratar de forma isonômica quaisquer pacote de dados, sem estabelecer distinções por conteúdo, origem e destino, serviço, terminal ou aplicação"[30], além de estabelecer que nos casos de degradação e mitigação dos tráfego, o responsável pelo tratamento deverá seguir o rito previsto no §2º do referido artigo

[30]Ibidem.

> § 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 doart. 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.

No que concerne a regulamentação de registros de conexão e de acesso a aplicações de internet, incluindo-se os dados pessoais e o conteúdo de comunicações privadas, há o e estreitamento com o conteúdo da preservação da intimidade, da vida privada, da honra e da imagem dos agentes envolvidos na relação, com enfoque na disponibilização mediante ordem judicial de dados de comunicação privada.

Destaca-se no Marco Civil a imposição de medidas que impõem responsabilização de terceiros no tratamento dos dados pessoais, estabelecendo que o provedor de internet não poderá ser responsabilizado civilmente por danos causados por terceiros, exceto nos casos em que mesmo após ordem judicial não tome providências necessárias para tornar indisponível o conteúdo infringente.

Entretanto, diante do exposto, percebe-se que o trâmite para responsabilização dos provedores é extremamente burocrático, podendo causar efeitos danosos para o sujeito que possui algum de seus direitos mitigados de ter sua pretensão acolhida, justamente porque os interesses das grandes empresas na área foram priorizados, apesar de que no seu processo legislativo foram acolhidas demandas enviadas pela sociedade civil para sua melhor adequação.

Nos últimos anos os Tribunais Brasileiros utilizam o Marco Civil da Internet como principal regulação legal com o fito de dirimir as pretensões de direito dos indivíduos pertencentes ao ciberespaço. Como ilustra a seguinte jurisprudência do Superior Tribunal de Justiça

> RECURSO ORDINÁRIO EM MANDADO DE SEGURANÇA. INQUÉRITO POLICIAL. QUEBRA DE SIGILO TELEMÁTICO. DESCUMPRIMENTO DE ORDEM JUDICIAL. ALEGAÇÕES DE AUSÊNCIA DE INDÍCIOS DE AUTORIA DELITIVA E DE VIOLAÇÃO A DIREITO DE TERCEIRO. NÃO CABIMENTO. APLICAÇÃO DE MULTA DIÁRIA. EMPRESA SITUADA NO PAÍS. SUBMISSÃO À LEGISLAÇÃO NACIONAL. **MARCO CIVIL DA INTERNET**. INCIDÊNCIA. 1. Consta dos autos ter sido instaurado o Inquérito

> Policial nº 58728-34.2012.4.01.3400 com o objetivo de investigar a prática dos crimes tipificados no art. 10 da Lei nº 9.296/1996 (Lei de interceptação) e art. 153, § 1º-A, do Código Penal - CP. Situação em A YAHOO! DO BRASIL INTERNET LTDA alega que o acórdão impugnado efetuou interpretação equivocada do **art. 10, § 1º, do Marco Civil da Internet e que ela tem o direito líquido e certo de não ser obrigada a fornecer dados pelos quais não é responsável pela guarda**. 2. É incabível, em sede de mandado de segurança - que na sua essência visa preservar direito líquido e certo - discutir indícios de autoria delitiva, matéria afeta ao Juízo criminal, que, ademais, demanda a análise dos elementos de prova colhidos na investigação. Precedentes. Para a impetração do mandamus é imprescindível que a prova do direito seja pré-constituída, sendo inviável imiscuir-se em matéria fática, mormente no caso concreto, em que a investigação não recai sobre a impetrante, mas sobre terceiros. A propósito, esta Corte Superior já se manifestou no sentido de que a destinatária da interceptação de dados não pode invocar direitos fundamentais de terceiros para eximir-se se cumprir a decisão judicial. Precedente. 3. Conforme jurisprudência do Superior Tribunal de Justiça "por estar instituída e em atuação no País, a pessoa jurídica multinacional submete-se, necessariamente, às leis brasileiras, motivo pelo qual se afigura desnecessária a cooperação internacional para a obtenção dos dados requisitados pelo juízo" (RMS 55.109/PR, Rel. Ministro REYNALDO SOARES DA FONSECA, QUINTA TURMA, julgado em 07/11/2017, DJe 17/11/2017) 4. Observe-se, ainda, que não há qualquer ilegalidade no fato de o delito investigado ser anterior à vigência do Marco Civil da Internet. Isto porque a Lei n.º 12.965/2014 diz respeito tão somente à imposição de astreintes aos descumpridores de decisão judicial, sendo inequívoco nos autos que a decisão judicial que determinou a quebra de sigilo telemático permanece hígida. Com efeito, a data dos fatos delituosos é relevante para se aferir apenas a incidência da norma penal incriminadora, haja vista o princípio da anterioridade penal, sendo certo que o inquérito policial investiga condutas que se encontram tipificadas no art. 10 da Lei nº 9.296/1996 (Lei de interceptação) e art. 153, § 1º-A, do Código Penal - CP e não na Lei n. 12.965/2014. 5. Recurso ordinário em mandado de segurança ao qual se nega provimento.
>
> (STJ - RMS: 55019 DF 2017/0201343-2, Relator: Ministro JOEL ILAN PACIORNIK, Data de Julgamento: 12/12/2017, T5 - QUINTA TURMA, Data de Publicação: DJe 01/02/2018)

A primeira jurisprudênciadiz respeito da suposta aplicação equivocada do art. 10 do Marco Civil em um caso de quebra de sigilo telemático, alegação realizada pela empresa Yahoo em sede recursal, recurso esse improvido. O art. 10 do Marco Civil determina que

> 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.

Nesse caso, buscava-se a quebra do sigilo como fito de angariar material probatório que lastreasse a acusação realizada, e a empresa Yahoo era a detentora de dados considerados essenciais ao seguimento do processo em análise.

Colaciona-se outro julgado com o objetivo de ilustrar a aplicação do Marco Civil no judiciário brasileiro

> RECURSO ESPECIAL. OBRIGAÇÃO DE FAZER E REPARAÇÃO CIVIL. DANOS MORAIS E MATERIAIS. **PROVEDOR DE SERVIÇOS DE INTERNET. REDE SOCIAL "ORKUT". RESPONSABILIDADE SUBJETIVA. CONTROLE EDITORIAL. INEXISTÊNCIA. APRECIAÇÃO E NOTIFICAÇÃO JUDICIAL. NECESSIDADE. ART. 19, § 1º, DA LEI Nº 12.965/2014 (MARCO CIVIL DA INTERNET). INDICAÇÃO DA URL. MONITORAMENTO DA REDE. CENSURA PRÉVIA.** IMPOSSIBILIDADE. RESSARCIMENTO DOS HONORÁRIOS CONTRATUAIS. NÃO CABIMENTO. 1. Cuida-se de ação de obrigação de fazer cumulada com indenização por danos morais e materiais, decorrentes de **disponibilização, em rede social, de material considerado ofensivo à honra do autor.** 2**. A responsabilidade dos provedores de conteúdo de internet em geral depende da existência ou não do controle editorial do material disponibilizado na rede. Não havendo esse controle, a responsabilização somente é devida se, após notificação judicial para a retirada do material, mantiver-se inerte.** Se houver o controle, o provedor de conteúdo torna-se responsável pelo material publicado independentemente de notificação. Precedentes do STJ. 3. Cabe ao Poder Judiciário ponderar os elementos da responsabilidade civil dos indivíduos, nos casos de manifestações de pensamento na internet, em conjunto com o princípio constitucional de liberdade de expressão (art. 220, § 2º, da Constituição Federal). 4. **A jurisprudência do STJ, em harmonia com o art. 19, § 1º, da Lei nº 12.965/2014 (Marco Civil da Internet), entende necessária a notificação judicial ao provedor de conteúdo ou de hospedagem para retirada de material apontado como infringente, com a indicação clara e específica da URL - Universal Resource Locator. 5. Não se pode impor ao provedor de internet que monitore o conteúdo produzido pelos usuários da rede, de modo a impedir, ou censurar previamente, a divulgação de futuras manifestações ofensivas contra determinado indivíduo.** 6. A Segunda Seção do STJ já se pronunciou no sentido de ser incabível a condenação da parte sucumbente aos honorários contratuais despendidos pela vencedora. 7. Recurso especial provido.
>
> (STJ - REsp: 1568935 RJ 2015/0101137-0, Relator: Ministro RICARDO VILLAS BÔAS CUEVA, Data de Julgamento: 05/04/2016, T3 - TERCEIRA TURMA, Data de Publicação: DJe 13/04/2016) **(grifou-se)**

Essa jurisprudência diz respeito a uma Ação de Obrigação de Fazer cominada com Danos Morais e Materiais, pela disponibilização indevida realizada pela rede social Orkut de material considerado ofensivo a honra do autor. O artigo utilizado foi o 19, §1º, *in verbis*

> 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.

O recurso foi provido com a justificativa que é necessária a notificação judicial ao provedor de conteúdo ou de hospedagem para retirada de material apontado como infringente, com a indicação clara e específica da *URL - Universal Resource Locator*, além de explanar a

dificuldade que o provedor tem de monitorar individualmente e ao mesmo tempo todo o conteúdo de seus usuários.

Contudo, o Marco Civil da Internet não conseguiu suprir efetivamente as demandas existentes, em razão dos avanços tecnológicos e sociais a legislação se tornou deficiente, o que implicou na necessidade de realização de um novo projeto de lei para completar as lacunas oriundas do Marco. A partir de consultas legislativas, de estudos de legislações estrangeiras, objetivando-se a maior abrangência da tutela jurídica dos direitos dos usuários da Internet, foi criada a Lei Geral de Proteção de Dados Pessoais, que em 14 de agosto de 2020 substituirá definitivamente o Marco Civil da Internet.

A experiência proveniente da vigência do Marco Civil da Internet no contexto jurídico brasileiro é de que sempre será necessária a atualização, tanto legal quanto jurisprudencial, com o escopo de efetivar adequadamente a garantia de direitos fundamentais dos agentes das relações jurídicas virtualizadas.

4.2. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: SURGIMENTO E INOVAÇÕES NO ORDENAMENTO JURÍDICO BRASILEIRO

A Lei Geral de Proteção de Dados Pessoais surge no Brasil no contexto da globalização do acesso à Internet, além de aspectos importantes como a crescente modernização dos meios de comunicação, além dos avanços sociais de integração dos indivíduos ao aspecto tecnológico atual. Essa Lei surge em sucessão ao Marco Civil da Internet, que ainda se encontra em vigência, mas perderá seu caráter normativo diante da entrada em vigor da LGPD em 2020.

A legislação brasileira teve como fundamento legal a *General Data Protection Regulation*, que por sua vez aparece em substituição à Diretiva 95/46/CE[31]. Essa lei é um conjunto de regras que tem como escopo a proteção de dados pessoais dos cidadãos pertencentes à União Europeia incluindo o fluxo de dados existente nos países membros e nos países que possuem contato com o mercado europeu, abarcando a ampliação de direitos dos

[31] **DIRETIVA 94/46/CE do Parlamento Europeu**. Acesso em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046

usuários o que implica em uma maior responsabilização das entidades que realizam o processamento de dados.

O processo de criação do texto legal da LGPD aconteceu vagarosamente, com debates propostos pelo Ministério da Justiça, buscando a participação popular na opinião do anteprojeto da LGPD com a divisão em eixos de discussão que iam desde os princípios reguladores à disposições transitórias, até a criação de três Projetos de Leis (4.060/2012, 330/2013 e 5.276/2016) essenciais para o Projeto de Lei 53/2018, que foi posteriormente aprovado pelo Congresso Nacional.

A Lei Geral de Proteção de Dados foi sancionada em 14 de agosto 2018, com a escolha legislativa de possuir uma *vacatio legis* com a duração de dois anos, o que implicou na entrada em vigor apenas a partir do ano de 2020. Isso acontece para que as empresas que realizam tratamentos de dados gozem do tempo necessário para se adequarem a nova legislação, em razão dos critérios rigorosos impostos pela lei, bem como para ciência geral ao novo limite regulatório.

Sua aplicação produzirá impactos nos negócios das empresas brasileiras, como também em todas as empresas nacionais ou estrangeiras que se valem da oferta produtos, serviços e outros para o mercado brasileiro, ou que tratem do monitoramento de comportamento dados de usuários localizados no Brasil, não importando sua nacionalidade ou residência.

Em síntese, a LGPD surge com o intuito de articular o interesse das empresas que realizam tratamento, coleta e armazenamento de dados, bem como dos titulares dos dados, sem prejudicar de qualquer forma os avanços tecnológicos, já que sua finalidade é conferir aos cidadãos segurança jurídica sobre a tutela de seus dados pessoais compatibilizando com os interesses das instituições privadas.

Em seus primeiros artigos a LGPD dispõe sobre o tratamento de dados pessoais, inclusive no âmbito digital, objetivando assegurar, tanto para as pessoas naturais como para as

jurídicas de direito público ou privado, a proteção dos direitos fundamentais à privacidade e liberdade, assim como o livre desenvolvimento da personalidade da pessoa natural.[32]

Por tratamento de dados, a lei dispõe que

> Art. 5º, X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Os fundamentos da LGPD presentes no art. 2º lastreiam-se no respeito à privacidade, na autodeterminação informativa, na liberdade de expressão, de informação, de comunicação e de opinião, na inviolabilidade da intimidade, da honra e da imagem, no desenvolvimento econômico e tecnológico e a inovação, na livre iniciativa, a livre concorrência e a defesa do consumidor, e por fim nos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.[33] Muitos desses fundamentos já estavam presentes no Marco Civil da Internet, como o respeito à privacidade e à liberdade de expressão, o que ratifica a indispensabilidade de tais direitos.

A LGPD tem como princípios basilares em seu art. 6º a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Há também a determinação da jurisdição em que o marco regulatório será aplicado, sustentando que a lei será aplica da operações de tratamento de dados, realizadas no território nacional, bem como se a atividades 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 os dados pessoais objeto do tratamento tenham sido coletados no território nacional, de forma que a LGPD considera os dados coletados no território nacional aqueles em que seu titular se encontre no momento da coleta.[34]

A LGPD ainda trata de vários aspectos importantes que não foram abordados no Marco Civil, como a distinção entre dados sensíveis, pessoais e anonimizados, a criação de

---

[32] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
[33] Idem.
[34] Idem.

uma Agência Reguladora de Dados Pessoais, além do *upgrade* em relação às questões de responsabilização no tratamento de dados, que serão explicados a seguir.

4.2.1. Dados sensíveis, anonimizados e pessoais

A lei considera como dado pessoal toda informação relacionada a pessoa natural identificada ou identificável. Este conceito de pessoa identificada ou identificável se alinha com o conceito bastante utilizado na segurança da informação, o *Personality Identifiable Information (PII*), que tem como objeto qualquer informação referente a uma pessoa identificada ou que pode ser identificada, a partir de documentos pessoais, como carteira de identidade, dados biométricos, cartões de crédito, em suma todo documento capaz de fornecer identificação (ERHARDT; PEIXOTO, 2019).

Por dado pessoal sensível, tem-se que é todo

> 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.

Ou seja, todo dado que se relacionar com o tipo de comportamento que o indivíduo possui perante a sociedade, aspectos que definem relacionamentos interpessoais, como filiações políticas, saúde, sexualidade e biometria. O tratamento dos dados pessoais sensíveis deverá acontecer mediante o consentimento do titular, de forma específica e detalhada e com uma finalidade específica. Excetua-se o consentimento expresso do titular nos casos de, *in verbis*

> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

A LGPD também elucida as questões referentes ao tratamento de dados pessoais de crianças e adolescentes, priorizando o melhor interesse e condicionando esse tratamento ao consentimento expresso dos pais ou responsáveis, o consentimento não será exigido quando a coleta for necessária para estabelecer contato com os pais ou o responsável legal, sendo utilizados apenas uma vez e sem armazenamento, podendo ser utilizados também para proteção, não podendo ser repassados a terceiros sem o consentimento expresso.

Já no que diz respeito aos dados anonimizados, a lei preleciona que são todos os dados relativos a titular que não possa ser identificado, de forma a considerar a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento, e por anonimização tem-se a 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.

O dado anonimizado passa por diversas etapas que realizam a desvinculação deste ao seu titular originário, modificando o conjunto de dados para remover ou encriptar a *Personal Identifiable Information (PII)*, de forma a proteger a privacidade dos titulares dos dados quando reduz a possibilidade de *"linkar"* o dado ao seu titular (BRASCHER, 2018). Em razão disso, a LGPD não se estenderá aos dados anonimizados justamente por não ser possível a identificação de seu titular, entretanto sua tutela acontecerá caso haja o desmembramento digital gerando a identificação do titular original, não possuindo mais a alcunha de dado anonimizado, mas sim pseudoanonimizado.

A anonimização baseia-se no modelo de *release-and-forget* (lança e esquece), que segundo Paul Ohm (2010) acontece quando o administrador de dados "libera registros publicamente, em particular para terceiros, ou internamente dentro de sua própria organização, e então esquece", não há a tentativa posterior de rastrear os dados após o lançamento, e antes de colocar o dado em risco, existe uma prévia modificação.

Existem diversos tipos de técnicas de anonimização, como a supressão, generalização, agregação, randomização com adição de ruídos e substituição, conforme o exposto

a) Supressão: esse método de anonimização envolve modificação de campos de informações (OHM, 2010), esse é o tipo de anonimização que permite uma maior proteção ao titular dos dados, tendo em vista que reduz consideravelmente a utilidade dos dados anonimizados (BRASHER, 2018);

b) Generalização: esse método se baseia na modificação de valores do identificador que estão a mostra, como modificação do ID de localização de um país, por exemplo;
c) Randomização[35]:esse tipo de anonimização consiste em modificar os valores reais, e com isso cria óbices que impedem a vinculação entre os dados anonimizados e os valores originais. Essa técnica se utiliza de inúmeras metodologias, que vão desde injeção de ruído até troca de dados (permutação), insta salientar que a remoção de um atributo equivale a uma forma extrema de randomização deste atributo, com a cobertura completa do atributo por ruídos.

Esse modelo gera grandes benefícios ao desenvolvimento da inteligência artificial, análise comportamental, da tecnologia em geral, por permitir o aperfeiçoamento nos aspectos da segurança e organização, tanto de entes públicos quanto de entes privados.

Contudo, um dado anonimizado pode passar pelo processo de desanonimização, o que implica em uma reidentificação do dado a partir da ligação do registro de dados anonimizados a informações auxiliares, com uma tecnologia conhecida como *linkage attack* (ataque de ligação) (*apud* RUBISNTEIN & HARTZOG). Em função da possibilidade de reidentificação do titular, a LGPD fornece guarida a esse tipo de dados justamente por estar diretamente ligado ao direito à privacidade do titular de dados.

A legislação brasileira, nesse ponto em especial, difere da sua inspiração a Regulação Geral de Proteção de Dados da União Europeia, esta não prevê a proteção para dados que foram anonimizados. Segue o que aponta o *Article 29 Working Party* em sua *Opinion 05/2014*[36], que traz disciplinas importantes no que se entende por dado anonimizado, além de prever questões como o risco de reidentificação de dados genéticos de domínio público, bem como os metadados sobre doadores potencialmente anônimos de DNA.

4.2.2. Responsabilização Civil e Sanções Administrativas

---

[35]Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[36] Ibidem.

No que concerne à responsabilização pelo tratamento de dados, a LGPD em seu art. 42 prevê que o operador/controlador que causar danos a outrem, sejam danos patrimoniais, morais, individuais/coletivos é obrigado a repará-lo.

Por controlador, conceitua a lei que é "pessoa natural ou jurídica, de direito público ou privado, a quem competem às decisões referentes ao tratamento de dados pessoais". Já o operador é toda" pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

Necessária diferenciação para o entendimento do §1º, que visa assegurar a efetiva indenização quando o operador descumprir a lei de proteção de dados, bem como não tiver seguido as instruções determinadas licitamente pelo controlador, sendo dessa forma equiparado ao controlador, respondendo solidariamente pelo tratamento de dados. No caso do controlador, ele responderá solidariamente quando estiverem envolvidos diretamente no tratamento dos dados que implicaram em danos ao titular.

A LGPD determina no art. 43 que o ônus da prova é incumbido aos agentes de tratamento, de forma que devem provar para que não seja configurada a responsabilização

> 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.

Nesse sentido, o tratamento irregular de dados acontecerá quando a legislação não for observada ou quando não houver a devida segurança para seu titular, devendo ser consideradas como circunstâncias relevantes: o modo que o tratamento é realizado, os resultados e riscos esperados e as técnicas de tratamento utilizadas à época do tratamento. De modo que haverá a responsabilização do controlador/operador que não observar as medidas necessárias de segurança e sigilo, como determina o art. 46

> 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.

No que se refere às sanções administrativas, os agentes de tratamento de dados são submetidos à advertências, multas, publicização de infrações, além do bloqueio e eliminação a que se refere a infração, devendo ser oportunizada a ampla defesa para o agente de tratamento de acordo com as especificidades do caso concreto, considerando a gravidade e a natureza da

infração e dos direitos atacados, a boa-fé do infrator, o tipo de vantagem que o autor auferiu diante de sua conduta, a reincidência, o grau do dano, a cooperação do infrator, as tentativas de minimização do dano, a adoção de boas práticas e governança, bem como a adoção de medidas corretivas e a proporcionalidade entre a falta cometida e a sanção aplicada.

Uma inovação importante é a da possibilidade de conciliação direta entre o controlador dos dados e o titular do direito nos casos de vazamentos de dados ou de acessos não autorizados, de acordo com a disposição do supracitado art. 46. Isso demonstra que o legislador se preocupou em minimizar as questões referentes à cultura do litígio presente na sociedade brasileira, trazendo a conciliação como forma extrajudicial e pacífica de resolução de conflitos.

No caso da responsabilização de órgãos públicos pelo tratamento de dados, essa acontecerá de acordo com as medidas cabíveis determinadas pela Autoridade Nacional, que também poderá solicitar a publicação de relatórios de impacto, além de sugerir adoção de padrões e boas práticas para o tratamento de dados pelo Poder Público.

4.2.3. Processo de criação da Autoridade Nacional de Proteção de Dados e suas atribuições

A promulgação da LGPD em 2018 foi realizada pelo então Presidente da República Michel Temer, com importantes vetos realizados. Um dos mais importantes foi o da criação da Autoridade Nacional de Proteção de Dados (ANPD), esta pode ser considerada um "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei em todo o território nacional". A justificativa utilizada no veto foi a que houve um vício de iniciativa, tendo em vista que sua criação cabia ao Poder Executivo[37], e não ao Poder Legislativo, como havia acontecido.

Diante disso, o governo, por intermédio da Medida Provisória nº 869 propôs a criação da Autoridade Nacional de Proteção de Dados, alterando o conteúdo normativo da Lei nº 13.709/18. A ANPD foi instituída como um órgão integrante da Presidência da República, sem a previsão de aumento de despesas, sendo composta por um Conselho Diretor, um

[37]Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, uma Corregedoria, uma Ouvidoria, um órgão próprio de assessoramento jurídico e demais unidades administrativas e finalísticas necessárias ao exercício de suas competências legais[38].

Critica-se no texto proposto pelo Governo Temer a escolha da ANPD ser um órgão subordinada a Presidência da República, não possuindo autonomia financeira. Outro ponto a ser discutido é o caráter transitório que essa Autoridade possui, tendo em vista que o Poder Executivo pode, no prazo de 2 (dois) anos, avaliar a possibilidade de alteração da natureza jurídica da ANPD, transformando-a em Autarquia de forma a garantir autonomia técnica e decisória.

Em 8 de julho de 2019 a Lei nº 13.853 foi sancionada, que introduz as mudanças já citadas na Lei Geral de Proteção de Dados. O art. 55-A cria a ANPD, sem o eventual aumento de despesa e com sua vinculação à Presidência da República, seguindo o disposto na MP nº 869. Segundo o art. 55-B é garantida à ANPD autonomia técnica e decisória, entretanto isso causa uma celeuma, tendo em vista que há uma subordinação da ANPD face à Presidência da República o que na prática não configura a verdadeira autonomia dessa Autoridade.

Isso demonstra que será necessária uma devida adaptação dos usuários, dos agentes de tratamento de entidades públicas e privadas, e principalmente do Poder Judiciário, já que este será o responsável na resolução dos conflitos resultantes das relações jurídicas tuteladas pela LGPD, devendo prestar a devida importância às contradições que a própria lei elenca em seu texto.

[38] Disponível em: Sumário Executivo da Medida Provisória nº 869.

CONCLUSÃO

A monografia em apreço objetivou, primordialmente, o estudo do conteúdo jurídico da privacidade e sua contextualização na virtualização das relações jurídicas, com o escopo de estabelecer quais os aspectos mais relevantes desse direito, bem como os efeitos decorrentes de seu exercício, além da análise da legislação brasileira de dados, quer esta seja a Lei Geral de Proteção de Dados Pessoais, assim como da Regulação Geral de Proteção de Dados proveniente da União Europeia, já que a primeira veio na mesma direção da vanguarda europeia.

Primitivamente, o direito à privacidade surge diante da necessidade de separar o aspecto público do privado, como forma de garantir ao sujeito de direito que seu âmago não sofreria intromissões alheias. A análise do desdobramento histórico desse direito perpassa por diversos períodos, que vão desde a antiguidade até o contexto atual da pós-modernidade, em que a maior inquietação reside na fluidez das relações que viabilizam seu vilipendio.

O avanço tecnológico e social incessante permite a criação de novos tipos de relações jurídicas pautadas na efemeridade das redes digitais. O tipo de comunicação entre os agentes, os modos de consumo, de laser e até de relacionamentos sofreram modificações drásticas, muitas ainda em curso. Mecanismos criados como forma de vigiar todos os passos tomados pelos indivíduos com o modelo de panóptico moderno, ou ainda o desenvolvimento de algoritmos manipuladores de opiniões políticas ou que influenciam no consumo, tudo isso desemboca no conceito de pós-modernidade, com suas relações líquidas, superexposição e a necessidade de integração social no âmbito digital.

Em face disso, os novos contornos do direito à privacidade invocam atitudes ativas do operador do Direito, com o fito de estabelecer parâmetros reguladores das relações do trato social pós-moderno.

Utilizando-se da doutrina e jurisprudência pátria, conclui-se que o Brasil, malgrado a existência dos regulamentos legais existentes, ainda necessita percorrer uma longa jornada para adequar-se ao presente contexto da sociedade da informação, e assim, promover a devida proteção ao direito à privacidade.

A nova Lei Geral de Proteção de Dados Pessoais, surge como instrumento para dirimir questões de direito que não foram abarcadas pelo Marco Civil da Internet, que esteve em vigor por mais de 5 (cinco) anos como legislação base na proteção dos dados dos usuários da rede mundial de computadores, entretanto, verifica-se que seu texto é insuficiente na proteção extensiva do direito do titular dos dados e pouco rígido na responsabilização do responsável pelo tratamento desses dados.

Partindo do exemplo estrangeiro de legislação referente á proteção de dados pessoais, bem como o direito à privacidade, em especial o Regulamento Geral de Proteção de Dados da União Europeia, percebe-se que há um refinamento da lei, com sua devida aplicação, inclusive com a previsão de sanções pertinentes ao caso concreto. A Europa segue na vanguarda na proteção de direitos fundamentais de natureza digital, todavia esse aperfeiçoamento se justifica em razão de um longo percurso realizado, que vai desde a Convenção de Estrasburgo, perpassando pela Diretiva 96/45/CE até o Regulamento Geral de Dados.

Verifica-se o esforço legislativo realizado surge da constante deturpação dos dados pessoais, como ocorreu no escândalo do vazamento de dados em larga escala, como forma de manipulação política, pela empresa *Cambridge Analytica*.

Já no que se refere ao contexto brasileiro, a LGPD está passando pelo período de adaptação das empresas e dos titulares de dados, que será encerrado em agosto do ano de 2020. A partir da entrada em vigor do novo marco regulatório será possível contemplar seus efeitos no caso concreto, com foco principal na aplicação na jurisprudencial. Presume-se que diante da edição da LGPD, o tratamento de dados será realizado com cautela e responsabilidade e o direito à privacidade do usuário poderá ser efetivamente resguardado, sob pena de responsabilização

Contudo, como a experiência demonstra, o dever-ser normativo nem sempre produz a eficácia social dele esperada e grandes são os desafios dos operadores e estudiosos do direito para acompanhar e efetivar o mandamento legal.

REFERÊNCIAS BIBLIOGRÁFICAS

Artigos:

ACIOLI, Bruno de Lima; EHRHARDT JÚNIOR, Marcos. Notas sobre o direito à privacidade e o direito ao esquecimento no ordenamento jurídico brasileiro. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabíola Albuquerque (Coord.). Privacidade e sua compreensão no direito brasileiro. Belo Horizonte: Fórum, 2019, p. 127-158.

ARAUJO, Luiz Ernani Bonesso; CAVALHEIRO, Larissa Nunes. **A proteção de dados pessoais na sociedade informacional brasileira: o direito fundamental a privacidade entre a autorregulação das empresas e a regulação protetiva do internauta.** *In:* Revista do Direito Público. Londrina, v.9, n.1, p.209-226, jan./abr.2014. DOI: 10.5433/1980-511X.2014v9n1p209.

AGRAWAL, Shashank; VIEIRA, Dario. ***A survey on Internet of Things***. *In:* Abakós. Belo Horizonte, v. 1, n. 2, p. 78 – 95, maio 2013 – ISSN:2316–9451.

BRANDEIS, Louis D.; WARREN, Samuel D. ***The rigtht to privacy***. Disponível em: www.lawrence.edu/fast/boardmaw/privacy_brand_warr2.html. Acesso em: 08/08/2019.

BRASHER, Elizabeth A. ***Addressing the failure of anonymization: guidance from the European Union's General Data Protection Regulation***. *In: Columbia Bussiness Law Review.* Vol. 2018. No. 1:209. Disponível em: https://academiccommons.columbia.edu/doi/10.7916/d8-zgve-y962. Acesso em: 13/01/2020.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. **Violação dos direitos de personalidade no meio ambiente digital: a influência da jurisprudência europeia na fixação da jurisdição/competência dos tribunais brasileiros**. *In:* Civilistica.com. Rio de Janeiro, a. 8, n. 1, 2019. Disponível em: http://civilistica.com/violacao-dos-direitos-de-personalidade/

CASTETS-RENARD, Céline; VOSS, W. Gregory. ***Proposal for an international taxonomy on the various forms of "right to be forgotten" a study on the convergence of norms.*** *In: Colorado Technology Law Journal.* Vol. 14.2. Disponível em: https://ctlj.colorado.edu/wp-content/uploads/2016/06/v.3-final-Voss-and-Renard-5.24.16.pdf.

DONEDA, Danilo. A **proteção dos dados pessoais como um direito fundamental**. *In*: Espaço Jurídico. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em: 12/01/2020.

EHRHARDT JÚNIOR, Marcos; NUNES, Danyelle Rodrigues de Melo; PORTO, Uly de Carvalho Rocha. **Direito ao esquecimento segundo o STJ e sua incompatibilidade com o sistema constitucional brasileiro**. *In:*Revista de Informação Legislativa: RIL, v. 54, n. 213, p. 63-80, jan./mar. 2017. Disponível em: <http://www12.senado.leg.br/ril/edicoes/54/213/ril_v54_n213_p63>. Acesso em: 10/11/2019.

HEYLLIARD, Charlotte. ***Le droit à l'oubli sur Internet***. Disponível em: https://www.lepetitjuriste.fr/wp-content/uploads/2013/01/MEMOIRE-Charlotte-Heylliard2.pdf. Acesso em: 07 de outubro de 2019.

JOVANELLE, Valquíria de Jesus. **Aspectos Jurídicos dos Contratos Eletrônicos**. Tese (Mestrado em Direito) – Faculdade de Direito, Universidade de São Paulo. São Paulo, 2012.

LIMA, Caio César Carvalho. **Objeto, aplicação material e aplicação territorial**. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). **Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia**. São Paulo: Thompson Reuters Brasil, 2018, p. 23-36.

LÔBO, Paulo. **O direito à privacidade e sua autolimitação**. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabíola Albuquerque (Coord.). **Privacidade e sua compreensão no direito brasileiro**. Belo Horizonte: Fórum, 2019, p. 15-31.

NASCIMENTO, Valéria Ribas do. **Direitos fundamentais da personalidade na era da sociedade da informação: transversalidade da tutela à privacidade**. *In:* Revista de Informação Legislativa: RIL, v. 54, n. 213, p. 265-288, jan./mar. 2017. Disponível em: <http://www12.senado.leg.br/ril/edicoes/54/213/ril_v54_n213_p265>.

PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. **Breves notas sobre a ressignificação da privacidade**. *In:* Revista Brasileira de Direito Civil - RBDCilvil, Belo Horizonte, v. 16, p. 35-56, abr./jun. 2018.

OHM, Paul. ***Broken promisses of privacy: responding to the surprising failure of anonymization***. *In: UCLA Law Review*, 2010. 57 UCLA L. Rev. 1701. Disponível em: https://www.uclalawreview.org/pdf/57-6-3.pdf. Acesso em: 14/01/2020.

PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos**. Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias**. *In:* EHRHARDT JÚNIOR, Marcos; LOBO, Fabíola Albuquerque (Coord.). **Privacidade e sua compreensão no direito brasileiro.** Belo Horizonte: Fórum, 2019, p. 33-53.

PINCHARD, Mathilde. ***La communication de crise à l'ère des médias sociaux et d'Internet. Le cas particulier du scandale Facebook-Cambridge Analytica de 2018***. Tese de Doutorado. Disponível em: https://matheo.uliege.be/bitstream/2268.2/6689/4/La%20communication%20de%20crise%20%c3%a0%20l%27%c3%a8re%20des%20m%c3%a9dias%20sociaux%20et%20d%27Internet.%20Le%20cas%20particulier%20du%20scandale%20Facebook-Cambridge%20Analytica.pdf

STRAUSS, David A. ***Do We Have a Living Constitution?*** *In:Drake Law Review*. Disponível em: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=3009&context=journal_articles. Acesso em: 01/10/2019.

Livros:

BALKIN, Jack M. ***Living Originalism***. *Massachusetts: Library of Congress Cataloging-in-Publication Data,* 2011.

BAUMAN, Zygmount. **Modernidade Líquida**. Rio de Janeiro: Zahar, 2001.

_____; LYON, David. **Vigilância Líquida:** diálogos com David Lyon. Rio de Janeiro: Zahar, 2014.

CASTELLS, Manuel. **A sociedade em rede. Volume 1.**6ª ed. São Paulo: Paz e Terra, 1999.

_____. A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**.Vol.3. São Paulo: Saraiva, 2014.

HAN, Byung-chul. **Sociedade da Transparência**. Petropólis, Rio de Janeiro: Vozes, 2017.

LYON, David. ***Surveillance Society: monitoring everyday life****. Oxford: Marston Book Services Limited*, 2001.

MATIAS, Eduardo Felipe P. **A humanidade e suas fronteiras - Do Estado Soberano à Sociedade Global**. São Paulo: Paz e Terra, 2005.

MIRANDA, Leandro Alvarenga. **A proteção de Dados Pessoais e o Paradigma da Privacidade**. São Paulo: *All Print* Editora, 2018.

Legislação:

BRASIL, Lei nº. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. *In*: PLANALTO FEDERAL. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 24 de setembro 2019.

BRASIL. Constituição Federal da República Federativa do Brasil. *In*: PLANALTO FEDERAL. Disponível em :http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 de setembro 2019.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014.Marco Civil da Internet. *In*: PLANALTO FEDERAL. Disponível em**:** http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 24 de setembro de 2019.

BRASIL. DECRETO Nº 10.046, DE 9 DE OUTUBRO DE 2019.*In:* PLANALTO FEDERAL. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 10/11/2019.

BRASIL. DECRETO Nº 10.047, DE 9 DE OUTUBRO DE 2019. *In*: PLANALTO FEDERAL. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10047.htm. Acesso em 10/11/2019.

UNIÃO EUROPEIA. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016. *General Data Protection Regulation*. Disponível

em:https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Acesso em: 07/01/2020.

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Disponível em:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 06/01/2020.

Parecer:

SARMENTO, Daniel. **Liberdades Comunicativas e "Direito ao esquecimento" na ordem constitucional brasileira**. Parecer emitido em: 22 de janeiro de 2015. Disponível em: https://www.migalhas.com.br/arquivos/2015/2/art20150213-09.pdf. Acesso em: 15/09/2019.