A PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS NA PANDEMIA DE COVID-19

Maria Izabella Alves de França Coelho

Lisboa

2024

A PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS NA PANDEMIA DE COVID-19

Maria Izabella Alves de França Coelho

Nº de Aluna:61792

Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade de Lisboa, como exigência para aprovação no curso Mestrado Bolonha em Direito e Ciência Jurídica.
Orientador: Professor Doutor António Barreto Espadinha de Menezes Cordeiro.

Lisboa

2024

AGRADECIMENTOS

Aos meus pais, irmão, e namorado, que sempre me apoiaram de maneira incondicional.

À minha cara amiga Thais Lacorte, que foi a melhor parceira que eu poderia ter nesta incrível jornada.

Ao Prof. Dr. António Barreto Espadinha de Menezes Cordeiro, pela inspiração, sabedoria e gentileza, em nome de quem agradeço a todos os professores e servidores da Faculdade de Direito da Universidade de Lisboa.

Ao amigo Jarbas Júnior, que me ouviu, apoiou e compreendeu em todos os momentos da realização desse sonho, especialmente nos mais sombrios.

Por fim, a todos aqueles que contribuíram, direta ou indiretamente, para a realização desta dissertação, os meus mais sinceros agradecimentos.

RESUMO

As medidas extraordinárias adotadas durante a pandemia de COVID-19 para conter a propagação do vírus aumentaram a necessidade de explorar a interseção entre a proteção de dados pessoais e o direito à privacidade. Assim, analisar como as iniciativas de rastreamento de contatos, tecnologias de vigilância, e a coleta ampliada de dados de saúde impactam a privacidade dos indivíduos torna-se de suma importância. A partir disso, o objetivo do presente estudo é compreender as implicações legais, éticas e sociais dessas medidas, buscando um equilíbrio entre a proteção da saúde pública e o respeito aos direitos individuais. A metodologia aqui adotada baseia-se em pesquisa bibliográfica, examinando legislações nacionais e internacionais, estudos acadêmicos, e posicionamentos de órgãos regulatórios. Esse enfoque permitirá uma análise das leis de proteção de dados, princípios éticos, e os impactos percebidos sobre a privacidade em diferentes contextos. A justificativa para esta pesquisa reside na importância de entender como as medidas emergenciais adotadas durante a pandemia podem moldar futuras abordagens à proteção de dados e privacidade. O tema torna-se pertinente na medida em que a sociedade busca um equilíbrio delicado entre a necessidade de enfrentar emergências de saúde pública e a preservação dos direitos individuais.

Palavras – Chave: Covid-19. Privacidade. Proteção de Dados Pessoais.

ABSTRACT

The extraordinary measures taken during the COVID-19 pandemic to contain the spread of the virus have increased the need to explore the intersection between personal data protection and the right to privacy. Therefore, analyzing how contact tracing initiatives, surveillance technologies, and expanded health data collection impact individuals' privacy becomes of paramount importance. The objective of this study is to understand the legal, ethical, and social implications of these measures, seeking a balance between public health protection and respect for individual rights. The methodology adopted here is based on bibliographic research, examining national and international legislations, academic studies, and regulatory body positions. This approach will allow an analysis of data protection laws, ethical principles, and perceived impacts on privacy in different contexts. The justification for this research lies in the importance of understanding how the emergency measures adopted during the pandemic can shape future approaches to data protection and privacy. The topic becomes relevant as society seeks a delicate balance between the need to address public health emergencies and the preservation of individual rights.

Keywords: Covid-19. Privacy. Protection of Personal Data.

SUMÁRIO

INTRODUÇÃO

A pandemia de Covid-19, que irrompeu no cenário global especialmente entre os anos de 2020 e 2022, desencadeou uma série de desafios sem precedentes, não apenas em termos de saúde pública, mas também no que toca à gestão de dados pessoais e à preservação do direito à privacidade.

Em meio a esforços para conter a disseminação do vírus, governos e organizações implementaram medidas extraordinárias que, muitas vezes, envolveram a utilização intensiva de tecnologias de monitoramento, rastreamento de contatos, e coleta massiva de dados de saúde. Se, por um lado, essas ferramentas foram cruciais para mapear a propagação do vírus e implementar estratégias eficazes de saúde pública, por outro, levantaram sérias questões éticas e legais relacionadas à privacidade e proteção de dados pessoais. A balança entre o interesse coletivo na contenção da pandemia e a preservação dos direitos individuais tornou-se um desafio intricado.

A partir disso, o objetivo geral desta pesquisa é analisar a interseção entre a proteção de dados pessoais e o direito à privacidade no contexto da pandemia de Covid-19. Pretende-se compreender como as medidas adotadas para enfrentar a crise sanitária impactam esses direitos fundamentais, buscando identificar desafios, boas práticas e oportunidades para aprimorar a proteção dos dados em situações de emergência.

Para atingir tal objetivo, será realizada uma pesquisa bibliográfica abrangente, explorando fontes acadêmicas, legislações nacionais e internacionais, bem como documentos oficiais de organizações de saúde e regulatórias. A revisão de literatura será fundamental para entender as bases teóricas que permeiam a proteção de dados pessoais, o direito à privacidade e as dinâmicas específicas relacionadas à pandemia de Covid-19. Ademais, a análise crítica dessas fontes permitirá uma avaliação profunda das implicações éticas, legais e sociais das medidas adotadas.

A escolha desse tema se justifica pela urgência em compreender as implicações da pandemia de Covid-19 nas questões de proteção de dados e privacidade, considerando os impactos a longo prazo dessas medidas excepcionais. A pesquisa visa preencher lacunas de conhecimento, oferecendo

visões valiosas para formuladores de políticas, profissionais da área de saúde, acadêmicos e a sociedade em geral.

Em um momento em que a tecnologia desempenha um papel crucial no combate à pandemia, é fundamental examinar até que ponto as medidas adotadas estão em conformidade com os princípios éticos, legais e de proteção aos direitos individuais. Além disso, a pesquisa busca contribuir para a criação de diretrizes mais eficazes que possam ser aplicadas em emergências, protegendo simultaneamente a saúde pública e os direitos fundamentais dos cidadãos.

Por fim, a relevância deste estudo estende-se além do contexto imediato da pandemia, alimentando discussões sobre como sociedades contemporâneas equilibram as demandas por segurança e saúde com a necessidade vital de preservar a privacidade individual. Ao se compreender melhor essa dinâmica, pode-se construir alicerces mais robustos para enfrentar futuras crises, promovendo uma abordagem equilibrada e ética no tratamento de dados pessoais em cenários de exceção.

1. BREVES CONSIDERAÇÕES ACERCA DO DIREITO À PRIVACIDADE CONTEMPORÂNEO

A consolidação do direito à privacidade sempre esteve intrinsicamente ligada às potencialidades e implicações advindas do progresso de novas tecnologias. Desde o surgimento de suas primeiras concepções nos Estados Unidos, expressas como o "*right to be let alone*"[1], até as interpretações mais contemporâneas, que o concebem como o direito de controlar a circulação de informações pessoais tanto dentro quanto fora da esfera individual (o direito de não saber[2]), é possível observar uma constante busca na tutela da esfera privada do indivíduo e de sua personalidade diante das ameaças apresentadas pelos avanços tecnológicos.

A evolução desse direito no cenário doutrinário e jurisprudencial revela uma expansão contínua de sua abrangência, frequentemente associando-o a outros direitos, como o acesso à informação, o livre desenvolvimento da personalidade e a liberdade. Além disso, essa expansão torna-se evidente ao considerarmos que o desenvolvimento do direito à privacidade é o precursor do chamado direito à proteção de dados pessoais[3].

Em virtude de sua singular importância, o direito à privacidade foi oficialmente reconhecido como um direito fundamental. No âmbito internacional, a Declaração Universal dos Direitos Humanos (DUDH) de 1948, em seu artigo 12, expressa o seguinte:

> Ninguém será sujeito a interferências em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataques à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques[4].

---

[1] WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy.* Harvard Law Review, v. 4, n. 5, dec. 1890. Disponível em: http://www.jstor.org/stable/1321160. Acesso em: 20/11/2023

[2] RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. P.24.

[3] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2016. p.163

[4] ONU. *Declaração Universal dos Direitos Humanos*. Adotada e proclamada pela resolução 217 A (III) da Assembleia Geral das Nações Unidas em 10 de dezembro de 1948. Disponível em: http://unesdoc.unesco.org/images/0013/001394/139423por.pdf. Acesso em: 15 de dezembro de 2023.

Quando se trata de um direito fundamental, é imperativo considerar o contexto social, político e econômico em que ele está inserido. A negligência em relação à realidade factual de uma determinada organização social não apenas resulta no esvaziamento desse direito, mas também na inviabilidade de sua concretização. Portanto, conceber o direito à privacidade nos mesmos termos do século XIX implicaria ignorar várias de suas facetas e evitar enfrentar diversas problemáticas associadas, levando a uma proteção inadequada do mesmo[5].

Um exemplo emblemático é a evolução dos direitos da personalidade como resposta aos excessos ocorridos após as revoluções liberais. Isso evidencia a constante necessidade de atualização do direito. Em um contexto de opressão de minorias baseada no poder econômico e concentração dos meios de produção, a própria noção de autonomia foi reinterpretada, resultando nos chamados direitos da personalidade, que sobrepujaram a liberalidade individual[6]. Esse contexto justificou a superação da teoria liberal clássica, que restringia o alcance dos direitos fundamentais às relações públicas, passando a afetar as relações entre particulares.

Da mesma forma, as mudanças constitucionais têm ganhado espaço nos mais diversos ordenamentos jurídicos nacionais como meio de ajustar o direito existente à realidade jurídico-social. Assim, é essencial considerar as características e peculiaridades do contexto social ao inserir o direito à privacidade. Contudo, em uma era pós-moderna caracterizada por transformações rápidas e constantes, essa tarefa é desafiadora[7]. A explosão de conceitos na tentativa de representar uma sociedade marcada pelos avanços das tecnologias da informação

---

[5] RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.P.29.

[6] A Revolução Industrial fora marcada pela constante exploração do proletariado por parte daqueles que detinham o poder econômico – burguesia – evidenciando que não mais bastava coibir as ingerências do Estado frente ao particular para garantir a tão aclamada liberdade que motivara a derrubada dos regimes absolutistas. O monopólio dos meios de produção fazia com que as classes menos favorecidas se submetessem a condições de trabalho degradantes, bem como a jornadas de trabalho desumanas, a fim de garantir sua subsistência. Rompeu-se, então, com essa falsa noção de autonomia, a partir do reconhecimento de direitos que se sobrepunham à própria liberdade do indivíduo, vez que se tratavam de direitos inatos, inerentes à própria pessoa e, portanto, inalienáveis, intransmissíveis e irrenunciáveis. SCHREIBER, Anderson*. Direitos da personalidade.* 3. ed. São Paulo: Atlas, 2014.

[7] SARMENTO, Daniel; GOMES, Fábio Rodrigues. *A eficácia dos direitos fundamentais nas relações entre particulares: o caso das relações de trabalho*. Rev. TST, Brasília, v. 77, n. 4, p. 60-101, out./dez. 2011.

e comunicação evidencia a dificuldade de definir uma realidade caracterizada por mutabilidade constante[8].

É notável que os avanços tecnológicos têm vários efeitos na sociedade, influenciando sua organização de maneira significativa. Esse cenário exige uma adaptação da sociedade para resolver os problemas decorrentes das rupturas sociais, frequentemente indicando uma nova distribuição de poder. No caso específico do direito à privacidade, as inovações tecnológicas criam meios de interferência na esfera privada do indivíduo, exigindo respostas da sociedade e a reformulação desse direito[9].

O argumento frequente de que renunciar a certo grau de privacidade é necessário para aproveitar os benefícios da sociedade moderna é considerado desnecessário e equivocado. Garfinkel[10] compara essa situação ao discurso durante a crise ambiental das décadas de 1950 e 1960, onde se afirmava que o desenvolvimento econômico só era possível à custa da degradação ambiental. Essa ideia foi fragilizada com a construção do conceito de sustentabilidade. Portanto, o direito à privacidade não está condenado, mas sim necessita de uma reinterpretação na sociedade contemporânea[11].

Reconhecendo que a formulação inicial desse direito, o direito a ser deixado só, não é mais reivindicada com a mesma intensidade, é necessário considerar as possíveis consequências dos avanços tecnológicos em relação à privacidade[12]. Diversos pensadores, como Pérez Luño, Rodotà e Castells, oferecem perspectivas sobre essas mudanças, desde a mutação da intimidade para um direito

---

[8] Bauman refere-se a uma “Modernidade Líquida”; Castells, por sua vez, utiliza a denominações como “Sociedade em Rede” ou “Era da Informação”; Beck utiliza o termo “Sociedade de Risco”; Rodotà traz a figura da “Sociedade de Vigilância”. BAUMAN, Zygmunt. Vigilância líquida: diálogos com David Lyon. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013; CASTELLS, Manuel. A galáxia internet. Reflexões sobre internet, negócios e sociedade. Tradução Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004; BECK, Ulrich. World risk society. In: OLSEN, J. K. B.; PEDERSEN, S. A.; HENDRICKS, V. F. (Ed.). A companion to the philosophy of technology. Oxford: Blackwell Publishing Ltd, 2009. p. 495-499; RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

[9] CASTELLS, Manuel. *A galáxia internet. Reflexões sobre internet, negócios e sociedade*. Tradução Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004.

[10] GARFINKEL, Simson. *Database nation: the death of privacy in the 21st century*. Boston: O'Reilly Media, 2010.

[11] LIMBERGER, Têmis. *Mutações da privacidade e a proteção dos dados pessoais*. In: RUARO, Regina Linden; PIÑAR MAÑAS, José Luis; MOLINARO, Carlos Alberto (Org.). Privacidade e proteção de dados pessoais na sociedade digital. Porto Alegre: Fi, 2017.

[12] *Ibidem.*

patrimonial[13] até a reinvenção da privacidade através da constitucionalização da pessoa humana e da ressignificação da liberdade de expressão[14].

Portanto, este capítulo busca enfrentar as tendências tecnológicas nas TICs e nas tecnologias de vigilância, bem como suas implicações na construção do direito à privacidade dentro do atual paradigma sociopolítico-econômico, embora sem a pretensão de esgotar o assunto.

1.1 O *right to privacy*[15] enquanto um *right to be let alone*

Trabalhar com a primeira formulação jurídica[16] do direito à privacidade não apenas representa a construção histórica desse direito, mas também implica enfrentar uma de suas diversas facetas. As mudanças na formulação do direito à privacidade, como mecanismos de adaptação a novos desafios sociais, não resultam na superação das formulações anteriores, mesmo que a primeira delas remonte ao século XIX.

O que se observa, na realidade, é um fenômeno de expansão gradual do direito à privacidade, que passa a incorporar diversas facetas que podem se manifestar de maneira individual ou concomitante, dependendo do caso específico[17]. Diante disso, torna-se relevante contextualizar brevemente o cenário

---

[13] Em síntese, o direito à intimidade manter-se-ia como direito da personalidade – dotado dos atributos de inviolabilidade, irrenunciabilidade e inalienabilidade – somente em relação às crianças e aos adolescentes. Para os maiores, ele se deslocaria para a órbita patrimonial, podendo "[...] ser objeto de transações consentidas, de renúncias e cessões, em troca das correspondentes prestações econômicas". PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012, apud LIMBERGER, op. cit., p. 154.

[14] CASTELLS, Manuel. *A galáxia internet. Reflexões sobre internet, negócios e sociedade.* Tradução Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004.

[15] O termo em inglês *right to privacy* é utilizado frequentemente sem tradução no presente trabalho, vez que o *right to privacy* americano não corresponde exatamente ao direito à privacidade no ordenamento jurídico brasileiro ou português. Tal direito corresponde quase a um direito geral de personalidade abordando, não raras vezes, questões que transcendem a noção de direito à privacidade. Destarte, adota-se, em diversas oportunidades, o termo na língua original, a fim de se evitar possíveis inadequações.

[16] Ressalta-se que, enquanto construção cultural, pode-se identificar uma formulação de *privacy* na própria noção de liberdade trabalhada por filósofos como Aristóteles, Cícero e Thomas de Aquino, ou então em contratualistas como John Mill, Locke e Hobbes, bem como em raízes anglosaxônicas com a máxima man's house is his castle. Ou seja, a noção de privacidade já existia, o que tardou para ocorrer foi a recepção desta figura no ordenamento jurídico. MILLS, John L. *Privacy: the lost right*. New York: Oxford University, 2008.

[17] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2016.p.31.

que deu origem ao artigo "Right to Privacy" de Warren e Brandeis[18] para a Harvard Law Review, publicado em 15 de dezembro de 1890. Apesar de não ser o primeiro a abordar o assunto, esse artigo é considerado um marco "inicial" na construção doutrinária do direito à privacidade e permanece o mais influente e citado na área.

O final do século XIX é identificado como o ápice do liberalismo jurídico clássico e a "idade de ouro da privacidade". Não é surpreendente que a privacidade tenha surgido como um direito "tipicamente burguês", com conotações elitistas e individualistas, apoiado em uma visão patrimonialista característica da época[19]. Warren e Brandeis[20] buscaram abordar as circunstâncias e problemas de sua época, notadamente as implicações intrusivas das câmeras fotográficas na privacidade, expressando preocupação especial com a exposição abusiva pela imprensa.

Feitas essas considerações iniciais, é pertinente abordar o artigo em questão. Os autores partem do pressuposto de que mudanças políticas, econômicas e sociais demandam o reconhecimento de novos direitos para atender às necessidades da sociedade. Identificam uma alteração qualitativa do direito à vida, que passa a englobar não apenas o direito de "(sobre)viver", mas também o direito de desfrutar a vida. Reconhecem direitos além dos bens materiais e do corpo do indivíduo, protegendo aspectos como a natureza espiritual, sentimentos e intelecto[21].

Com base nessa premissa, os autores americanos desenvolvem o conceito de "direito a ser deixado só" como um instrumento para resguardar o indivíduo diante das invasões constantes à vida privada e doméstica perpetradas pelos jornais, intensificadas pelo avanço da fotografia. Embora ancorado em noções de "*property-privacy*", ou seja, na construção do direito à privacidade a partir do direito de propriedade, o artigo estabelece as bases para uma construção do direito à

---

[18] Do próprio artigo de Warren and Brendeis se depreende que a noção de um *the right to be let alone* já era empregada pelo juiz Cooley na obra Cooley on Torts. Ademais, eles mencionam que, na França, já se reconhecia um *right to privacy*. WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review, v. 4, n. 5, dec. 1890. Disponível em: http://www.jstor.org/stable/1321160. Acesso em: 20/11/2023

[19] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2016.p.32.

[20] WARREN, Samuel D.; BRANDEIS, Louis D. *op. cit*., p. 195.

[21] *Idem*, p.197.

privacidade que transcende essa noção, vinculando esse direito ao ser humano em si, reconhecendo o resguardo à privacidade e até o isolamento como essenciais ao ser humano[22].

Descartando uma analogia superficial entre a proteção contra difamação e a proteção à privacidade, os autores buscam nas leis de propriedade intelectual e artística fundamentos para o "*right to privacy*" geral. Defendem que o *common law* garante a cada indivíduo o direito de determinar, ordinariamente, e em que extensão, seus pensamentos, sentimentos e emoções podem ser compartilhados com terceiros[23].

Os autores argumentam que o sistema jurídico dos Estados Unidos garante ao cidadão o direito de decidir se deseja ou não divulgar aspectos de sua vida a terceiros, salvo em situações de depoimentos ou testemunhos em que a exposição dos fatos é obrigatória. Além disso, afirmam que é assegurado ao cidadão o direito de estabelecer os limites da publicidade dada às suas informações pessoais. Em resumo, eles introduzem o conceito de consentimento e discutem as bases para a formulação da autodeterminação informativa[24].

Além disso, o artigo, fundamentado em vários julgamentos e uma análise preliminar de direitos autorais, estabelece uma distinção entre esses direitos e a proteção inerente ao direito à privacidade, com base em dois critérios: valor econômico e objeto de tutela. Enquanto os direitos autorais protegem a forma da produção e seu valor econômico, artístico ou intelectual, a privacidade leva em consideração o conteúdo do que foi produzido. Por exemplo, sob a ótica dos direitos autorais, seria impossível proibir a descrição do conteúdo de uma carta, limitando-se a tutelar seu texto, enquanto a proteção da privacidade se daria em relação ao conteúdo, por meio do direito à privacidade[25].

Nesse contexto, a proteção contra publicações não autorizadas em determinados casos reflete um direito de ser deixado só, não fundamentado no princípio da propriedade privada, mas na inviolabilidade da personalidade. Warren e Brandeis argumentam a favor de proteção contra interferências da imprensa e

---

[22] WARREN, Samuel D.; BRANDEIS, Louis D. *op. cit*., p. 195.
[23] *Ibidem*.
[24] WARREN, Samuel D.; BRANDEIS, Louis D. *op. cit*., p.205.
[25] *Ibidem*, p.198.

outros agentes detentores de dispositivos de gravação e reprodução. Eles defendem um direito geral à privacidade para pensamentos, emoções e sensações, independentemente da forma como são expressos[26].

Além disso, os autores identificam valores como confiança e confidência nos julgamentos das cortes norte-americanas, destacando o reconhecimento judicial de que a moralidade pública, a justiça privada e o senso comum demandam o reconhecimento do direito à privacidade. No entanto, Warren e Brandeis[27] percebem que essas construções não são suficientes para tutelar a privacidade em casos de invasão por terceiros estranhos, rejeitando noções como confiança especial ou contrato como fundamentos para o direito à privacidade.

Por fim, os autores apresentam critérios, como consentimento e interesse público, para definir os limites do direito à privacidade. Concluindo, o artigo "*Right to Privacy*"[28] sugere que as mudanças sociais exigem o reconhecimento de novos direitos, destacando o direito à privacidade como um mecanismo de proteção contra intromissões na vida privada, influenciado significativamente pelo desenvolvimento de novas tecnologias.

1.2 Do *right to privacy* aos direitos de personalidade: privacidade como expressão da proteção à dignidade da pessoa humana

A partir das premissas estabelecidas por Warren e Brandeis[29], que fundamentaram o direito à privacidade como um direito defensável, a doutrina evoluiu para reconhecer e consagrar esse direito como fundamental e inerente à personalidade. No contexto jurídico brasileiro, os direitos à vida privada e à

[26] WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review, v. 4, n. 5, dec. 1890. P. 195. Disponível em: http://www.jstor.org/stable/1321160. Acesso em: 20/11/2023
[27] *Idem*, p.198
[28] *Idem*, p. 218.
[29] WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review, v. 4, n. 5, dec. 1890. Disponível em: http://www.jstor.org/stable/1321160. Acesso em: 20/11/2023

intimidade são explicitamente previstos no Código Civil de 2002, no artigo 21[30], e na Constituição Federal de 1988, no artigo 5º, inciso X[31].

Esse reconhecimento foi crucial para superar a conotação elitista associada ao direito à privacidade desde sua origem, principalmente nos tribunais, a partir da década de 1960. A transição de um estado liberal para um *welfare state* e o fortalecimento de movimentos sociais contribuíram para democratizar o direito à privacidade, conferindo-lhe a natureza de um direito fundamental. Paralelamente, os avanços tecnológicos, especialmente nas Tecnologias de Informação e Comunicação (TICs), destacaram a interligação do direito à privacidade com o livre desenvolvimento da personalidade, a liberdade e a autonomia[32].

George Orwell[33] antecipou as diversas possibilidades de vigilância oferecidas pelos avanços tecnológicos, como a figura do Grande Irmão, representando um Estado onipresente e onisciente. Esses mecanismos de vigilância, conforme Orwell descreveu, servem como ferramentas de repressão, evocando a estrutura do panóptico de Jeremy Bentham, que Michel Foucault explorou em "Vigiar e Punir." [34]

Foucault[35], ao abordar a disciplina, evidencia a redução do indivíduo a um produto manipulado e treinado constantemente. O panóptico, inicialmente concebido para prisões, torna-se uma alegoria da vigilância, com uma torre central exposta a todas as células, simbolizando a ameaça constante de vigilância que assegura o funcionamento automático do poder[36].

---

[30] Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.” BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União, seção 1, Brasília, DF, a. 139, n. 8, p. 1-74, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/CCivil_03/leis/2002/L10406.htm. Acesso em: 20/11/2023

[31] 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; [...].” Id. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 20/11/2023

[32] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2016.p.33.

[33] ORWELL, George. *1984.* Tradução Alexandre Hubner, Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

[34] FOUCAULT, Michel. *Vigiar e punir: nascimento da prisão*. 31. ed. Tradução Raquel Ramalhete. Petrópolis: Vozes, 2006.

[35] *Ibidem*.

[36] Outras obras consagradas também evidenciam essa íntima relação entre a informação (ou conhecimento) e o poder. Segundo a arte da guerra – Sun Tzu –, uma das premissas para vitória em uma batalha é não só conhecer o inimigo, mas a si mesmo. Maquiavel, em sua obra O Príncipe,

Além do contexto literário, o aumento do fluxo de informações, a acessibilidade e o aprimoramento dos mecanismos de coleta e tratamento de dados ampliaram significativamente as ameaças à privacidade. Câmeras fotográficas, filmadoras, câmeras de segurança, coleta intensificada de informações pelo Estado e a criação de bureaus de crédito são exemplos de ameaças que não discriminam com base no "status social", afetando uma parcela mais ampla da população. Essas mudanças reforçam a importância de equilibrar a necessidade de segurança e saúde pública com a preservação dos direitos individuais, especialmente o direito à privacidade[37].

O conceito do panóptico do século XVIII foi transplantado para a era digital, resultando no panóptico digital ou panóptico do século XXI. Este último difere do panóptico original de Bentham, pois dispensa a necessidade de confinamento central, tornando-se um tema frequente para aqueles que enfrentam uma sociedade sob constante vigilância[38].

Vive-se, portanto, em um mundo onde a distopia do Grande Irmão, concebida por Orwell[39] em 1984, é agora tecnicamente realizável. A ideia de vigilância constante ressurge, sendo articulada através da utilização de ferramentas e instrumentos de monitoramento de indivíduos e processamento de dados pessoais, os quais estão cada vez mais presentes tanto no setor público quanto no privado.

Neste contexto, torna-se evidente a importância do reconhecimento de um direito fundamental à privacidade e a inclusão desse direito no escopo dos direitos da personalidade. Esta prerrogativa tem se mostrado crucial para a efetiva proteção do indivíduo diante das crescentes ameaças à privacidade. Não se trata apenas de uma construção teórica e jurisprudencial, mas sim de um direito respaldado por

---

defende que é preciso saber de que espécie é determinado principado para saber qual a melhor forma de conquista-lo ou de mantê-lo sob seu domínio. Ou seja, ainda que com algumas variações essas obras identificam o conhecimento sobre o outro como premissa de subjugá-lo a sua vontade. TZU, Sun. A arte da guerra. Tradução Sueli Barros Cassal. Porto Alegre: L&PM, 2006; MAQUIAVEL, Nicolau. O príncipe. 4. ed. São Paulo: Edipro, 2015.

[37] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2016.p.26.

[38] Idem, p.40

[39] ORWELL, George. *1984*. Tradução Alexandre Hubner, Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

uma estrutura sistemática própria no ordenamento jurídico, com fundamentação constitucional, conforme será discutido adiante.

1.2.1 Direito fundamental à privacidade

Enfrentar todas as complexidades que cercam a categoria dos direitos fundamentais, especialmente quando aplicadas ao direito à privacidade, representa uma tarefa desafiadora, ultrapassando os limites do escopo desta dissertação. É importante salientar que não se busca esgotar a temática da eficácia e do conteúdo do direito fundamental à privacidade, mas sim abordar questões pontuais essenciais para o desenvolvimento deste estudo.

Inicialmente, destaca-se que a privacidade, enquanto direito fundamental de primeira dimensão, está em constante processo de expansão e fortalecimento[40]. Essa observação respalda a tese de que não se pode aceitar o *trade-off* entre privacidade e as conveniências da vida moderna como uma alternativa adequada, sem, no entanto, endossar uma releitura *luddita*[41] desse discurso[42].

No que diz respeito à oponibilidade desse direito fundamental, é identificável que o cidadão pode opor tal direito tanto em relação ao Estado (eficácia vertical) quanto em relação a outros particulares (eficácia horizontal[43]). Em outras palavras,

---

[40] É o que se extrai da crítica de Sarlet ao emprego do vocábulo “gerações” de direitos fundamentais, o qual “[...] conduz ao entendimento equivocado de que os direitos fundamentais se substituem ao longo do tempo, não se encontrando em permanente processo de expansão, cumulação e fortalecimento”. SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. Porto Alegre: Livraria do Advogado, 2015.p.500.

[41] O Ludismo foi um movimento do Século XIX que era contra a automação ou mecanização do trabalho durante a Revolução Industrial, em razão da substituição da mão de obra humana pela máquina. Tal conceito é utilizado hoje para representar aqueles que se opõe à industrialização ou às inovações tecnológicas, também podendo ser chamado de neoludismo. JIN, Julia. Luddism during the Industrial Revolution. In: WESTERN Civilization II guides. 24 abr. 2012. Disponível em: http://westerncivguides.umwblogs.org2012/04/24/luddism-during-the-industrial-revolution/. Acesso em: 20/11/2023

[42] GARFINKEL, Simson*. Database nation: the death of privacy in the 21st century*. Boston: O'Reilly Media, 2010.

[43] No que toca ao emprego da expressão eficácia horizontal, oportuno apontar a ressalva feita por Limberger no sentido de que, ainda que tal termo possa levar a uma falsa impressão de que se trabalha com sujeitos em situação de igualdade material, tal situação nem sempre é verdadeira, especialmente em se tratando de grandes empresas ou instituições financeiras e seus trabalhadores ou consumidores. Destarte, deve-se atentar que eficácia horizontal significa que se está tratando da aplicabilidade em termos de relações privadas e não necessariamente isonômicas. LIMBERGER, Têmis. O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

trata-se de um direito oponível erga omnes. A fundamentalidade atribuída à privacidade, na perspectiva constitucional brasileira, a posiciona como um verdadeiro parâmetro hermenêutico e um valor superior, ao lado dos demais direitos fundamentais, em toda a ordem constitucional e jurídica. Essa fundamentalidade denuncia o conteúdo essencial desse direito, centrando-se na dignidade da pessoa humana[44].

Assim, rompe-se com a visão elitista e patrimonialista do direito à privacidade, transformando-o em um meio de concretização da dignidade da pessoa humana, estendendo sua proteção a qualquer indivíduo, não apenas aos detentores de propriedades[45].

No contexto brasileiro, apesar da Constituição Federal atribuir a titularidade dos direitos fundamentais apenas aos "brasileiros e aos estrangeiros residentes no País", há um entendimento consolidado no sentido da observância do princípio da universalidade[46] na interpretação do direito constitucional pátrio. Portanto, é pacífico o entendimento de que todas as pessoas humanas são titulares de direitos fundamentais, incluindo o direito à privacidade.

Além disso, é relevante notar a disposição no §1º do art. 5º da Constituição Federal brasileira de 1988, que confere aplicabilidade imediata às "normas definidoras de direitos e garantias fundamentais". A partir dessa disposição, fortalece-se a tese de que essas normas constitucionais possuem eficácia jurídica plena, resultando em sua aplicabilidade imediata[47].

Quanto à previsão constitucional desse direito à privacidade, o art. 5º, inciso X, estabelece que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral

---

[44] SARLET, Ingo Wolfgang*. A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional*. 12. ed. Porto Alegre: Livraria do Advogado, 2015. P. 205.

[45] *Ibidem.*

[46] De acordo com o princípio da universalidade, todas as pessoas, pelo fato de serem pessoas são titulares de direitos e deveres fundamentais, [...].” SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional*. 12. ed. Porto Alegre: Livraria do Advogado, 2015. p. 217.

[47] [...] § 1º As normas definidoras dos direitos e garantias fundamentais têm aplicação imediata.” BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 20/11/2023

decorrente de sua violação"[48]. O constituinte opta pelo termo "vida privada" em vez de "privacidade" e trata a "intimidade" de forma autônoma. Apesar da identidade semântica entre os termos, a doutrina atual emprega predominantemente a expressão "privacidade"[49]. A diferenciação feita pelo legislador entre "vida privada" (privacidade) e "intimidade" não justifica o tratamento individualizado desses direitos, uma vez que a intimidade consiste em uma esfera da vida privada[50].

A construção em questão remonta à teoria alemã dos círculos concêntricos, também conhecida como teoria das esferas[51]. Embora tenha sido proposta em 1953, essa teoria permanece relevante e se origina de uma distinção inicial entre a esfera individual (Individualsphäre) e a esfera privada (Privatsphäre). Essa diferenciação visa separar a proteção da personalidade na vida pública, abrangendo o "eu social" - incluindo o direito à honra e à imagem - da proteção em um âmbito mais privado, o "eu privado", que inclui a proteção à vida privada e à intimidade[52].

Além dessa divisão, a esfera privada é subdividida em três círculos concêntricos ou esferas, cada uma menor e contida pela anterior. A primeira e mais ampla é a esfera privada (Privatsphäre), abrangendo todos os comportamentos e informações pessoais que não devem ser expostos publicamente. A esfera do meio, contida pela primeira, é a esfera da intimidade (Vertrauenssphäre; Vertraulichkeitssphäre ou Intimsphäre), relacionada à confiança, familiaridade e intimidade[53].

Assim, não apenas questões públicas estão excluídas, mas também aquelas que são compartilhadas apenas com pessoas mais próximas e com quem se tem um convívio mais intenso. Por fim, a esfera mais restrita - abrangida pelas demais - é a esfera do sigilo (Geheimsphäre), englobando apenas as questões que o

---

[48] BRASIL. *Constituição (1988). Constituição da República Federativa do Brasi*l. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 20/11/2023

[49] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2016.p. 77.

[50] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme, MITIDIERO, Daniel. *Curso de direito constitucional.* 6. ed. São Paulo: Saraiva, 2017

[51] RUARO, Regina Linden; PIÑAR MAÑAS, José Luis; MOLINARO, Carlos Alberto (Org.). *Privacidade e proteção de dados pessoais na sociedade digital.* Porto Alegre: Fi, 2017

[52] COSTA JR., Paulo José Da. *O direito de estar só: tutela penal da intimidade*. São Paulo: Revista dos Tribunais, 1970. P. 34.

[53] *Idem*, pp.31-32.

indivíduo não compartilha com mais ninguém ou apenas com os amigos e familiares mais próximos[54]. Vale ressaltar que essas esferas não são rígidas e variam conforme aspectos subjetivos, como cultura, realidade social e atividade do titular[55].

É crucial observar que essa teoria não é imune a críticas. Costa Jr. destaca que a divisão em três esferas é "excessiva" e que a distinção em apenas duas seria suficiente, alinhando-se melhor com o ordenamento jurídico brasileiro, que prevê apenas a proteção à vida privada e à intimidade, conforme o art. 5º, inciso X, da Constituição Federal de 1988. Da mesma forma, Sarlet, Marinoni e Mitidiero simplificam a teoria das esferas para apenas três distinções:

> [...] uma esfera íntima (que constitui o núcleo essencial e intangível do direito à intimidade e privacidade), uma esfera privada (que diz com aspectos não sigilosos ou restritos da vida familiar, profissional e comercial do indivíduo, sendo passível de uma ponderação em relação a outros bens jurídicos) e uma esfera social (em que se situam os direitos à imagem e à palavra, mas não mais à intimidade e à privacidade) [...].[56]

Doneda[57], ao abordar as distinções entre vida privada, intimidade e privacidade, argumenta que a teoria dos círculos concêntricos já foi superada, especialmente após a decisão do Tribunal Constitucional Alemão sobre a lei do censo de 1983. O autor enfatiza que trabalhar com essas diferenciações pode resultar em mais confusões do que em uma construção coerente, como observado em muitos textos jurídicos.

Assim, Doneda[58] prefere adotar o termo "privacidade", considerando-o específico o bastante para diferenciar sua esfera de proteção de outros direitos da personalidade, como imagem e honra. Ele destaca que essa escolha é clara o suficiente para especificar o conteúdo da privacidade, unificando os valores expressos pelos termos intimidade e vida privada.

---

[54] HENKEL. Der Strafschutz des Privatlebens gegen Indiskretion, in Verhandlugen des 42. Deutschen Juristentages (Düsseldorf, 1957), Band II, Teil D, Erste Abteilung, Tübingen, 1958, apud COSTA JR, *O direito de estar só: tutela penal da intimidade*. São Paulo: Revista dos Tribunais, 1970.

[55] COSTA JR., Paulo José Da. *Op. cit*., p. 32.

[56] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme, MITIDIERO, Daniel. *Curso de direito constitucional*. 6. ed. São Paulo: Saraiva, 2017. p.408.

[57] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2016, p. 79.

[58] *Ibidem*,p.80.

A teoria das esferas da privacidade, segundo Doneda[59], não especifica adequadamente o conteúdo da privacidade, uma vez que as esferas menores, intimidade e segredo, são englobadas pela esfera maior, a privacidade. No entanto, ele reconhece que essa distinção proposta pode ser um critério para determinar o valor de eventual indenização em casos de violação da privacidade. Além disso, a distinção pode servir para estabelecer diferentes níveis de proteção, sendo mais rígida para a intimidade e menos rigorosa para a privacidade em si. Nesse contexto, a lição de Sarlet, Marinoni e Mitidiero[60] destaca a importância de um critério "material e não formal" na determinação do âmbito de proteção do direito à privacidade.

No que se refere à dimensão subjetiva do direito à privacidade, destaca-se que ele opera inicialmente como um direito de defesa e, posteriormente, como um verdadeiro direito de autodeterminação, expressão da liberdade pessoal. No tratamento específico do direito à intimidade, Limberger[61] ressalta não apenas sua dimensão negativa, enquanto direito a não ser molestado, mas também sua dimensão positiva, que implica prestações concretas pelo Estado, como a objetividade dos dados, o direito ao esquecimento e a necessidade de prazo para armazenamento de informações negativas.

Finalmente, no que diz respeito às limitações do direito fundamental à privacidade, destaca-se a inexistência de uma reserva legal expressa, sendo assegurada a inviolabilidade desse direito[62]. Apesar de não ser absoluto, sua estrutura normativa constitucional exige que quaisquer restrições se restrinjam aos casos em que sejam necessárias para conciliar a privacidade com outros direitos fundamentais ou valores constitucionalmente assegurados, o que só pode ser avaliado diante de situações concretas.

---

[59] *Ibidem*, p.81.
[60] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme, MITIDIERO, Daniel. *Op. cit.,* p.407.
[61] LIMBERGER, Têmis*. O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais.* Porto Alegre: Livraria do Advogado, 2007.
[62] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme, MITIDIERO, Daniel. *Op. cit*., p.410.

1.2.2 Privacidade e personalidade

O direito à privacidade, considerado um direito de personalidade, compartilha todos os atributos característicos dessa categoria de direitos. Os direitos da personalidade são intrínsecos, personalíssimos, extrapatrimoniais e fundamentais. Em outras palavras, são direitos intransmissíveis, imprescritíveis, impenhoráveis, vitalícios e oponíveis erga omnes[63]. O Código Civil brasileiro de 2002 reforça essa natureza ao afirmar, em seu artigo 11, que, exceto nos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não permitindo qualquer restrição voluntária ao seu exercício[64].

Nesse sentido, a intransmissibilidade está ligada ao conceito de infungibilidade, pois transmitir tais direitos implicaria em substituir uma pessoa por outra, o que é incompatível com a natureza personalíssima desses direitos. Contudo, é importante ressaltar que a intransmissibilidade não se estende aos efeitos patrimoniais decorrentes desses direitos, os quais podem ser objeto de transmissão[65].

A irrenunciabilidade dos direitos da personalidade encontra sua justificativa na qualidade intrínseca desses direitos como inerentes à condição humana. Apesar da disputa doutrinária entre as correntes juspositivista e jusnaturalista, ambas concordam na definição dos direitos de personalidade como essenciais e inatos[66]. Segundo os juspositivistas, esses direitos não são impostos por uma ordem natural ou sobrenatural aos sistemas jurídicos, conforme defendido por Pontes de Miranda:

> [...] efeitos de fatos jurídicos, que se produziram nos sistemas jurídicos, quando, a certo grau de evolução, a pressão política fez os sistemas jurídicos darem entrada a suportes fáticos que antes ficavam de fora, na dimensão moral ou na dimensão religiosa.[67]

---

[63] BITTAR, Carlos Alberto. *Os direitos da personalidade*. 8. ed. São Paulo: Saraiva, 2015.p.62
[64] BRASIL. *Lei nº 10.406*, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União, seção 1, Brasília, DF, a. 139, n. 8, p. 1-74, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/CCivil_03/leis/2002/L10406.htm. Acesso em: 20/11/2023
[65] PONTES DE MIRANDA. *Tratado de direito privado*. Atualizado por Rosa Maria Barreto Borriello de Andrade Nery. São Paulo: Revista dos Tribunais, 2012
[66] BITTAR, Carlos Alberto. *Op. cit*., p.64.
[67] PONTES DE MIRANDA. *Tratado de direito privado*. Atualizado por Rosa Maria Barreto Borriello de Andrade Nery. São Paulo: Revista dos Tribunais, 2012. p.7.

Cupis[68] argumenta que a atribuição de direitos subjetivos à pessoa pela ordem jurídico-positiva é condição necessária para afirmar a inatidão de certos direitos subjetivos. Para o autor os direitos da personalidade são inatos devido à sua essencialidade e, como tal, não se enquadram na categoria de direitos derivados ou adquiridos[69]. Essa perspectiva é compartilhada por Bittar[70] em relação ao Juspositivismo, embora ele não adote integralmente essa corrente doutrinária.

Por outro lado, a Corrente Jusnaturalista, influenciada por correntes filosóficas existencialistas, sustenta que não há criação de direitos da personalidade pelo Estado. Esses direitos são considerados inatos e, portanto, anteriores à própria noção de Estado. Consequentemente, cabe ao Estado apenas o reconhecimento e a tutela desses direitos que precedem sua existência. Seguindo essa corrente, a tutela dos direitos da personalidade é vista como conferindo legitimidade ao Estado, não o contrário[71].

Independentemente da corrente doutrinária adotada, é imperativo reconhecer que a aceitação e consolidação dos direitos da personalidade representam uma mudança paradigmática no ordenamento jurídico, especialmente no âmbito do direito civil. A transição de um direito centrado na propriedade para um ordenamento estruturado em torno da (dignidade da) pessoa humana resultou no reconhecimento de direitos fundamentais essenciais para o livre desenvolvimento da personalidade de maneira autônoma e digna[72].

No que diz respeito à vedação de limitação voluntária, é crucial distinguir isso do exercício regular de um direito da personalidade. Conforme Bittar[73], o exercício dos direitos da personalidade pode sofrer limitação voluntária, desde que não seja permanente nem geral.

---

[68] CUPIS, Adriano de*. Os direitos da personalidade*. Tradução Afonso Celso Furtado. Campinas: Romana, 2004

[69] Os direitos derivados ou adquiridos pressupõem o preenchimento de certos requisitos, além da própria personalidade. Por outro lado, os direitos inatos seriam aqueles em que bastaria a personalidade para sua atribuição. BITTAR, Carlos Alberto*. Os direitos da personalidade*. 8. ed. São Paulo: Saraiva, 2015.

[70] BITTAR, Carlos Alberto. *Os direitos da personalidade.* 8. ed. São Paulo: Saraiva, 2015.p.68.

[71] SCHREIBER, Anderson*. Direitos da personalidade*. 3. ed. São Paulo: Atlas, 2014.

[72] DONEDA, Danilo. *Os direitos da personalidade no Código Civil*. Revista da Faculdade de Direito de Campos, Rio de Janeiro, a. VI, n. 6, p. 71-99, jun. 2015. P. 82. Disponível em: http://www.uniflu.edu.br/arquivos/Revistas/Revista06/Docente/03.pdf. Acesso em: 20/11/2023

[73] BITTAR, Carlos Alberto*. Os direitos da personalidade.* 8. ed. São Paulo: Saraiva, 2015.

Schreiber[74] argumenta que limitações voluntárias pontuais, como furar a orelha para colocar um brinco ou um piercing, participar de um reality show ou praticar uma luta, são lícitas. Ele estabelece critérios para verificar a legitimidade dessas limitações, incluindo alcance, duração, intensidade e finalidade96.

Delgado[75] concorda que o art. 11 do Código Civil não veda a "fruição econômica" dos direitos da personalidade, permitindo, por exemplo, a comercialização da própria imagem para fins comerciais ou até mesmo para pornografia, desde que não seja uma cessão duradoura ou indeterminada. Embora terminologias diversas tenham sido apresentadas, a noção de disponibilidade dos direitos, conforme trabalhada por Bittar[76], é preferida, pois não entra em conflito com o disposto no art. 11 do Código Civil brasileiro de 2002, que expressamente veda a limitação voluntária.

Além disso, argumenta-se que, dependendo das características e da natureza do direito em análise, situações que parecem, à primeira vista, ser uma renúncia ou limitação voluntária podem, na verdade, constituir o exercício regular do direito. De acordo com Bittar:

> [...] diante das necessidades decorrentes de sua própria condição, da posição do titular, do interesse negocial e da expansão tecnológica, certos direitos da personalidade acabaram ingressando na circulação jurídica, admitindo-se ora a sua disponibilidade, exatamente para permitir a melhor fruição por parte de seu titular, sem, no entanto, afetar-se os seus caracteres intrínsecos.[77]

Desse modo, a divulgação de um acontecimento não necessariamente implica em uma restrição voluntária à privacidade por parte do detentor do direito. Ao conceber o direito à privacidade não apenas como uma proteção contra intromissões de terceiros - sejam eles do Estado ou privados - em sua esfera pessoal, mas também como o controle de informações de natureza pessoal, a exposição inicial de um fato privado não deve automaticamente resultar na

---

[74] SCHREIBER, Anderson*. Direitos da personalidade*. 3. ed. São Paulo: Atlas, 2014.
[75] DELGADO, Mário Luiz. *Big Brother Brasil: reality shows e os direitos da personalidade*. Revista Jurídica Consulex, Brasília, a. VIII, n. 169, p. 24-26, jan. 2004. Disponível em: https://marioluizdelgado.files.wordpress.com/2014/04/mario-luiz-delgado-3.pdf. Acesso em: 20/11/2023
[76] BITTAR, Carlos Alberto. *Os direitos da personalidade*. 8. ed. São Paulo: Saraiva, 2015.p.13.
[77] *Ibidem, p.14.*

limitação desse direito, uma vez que está intrinsecamente ligada ao seu próprio exercício: o controle de informações[78].

Nesse contexto, os critérios estabelecidos por Schreiber[79] para avaliar a legitimidade de uma restrição voluntária específica são particularmente relevantes. Ao analisar o exemplo dos direitos autorais apresentado por Bittar[80], torna-se evidente o interesse do titular em aumentar a circulação de sua obra, inclusive por meio de compensação financeira, sendo essa disponibilidade crucial para a plena fruição desse direito.

No que diz respeito ao direito à privacidade em particular, a situação dos programas de televisão do gênero reality show também pode ser compreendida à luz dos critérios de Schreiber[81], especialmente no que diz respeito ao critério (II) da temporalidade. Em casos de exposição temporária, reconhece-se a possibilidade de um indivíduo participar de programas como o "Big Brother", pois essa situação, a princípio, não viola seu direito à privacidade.

Nesse contexto, é essencial observar que a disponibilidade proposta não é absoluta, devendo atender a critérios específicos para evitar conflitos com a proibição estabelecidas na legislação civil[82].

Outra questão controversa na construção da privacidade como um direito da personalidade é a extensão desses direitos às pessoas jurídicas. Considerando que tais direitos são inerentes ao ser humano e essenciais para o livre desenvolvimento de sua personalidade, alguns argumentam que são incompatíveis com entidades não humanas[83].

No entanto, há defensores da ideia de que o artigo 52, do Código Civil brasileiro de 2002, ao afirmar que "aplica-se às pessoas jurídicas, no que couber, a proteção dos direitos da personalidade", estendeu esses direitos às pessoas jurídicas. Embora essa seja uma questão além do escopo deste trabalho, vale

---

[78] VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. Porto Alegre: Sergio Antonio Fabris, 2007

[79] SCHREIBER, Anderson. *Direitos da personalidade*. 3. ed. São Paulo: Atlas, 2014.

[80] BITTAR, Carlos Alberto. *Os direitos da personalidade*. 8. ed. São Paulo: Saraiva, 2015.

[81] SCHREIBER, Anderson. *Direitos da personalidade*. 3. ed. São Paulo: Atlas, 2014.

[82] SCHREIBER, Anderson. *Direitos da personalidade*. 3. ed. São Paulo: Atlas, 2014.

[83] LOTUFO, Renan; NANNI, Giovanni Ettore; MARTINS, Fernando Rodrigues (Coord.). *Temas relevantes do direito civil contemporâneo: reflexões sobre os 10 anos do Código Civil*. São Paulo: Atlas, 2012.

mencionar que o Superior Tribunal de Justiça do Brasil emitiu uma Súmula[84] sobre o tema, reconhecendo a possibilidade de uma pessoa jurídica sofrer dano moral. Superadas essas questões, torna-se pertinente delinear o direito à privacidade no contexto jurídico e social atual.

1.3 Novos contornos do direito à privacidade

Trabalhar sob uma abordagem contemporânea do direito à privacidade não implica na exclusão de suas formulações anteriores. Essa perspectiva, conforme indicado por Mills[85], implica no reconhecimento das influências exercidas por diversos fatores, tais como família, religião, riqueza, estrutura política, história, clima, hábitos de trabalho, geografia, ideologia, urbanização, normas culturais e tecnologia, sobre a definição social e jurídica desse direito.

Nesse contexto, é fundamental salientar que se vive, atualmente, na denominada sociedade da informação ou era da informação, caracterizada pelo fenômeno da globalização, tendo na internet sua principal manifestação. A designação "sociedade da informação" sugere uma sociedade organizada em torno da informação, considerada essencial para o desenvolvimento de qualquer atividade. Contudo, é incontestável que a comunicação e a coleta de dados sempre foram fundamentais para toda interação social, não sendo, por si só, suficientes para justificar tal nomenclatura[86].

O diferencial dessa sociedade reside na forma como a informação é tratada e aplicada em seu cotidiano. As transformações notáveis, especialmente no campo das tecnologias da informação a partir do século XX, revolucionaram a capacidade de organização, armazenamento e transmissão de dados, causando impactos significativos em todos os setores da interação social[87].

O advento da era da informação teve início com os meios de comunicação em massa, como rádio, televisão e jornais impressos. O poder influente da

---

[84] BRASIL. Superior Tribunal de Justiça. Súmula n° 227. A pessoa jurídica pode sofrer dano moral. Diário de Justiça, seção 2, Brasília, DF, p. 126, 08 out. 1999.
[85] MILLS, John L. *Privacy: the lost right*. New York: Oxford University, 2008.
[86] LEMOS, André; LÉVY, Pierre. *O futuro da internet: em direção a uma ciberdemocracia planetária.* São Paulo: Paulus, 2010.
[87] DONEDA, Danilo. *A proteção dos dados pessoais como um direito fundamental*. Espaço Jurídico, Joaçaba, v. 12, n. 2. p. 91-108, jul./dez. 2011. p.95

imprensa e dos meios de comunicação, conhecido como o "quinto poder", gerou preocupações sobre a manutenção da lógica do pensamento único que esses meios proporcionavam[88].

A internet surgiu como uma promessa de romper com esse monopólio, apresentando-se como uma ferramenta capaz de democratizar a informação tanto para os receptores quanto para os comunicadores, desde que devidamente articulada. Desde suas origens na rede de computadores da ARPA na década de 1960, a interatividade sempre foi um objetivo da internet, mesmo que inicialmente tenha sido desenvolvida para fins militares[89].

Posteriormente, com a influência de uma cultura libertária no desenvolvimento da rede, a criação da world wide web (www) em 1990 permitiu que a internet alcançasse uma audiência global, abrindo espaço para uma participação social mais ampla em escala global. Assim, a internet, especialmente em sua forma participativa conhecida como web 2.0[90], desempenha um papel crucial no exercício da democracia, chegando a ser considerada uma ciberdemocracia. Além de possibilitar o uso de vários mecanismos de participação direta, ela também quebra o monopólio detido pelas mídias clássicas na divulgação de informações.

No contexto das Tecnologias da Informação e Comunicação (TICs), a Comissão Europeia, por meio da Estratégia Europeia 2020, conferiu à Agenda Digital um papel de destaque, com especial ênfase no Big Data[91]. O Comissário da

---

[88] CASTELLS, Manuel. *A galáxia internet. Reflexões sobre internet, negócios e sociedade.* Tradução Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004.

[89] *Ibidem,*

[90] A definição de web 2.0 decorre de uma classificação criada para diferenciar as diferentes fases do desenvolvimento da rede mundial de computadores: a internet. A web 1.0, seria a internet em sua versão inicial, consistente em sites de conteúdo estático com pouca ou nenhuma interatividade. A web 2.0, por sua vez, é marcada pelo surgimento dos blogs, chats, redes sociais e outras formas de mídia colaborativa, nas quais o conteúdo dos sites na internet é gerado pelos próprios usuários, por isso também e chamada de web participativa. A web 3.0, por fim, seria a inserção de mecanismos inteligentes na internet, não só a partir de mecanismos como smartphones, mas com o desenvolvimento de softwares capazes de filtrar o conteúdo da internet, geralmente com base na utilização do usuário. EX2. Web 1.0, Web 2.0 e Web 3.0... Enfim o que é Isso? 2013. Disponível em: http://www.ex2.com.br/blog/web-1-0-web-2-0-e-web-3-0-enfim-o-que-e-isso/. Acesso em: 20/11/2023

[91] Big Data é o nome dado a um grande volume de dados armazenados de forma ordenada, a fim de que a interpretação destes permita a previsão de tendências e auxilie nas tomadas de decisão de uma empresa, do Estado ou até mesmo de um indivíduo. SAS Institute. Big data: o que é e por que é importante? Disponível em: https://www.sas.com/pt_br/insights/big-data/what-is-bigdata.html#. Acesso em: 20/11/2023

União Europeia, Neelie Kroes[92], declarou que o "Big Data é o novo petróleo", salientando sua capacidade de ser gerenciado e utilizado de maneiras inéditas graças a ferramentas eletrônicas avançadas. Ele também destacou o Big Data como um "combustível da inovação", ressaltando sua utilidade no contexto econômico.

Essa empolgação é respaldada pela projeção de que, até 2020, o universo digital conterá 44 zettabytes, em comparação aos 4.4 zettabytes registrados em 2013, representando um aumento significativo na disponibilidade de dados, dos quais cerca de 16 zettabytes são considerados utilizáveis[93].

A crescente disponibilidade de dados e sua apropriação por meio de ferramentas de Big Data em diversos setores econômicos têm o potencial de aumentar a eficiência na gestão e aplicação de recursos, resultando em economias substanciais. No setor público, especificamente na administração, estima-se uma redução de custos na ordem de 15% a 20% no Continente Europeu, equivalente a aproximadamente 300 bilhões de euros. Na área da saúde, a utilização de sistemas informatizados que processam Big Data pode gerar uma economia de 90 milhões de euros[94].

Nos Estados Unidos, a estimativa é de uma economia superior a 300 bilhões de dólares até 2020. Além disso, nos setores de energia e transporte, o uso de Big Data pode aumentar a eficiência em logística, especialmente com a coleta de dados de programas de navegação como Waze ou Google Maps, prevendo-se uma economia global de 500 bilhões de dólares em tempo e combustível, além da redução de 380 megatoneladas de emissões de CO2[95].

---

[92] “EU Commissioner Kroes stated, ‘Big Data is the new Oil’ that can be managed, manipulated, and used like never before thanks to high-performance digital tools, making big data the fuel for innovation”, em razão da importância da utilização do Big Data no âmbito econômico. [Tradução livre]. CAVANILLAS, José María; CURRY, Edward; WAHLSTER, Wolfgang. The big data value opportunity. In: _____ (Org.). New horizons for a data-driven economy: a roadmap for usage and exploitation of big data in Europe. Cham (Suiça): Springer Open, 2016

[93] Dados disponíveis em SAS Institute. Big data: o que é e por que é importante? Disponível em: https://www.sas.com/pt_br/insights/big-data/what-is-big-data.html#. Acesso em: 20/11/2023

[94] CAVANILLAS, José María; CURRY, Edward; WAHLSTER, Wolfgang. The big data value opportunity. In: _____ (Org.). New horizons for a data-driven economy: a roadmap for usage and exploitation of big data in Europe. Cham (Suiça): Springer Open, 2016

[95] OECD. Exploring data-driven innovation as a new source of growth – mapping the policy issues raised by “Big Data.” Rep. from OECD, 2013. Disponível em: http://dx.doi.org/10.1787/5k47zw3fcp43-en. Acesso em: 20/11/2023

Entretanto, é imperativo abordar essas perspectivas otimistas com cautela, conforme alertado por especialistas, evitando cair no viés do otimismo excessivo. A internet, embora seja uma tecnologia da liberdade, também pode ser utilizada para oprimir os desinformados e excluir aqueles desvalorizados pelos detentores do poder. A ubiquidade da internet em nossas vidas, permeando o ambiente familiar, profissional e até mesmo tornando-se uma extensão de nossos corpos por meio de smartphones, tem despertado o interesse significativo de grandes centros econômicos e entidades políticas em sua infraestrutura e conteúdo[96].

Nesse contexto, a interação entre a internet e o Big Data é evidente, pois a internet serve como meio para a coleta de dados, incluindo informações pessoais, introduzindo novas questões no domínio da privacidade. Atualmente, a dimensão informacional representa a principal preocupação daqueles que trabalham com o direito à privacidade.

O constante sujeitamento do indivíduo à coleta de seus dados pessoais, seja ao realizar uma transação com cartão de crédito ou ao navegar na internet, resulta na perda de controle sobre suas informações e na ameaça à sua esfera privada. Essa preocupação é evidenciada nos conceitos contemporâneos de privacidade, como definido por Rodotà[97], que a caracteriza como o direito de manter o controle sobre as informações pessoais e determinar as modalidades de construção da esfera privada. Doneda[98] complementa, destacando que a privacidade não se limita à questão de isolamento, mas também está relacionada à liberdade, autonomia, não discriminação, igualdade e à própria personalidade, enfatizando a íntima ligação entre privacidade e livre arbítrio.

Vieira conceitua o direito à privacidade como um direito subjetivo que não apenas obriga outros a respeitarem a esfera privada da pessoa, mas também concede o controle sobre suas informações pessoais, resistindo a intromissões indevidas. Em todos esses autores, percebe-se que a construção da privacidade

---

[96] FREITAS, Juarez. *A hermenêutica jurídica e a ciência do cérebro: como lidar com os automatismos mentais*. Revista da AJURIS, Porto Alegre, v. 40, n. 130, p. 223-244, jun. 2013.
[97] RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.p.49.
[98] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2016, p.95

está intrinsicamente ligada ao controle das próprias informações, enfatizando a importância da autonomia.

Mills[99], por sua vez, aborda a privacidade de maneira um pouco diferente, reconhecendo-a como um conceito subjetivo, mas preferindo trabalhar com a ideia de "expectativa razoável de privacidade" no âmbito legal. Ele sugere que a variação dessa expectativa é fundamentada na sociedade, não no indivíduo em si. O exemplo dos sites de relacionamento, como o Facebook, ilustra essa abordagem, onde o usuário tem a capacidade de decidir o que expor e o que proteger.

Além disso, reitera-se que o direito à privacidade é fundamental, servindo como proteção contra o Estado e particulares. Vieira[100] propõe categorias para delinear o direito à privacidade, considerando diferentes dimensões e formulações que são abrangidas por uma dimensão objetiva desse direito. Categorias como privacidade física, do domicílio, das comunicações e decisional são apresentadas como elementos constituintes desse direito geral à privacidade, cada uma com sua própria esfera de proteção, como contra procedimentos invasivos não autorizados, inviolabilidade do domicílio e das comunicações, e o direito à autodeterminação[101].

Por fim, a proteção da privacidade informacional é centrada nas informações pessoais e íntimas dos indivíduos. Nesse contexto, é evidente que adotar uma definição rígida e permanente de privacidade seria um equívoco. O direito à privacidade abrange a noção de "right to be let alone", protegendo a pessoa contra interferências de terceiros em sua esfera privada, além de resguardá-la contra a coleta e transmissão não autorizadas de informações pessoais. No futuro, este direito será influenciado pelas inovações tecnológicas e suas potenciais ameaças à esfera privada dos indivíduos[102].

Outro aspecto de grande relevância é o direito à privacidade no contexto do livre desenvolvimento da personalidade e identidade. De acordo com Garfinkel[103],

---

[99] MILLS, John L. Privacy: the lost right. New York: Oxford University, 2008.
[100] VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. Porto Alegre: Sergio Antonio Fabris, 2007
[101] SARLET, Ingo Wolfgang*. A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional.* 12. ed. Porto Alegre: Livraria do Advogado, 2015.
[102] VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. Porto Alegre: Sergio Antonio Fabris, 2007
[103] GARFINKEL, Simson. *Database nation: the death of privacy in the 21st century.* Boston: O'Reilly Media, 2010

a privacidade não se limita a ocultar informações, mas está intrinsecamente ligada à ideia de auto-posse, autonomia e integridade. Proteger a privacidade é, na verdade, resguardar o indivíduo de estigmas e questões sociais não resolvidas, destacando sua imprescindibilidade. O direito das pessoas de controlarem suas esferas privadas, decidindo quais aspectos de suas vidas permanecem privados e quais são divulgados, possibilita o desenvolvimento da individualidade, proporcionando uma defesa contra estigmas e preconceitos sociais.

Nesse sentido, a liberdade é um elemento crucial para a efetivação do direito à privacidade. O exercício da liberdade implica na existência da privacidade, permitindo um momento de reflexão entre o ser e seu íntimo, sem influências externas da sociedade interferindo nas escolhas individuais. A privacidade, portanto, assegura a autodeterminação do indivíduo. Por outro lado, é notável que em Estados autoritários, a supressão da privacidade é um dos principais mecanismos de manutenção do poder, permitindo um controle quase total sobre os cidadãos[104].

1.4 Da privacidade à proteção de dados pessoais

Com base nas considerações até aqui apresentadas, é observado que o direito à privacidade é um conceito em constante evolução. A influência dos avanços tecnológicos e suas repercussões na esfera privada do indivíduo desempenha um papel significativo na adaptação desse direito ao contexto socioeconômico[105].

Apesar da importância da dimensão negativa desse direito, expressa principalmente no "direito de ser deixado em paz", ela se revela inadequada para lidar com os desafios impostos pelos novos métodos de tratamento de informações pessoais. A evolução do direito à privacidade diante das novas tecnologias exige respostas a problemas mais complexos na sociedade contemporânea, onde as ameaças à esfera privada não são mais predominantemente físicas, mas sim

[104] SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional*. 12. ed. Porto Alegre: Livraria do Advogado, 2015.
[105] ORWELL, George. *1984*. Tradução Alexandre Hubner, Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

relacionadas à exposição do corpo informacional do indivíduo por meio da coleta sistemática de dados.

A ascensão de mecanismos de Big Data, particularmente aqueles capazes de depurar vastas informações, como o data mining, contribui para um ambiente em que o armazenamento de dados é cada vez mais facilitado, passando de dispositivos físicos tradicionais para o armazenamento em nuvem (cloud computing), com capacidades crescentes e custos decrescentes[106]. Isso resulta em uma mudança do paradigma do esquecimento para o paradigma da memória, onde praticamente tudo é retido e considerado em vários aspectos da vida do indivíduo.

Um exemplo emblemático dessa transformação é o caso do Google Spain, no qual um cidadão espanhol buscou a remoção de informações sobre a penhora de seu imóvel de mecanismos de busca, alegando o direito ao esquecimento. Esse caso, julgado pelo Tribunal de Justiça da União Europeia, destaca a importância da evolução do direito à privacidade diante das novas problemáticas, levando ao reconhecimento de um direito mais abrangente que não apenas protege contra ingerências externas, mas também aborda o controle das informações pessoais do indivíduo[107].

É diante desses cenários que a mutação do direito à privacidade se revela crucial. O reconhecimento dessas novas problemáticas pela doutrina foi essencial para moldar um direito à privacidade que vai além das intervenções físicas externas, focalizando no controle das informações pessoais do indivíduo. Desse desenvolvimento surge um novo direito: o direito à proteção de dados pessoais, destinado a abordar questões relacionadas à coleta e ao tratamento de dados, especialmente os conduzidos por meios informatizados. Esse novo direito não apenas visa evitar a exposição indesejada da pessoa, mas também busca proteger contra a discriminação e preservar a autonomia individual.[108]

O debate em torno do direito à proteção de dados pessoais transcende a dicotomia entre público e privado, buscando soluções para desafios distintos daqueles enfrentados pelo direito à privacidade. Dados pessoais considerados

---

[106] RUARO, Regina Linden; MACHADO, Fernando Inglez de Souza. *Ensaio a propósito do direito ao esquecimento: limites, origem e pertinência no ordenamento jurídico brasileiro*. Revista do Direito Público, Londrina, v. 12, n. 1, p.204-233, abr. 2017. p. 206.
[107] *Ibidem*, p. 211.
[108] *ibidem.*

"públicos" ou de acesso público podem ser utilizados de maneira prejudicial, mesmo sem violar a esfera privada do indivíduo. A criação de perfis de consumo ou comportamento, embora não afete diretamente a privacidade do titular dos dados, tem implicações significativas em sua vida[109].

Diante de questões dessa natureza, a proteção do direito à privacidade se mostra insuficiente, sendo o direito à proteção de dados pessoais a alternativa mais adequada para enfrentar esses novos desafios em um mundo cada vez mais informatizado.

[109] RUARO, Regina Linden; MACHADO, Fernando Inglez de Souza. *Ensaio a propósito do direito ao esquecimento: limites, origem e pertinência no ordenamento jurídico brasileiro*. Revista do Direito Público, Londrina, v. 12, n. 1, p.204-233, abr. 2017.

2. PROTEÇÃO DE DADOS NO SISTEMA DA UNIÃO EUROPEIA

A proteção de dados no contexto da União Europeia representa um paradigma significativo no panorama global, delineando-se como um modelo referencial em matéria de salvaguarda da privacidade e dos direitos fundamentais dos cidadãos. Esse sistema, intrinsecamente vinculado à evolução dos conceitos de privacidade e proteção de dados pessoais, destaca-se pela sua abordagem inovadora e pela criação de padrões que transcendem fronteiras nacionais.

No cerne desse complexo sistema, encontra-se a busca pela harmonização e integração, fundamentada nas premissas da União Europeia enquanto uma entidade supranacional. A capacidade integrativa da União Europeia se revela como um elemento distintivo, conduzindo à implementação de normas comuns para a proteção de dados, não apenas para garantir a coesão interna, mas também para promover o livre fluxo de informações entre os Estados-Membros.

A trajetória da proteção de dados na União Europeia remonta à sua decisiva intervenção com regras supranacionais, evidenciando um compromisso inabalável com a salvaguarda dos direitos dos cidadãos europeus. O reconhecimento do direito à privacidade como um direito de personalidade, e sua subsequente evolução para um direito autônomo à proteção de dados pessoais, exemplifica a profundidade e a abrangência desse sistema jurídico.

No intuito de compreender integralmente a estrutura normativa vigente, é essencial contextualizar não apenas as premissas que alicerçam a proteção de dados na União Europeia, mas também os elementos centrais que delineiam esse sistema. Ao explorar esses aspectos, emerge uma compreensão aprofundada do caráter central do sistema europeu, focado na natureza intrínseca dos direitos associados à proteção de dados pessoais. A partir disso, este capítulo visa lançar luz sobre a importância e a complexidade do sistema de proteção de dados na União Europeia, destacando seu papel como referência para abordagens progressistas e eficazes em um cenário global cada vez mais conectado.

2.1 O Histórico da Proteção de Dados Pessoais na União Europeia

A temática da proteção de dados pessoais não era uma questão nova nos Estados-Membros da União Europeia por ocasião da aprovação da primeira diretiva a respeito. Mais de uma década antes do início das discussões acerca da regulamentação desse tema em âmbito comunitário por meio de uma diretiva, já se debatia a proteção dos indivíduos em relação ao processamento automatizado de dados pessoais em diversos contextos.

Na França, no início do século XIX, os tribunais relutavam em reconhecer um direito subjetivo à proteção da intimidade, tratando a questão como algo excepcional. Somente em 1858, no caso Felix c. O'Connell[110], os tribunais franceses abordaram incidentalmente o direito à privacidade, apesar da existência anterior de regras esparsas que, com a introdução do conceito de privacidade, foram agrupadas, como é o caso do segredo de correspondência, estabelecido na França em 1790[111].

Assim em 1970, após um extenso processo jurisprudencial, o legislador francês modificou o artigo 9º do Código Civil para incluir o "direito ao respeito de sua vida privada"[112], levando os tribunais a proferirem numerosas decisões sobre a proteção da privacidade[113].

---

[110] JURISPRUDENCE française en matière de droit civil. Revue Trimestrielle de Droit Civil, Paris, p. 111, jan./mars. 1971

[111] Escritórios oficiais franceses responsáveis pela fiscalização da correspondência, onde cartas de pessoas ou com conteúdo suspeito eram abertas para verificação. A abolição de tais práticas e a confirmação do sigilo de correspondência veio pela Lei 10 de 24 de agosto de 1790 e Lei 10 de 11 de julho de 1791, na esteira da Revolução Francesa e da reforma de institutos e instituições características dos regimes absolutistas. A esse respeito, confira-se FERNANDES, Milton. Proteção civil da intimidade. São Paulo: Saraiva, 1977

[112] FERNANDES, Milton. Proteção civil da intimidade. São Paulo: Saraiva, 1977

[113] "A jurisprudência francesa é abundante em matéria de direitos da personalidade, ao proteger a vida privada, a imagem, o nome, a sepultura, os souvenirs de família, as 'lettres missives', o direito moral de autor e outros bens da personalidade. Sua força se fez sentir, quando em 17 de julho de 1970 foi promulgada a Lei nº 70.643, que modificou o art. 9º do Código Civil, ao reconhecer a proteção da vida privada, nestes termos: 'Chacun a droit au respect de sa vie privée'. A nota do referido artigo assinala que les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire teutes mesure, telles que séquestre, saisie et autres, popres à empêcher ou faire cesser un atteinte à l'intimité de la vie privée; ces mesures peuvent, s'il y a urgence, être ordenées en référe." GOGLIANO, Daisy. *Direitos privados da personalidade*. São Paulo: Quartier Latin, 2013

Na Itália, a atenção para a questão começou por volta de 1971, com o surgimento do "primeiro caso Fiat"[114]. A partir desse momento, a doutrina e a jurisprudência evoluíram o conceito de diritto alla riservatezza para abranger a proteção dos dados pessoais como uma extensão da proteção à personalidade e à identidade pessoal. Apesar de vários projetos de lei, o país só legislou sobre o assunto em 1996, causando problemas a empresas italianas, como o "segundo caso Fiat", que envolveu a transferência de dados de funcionários da filial francesa para a sede na Itália[115].

A primeira legislação nacional sobre a matéria, segundo relatos, foi a lei sueca de 1973 sobre o controle de bancos de dados. Em 1977, a lei federal alemã, seguindo o exemplo do Land de Hesse, denominada Bundesdatenschutzgesetz, foi promulgada. A lei francesa de 1978, Informatique et Libertés, estabeleceu a autoridade de dados pessoais do país, a CNIL - Commission Nationale de l'Informatique et des Libertés. Pouco depois, países como Dinamarca, Áustria e Noruega também promulgaram suas próprias leis[116].

Apesar do cenário internacional, a criação de regras específicas e vinculantes sobre o processamento de dados pessoais não resultou naturalmente de um interesse dos órgãos supranacionais da União Europeia ou de seus Estados-membros. Duas correntes explicam[117] a evolução do tratamento dessa matéria na comunidade europeia, adotando modelos opostos para explicar a sequência de eventos que levou à aprovação da Diretiva 95/46/CE[118].

---

[114] Não se pode confundir este caso com o famoso “caso Fiat” dos anos 1980, no qual a Fiat italiana foi impedida pela CNIL, autoridade francesa de dados pessoais, de receber dados dos empregados de sua filial francesa pela ausência de legislação sobre proteção de dados pessoais.
[115] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2016, p. 202.
[116] A primeira lei sobre o assunto não tinha alcance nacional: em 1970 no Land de Hesse, na Alemanha, foi promulgada a Hessisches Datenschutzgesetz, lei bastante sintética sobre a atividade de centros de processamento de dados geridos pelo Estado e instituições correlatas. A esse respeito, confira-se DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, cit., p. 228. DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2016
[117] DONEDA, Danilo. *Op,cit.*, p. 202.
[118] Diretiva que atualmente centraliza o trato da matéria na União Europeia. UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial L. 281, 23 de novembro de 1995. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A31995L0046.. Acesso em: 20/11/2023

A análise de Abraham Newman[119] sobre o papel dos agentes transnacionais na referida diretiva detalha essa dinâmica. O primeiro modelo é baseado em uma lógica intergovernamental liberal, no qual o desenvolvimento da matéria no âmbito comunitário ocorreu pela intervenção dos Estados-membros mais poderosos, devido a seus interesses econômicos.

A partir da década de 1970, França, Alemanha e Reino Unido adotaram regras rigorosas sobre a proteção de dados pessoais, criando uma desvantagem para as empresas dos países que ainda não haviam regulamentado esse aspecto[120].

No entanto, contrariando as expectativas, empresas de países com regulamentação rigorosa não advogaram pela busca de normativas equivalentes ou semelhantes no âmbito comunitário para promover a competitividade nacional. Associações empresariais pan-europeias, como a União de Confederações Industriais e Patronais da Europa (UNICE), opuseram-se veementemente à criação de regras supranacionais para regular a proteção de dados pessoais e o fluxo transnacional desses dados. Argumentavam que tal regulação imporia um ônus significativo à indústria[121].

Mesmo empresas de nações com altos padrões regulatórios, notadamente do Reino Unido e da Alemanha, mantiveram uma postura contrária à regulação regional, mesmo quando a Comissão Europeia revisou sua posição na década de 1990 e começou a preparar propostas para tal regulamentação. Surpreendentemente, não há evidências de que Estados-membros com regulamentação robusta tenham buscado influenciar a Comissão para a criação de normas supranacionais nas décadas de 1970 e 1980, conforme relatos de Newman[122].

O segundo modelo, fundamentado na tradição neofuncionalista, sugere que a Comissão Europeia tem a capacidade de expandir suas competências e ampliar o escopo das decisões supranacionais, adotando uma abordagem cume/base. De acordo com esse raciocínio, a Comissão poderia, ao criar grupos de estudos e

---

[119] NEWMAN, Abraham L. *Building transnational civil liberties: transgovernmental entrepreneurs and the European data privacy directive. International Organization*, v. 62, n. 1, p. 106, Jan. 2008. doi: https://doi.org/10.1017/S0020818308080041. Acesso em: 20/11/2023

[120] *Idem, Ibid.*

[121] *Idem, Ibid.*

[122] *Idem, Ibid.*

comissões transnacionais, incluir determinadas questões na agenda da regulação regional.

No entanto, as previsões desse modelo não coincidem com os eventos reais, como aponta Newman[123]. A formação de leis nacionais sobre proteção de dados na década de 1970 resultou na criação de uma rede de especialistas que pressionou as instituições europeias para a adoção de regulamentações regionais sobre o tema. Esses especialistas temiam que uma regulação parcial na região pudesse gerar riscos significativos, especialmente em relação às transferências internacionais de dados, contribuindo para a formação de "paraísos de dados pessoais".

Apesar dos esforços desse grupo, seus resultados foram limitados. Embora tenham obtido a aprovação de resoluções junto ao Parlamento Europeu clamando pela necessidade de regras pan-europeias, houve pouco interesse da Comissão, que alegava que a regulação supranacional aumentaria os custos operacionais na Europa e que as regras de privacidade eram mais adequadas ao setor público, ultrapassando a jurisdição da Comunidade Europeia[124].

Outro sucesso limitado foi a assinatura da Convenção de Estrasburgo em 1981, formulada no âmbito do Conselho da Europa. No entanto, essa convenção teve eficácia restrita devido à necessidade de implementação nacional e ao foco na simplificação dos obstáculos aos fluxos transnacionais de dados.

Diante da incapacidade dos modelos anteriores em explicar os eventos que conduziram à concretização da diretiva sobre proteção de dados pessoais, Newman[125] argumenta que a mudança na posição da Comissão Europeia em relação às regras pan-europeias foi resultado das pressões exercidas pelas Autoridades Nacionais de Proteção de Dados, órgãos administrativos autônomos e independentes, estabelecidos pelas leis nacionais de proteção de dados para supervisionar e controlar atividades relacionadas ao ramo, dotados de poderes delegados.

---

123 NEWMAN, Abraham L. *Building transnational civil liberties: transgovernmental entrepreneurs and the European data privacy directive.* International Organization, v. 62, n. 1, p. 106, Jan. 2008. doi: https://doi.org/10.1017/S0020818308080041. Acesso em: 20/11/2023

124 *Ibidem*.

125 *Ibidem.*

Em que pese as variações na composição e nas atribuições entre diferentes países, quase todos detinham o poder de influenciar as transferências transfronteiriças de dados pessoais, podendo condicionar ou proibir tais transferências. Baseando-se nos argumentos apresentados por especialistas desde 1970, que defendiam a regulamentação supranacional para aumentar a proteção dos usuários e evitar a criação de "paraísos de dados", as autoridades nacionais de dados, coordenadamente, passaram a pressionar as instituições da comunidade europeia por normas supranacionais.

Assim, a ameaça de bloquear o fluxo de dados em grande parte da Europa foi uma estratégia utilizada. O diferencial nesse processo foi o poder de proibir transferências para países sem níveis equivalentes de proteção. Diante da resistência encontrada, os critérios de análise da equivalência de proteção, já estabelecidos em leis nacionais, foram aplicados com maior rigor, resultando, em casos relevantes, no bloqueio de transferências de dados.

Após repetidas situações semelhantes, o grupo de autoridades conseguiu mudar a dinâmica decisória em relação à legislação supranacional sobre dados pessoais, tornando mais difícil a manutenção de um vácuo regulatório na comunidade europeia. Isso culminou, na década de 1990, na revisão pela Comissão Europeia de sua abordagem quanto à regulamentação da proteção e livre circulação de dados pessoais, resultando na Diretiva 95/46/CE, que foi a norma central na União Europeia até maio de 2018.

Durante o acompanhamento da implementação da Diretiva 95/46/CE, o primeiro relatório de 2003[126] indicou um atraso na transposição da diretiva pelos Estados-membros, mas até o relatório de 2007, constatou-se a transposição completa. No entanto, foram aprovadas outras diretivas complementares, abrangendo áreas não contempladas pelo sistema original. O processo de implementação da Diretiva foi completo, embora tenha enfrentado alguns atrasos, conforme previsto no artigo 33 da própria diretiva.

Em 2003, o Grupo de Trabalho 29 apresentou o primeiro relatório sobre a implementação da Diretiva, destacando o atraso na implementação pelos Estados-

[126] COMISSÃO EUROPEIA. *Relatório da Comissão. Primeiro Relatório sobre a implementação da Directiva relativa à protecção de dados (95/46/CE).* COM(2003) 265 final. Bruxelas, 15 maio 2003. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52003DC0265. Acesso em: 20/11/2023

membros, atribuído à dificuldade de transpor uma norma que, ao mesmo tempo, concedia ampla margem ao Estado e exigia respeito a detalhes específicos. O relatório também indicou que a Diretiva estava atingindo seu objetivo de proporcionar um alto nível de proteção de dados pessoais sem criar barreiras intransponíveis. No entanto, observou-se a falta de transparência na aplicação das regras, resultante da insuficiência de recursos das autoridades de controle, relutância dos responsáveis pelo tratamento em ajustar suas práticas e baixo conhecimento dos usuários sobre seus direitos. O relatório incentivou o monitoramento dessas tendências e a coleta de informações adicionais[127].

Outro ponto relevante mencionado no relatório dizia respeito às tecnologias que aumentam a privacidade, destacando a importância de promover e incentivar essas tecnologias como complemento às abordagens legais. O relatório sugeriu a necessidade de certificações para produtos em conformidade com as regras europeias de proteção de dados pessoais e privacidade[128].

O segundo relatório de 2007 informou que a implementação da Diretiva nos Estados-membros estava concluída, embora em alguns casos sua aplicação tenha sido insatisfatória. O relatório reiterou a adequação fundamental das regras estabelecidas, desaconselhando alterações na Diretiva naquele momento[129].

A partir de 2010, começou-se a discutir novamente a necessidade de reformas na proteção dos dados pessoais. O projeto de reforma surgiu com a comunicação da Comissão ao Parlamento Europeu em novembro de 2010, intitulada "Uma abordagem global da proteção de dados pessoais na União Europeia". Essa comunicação destacou a evolução tecnológica, a mudança na interação e compartilhamento de dados pessoais pelos indivíduos, especialmente em redes sociais e na computação em nuvem.

Por fim, em 2012, a Comissão apresentou propostas para uma nova Diretiva e um Regulamento, sendo este último conhecido como o General Data Protection

---

[127] COMISSÃO EUROPEIA. *Relatório da Comissão. Primeiro Relatório sobre a implementação da Directiva relativa à protecção de dados (95/46/CE)*. COM(2003) 265 final. Bruxelas, 15 maio 2003. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52003DC0265. Acesso em: 20/11/2023.

[128] *Ibidem.*

[129] COMISSÃO EUROPEIA. *Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o acompanhamento do programa de trabalho para uma melhor aplicação da directiva relativa à proteção de dados.* COM(2007) . Disponível em: https://eur-lex.europa.eu/PT/legal-content/summary/protection-of-personal-data.html. Acesso em:20/11/2023.

Regulation[130] (GDPR), aprovado em 2016 e tornando-se o principal regulamento na União Europeia para a proteção de dados pessoais. Este regulamento eliminou a necessidade de transposição e visava resolver as questões de aplicação divergente da Diretiva 95/46/CE pelos Estados-membros[131].

2.2 O Direito à Proteção dos Dados Pessoais

A ascensão do Direito à Proteção dos Dados Pessoais como um paradigma regulatório na União Europeia não é apenas um fenômeno regional; trata-se de uma referência global. O impacto do Regulamento Geral de Proteção de Dados (RGPD) transcende fronteiras, influenciando a elaboração de legislações semelhantes em várias jurisdições, inclusive no Brasil.

Desse modo, antes de se adentrar mais profundamente nesse tema, é essencial conduzir uma análise concisa sobre a evolução desse direito e sua consagração como um dos fundamentos primordiais na União Europeia, consolidado por meio de sua inclusão na Carta dos Direitos Fundamentais de tal bloco.

2.2.1. Da privacidade à autodeterminação informática

A incorporação da proteção de dados pessoais como uma faceta do direito à privacidade remonta ao início do século XX. Esse desenvolvimento ocorreu durante a transição do Estado liberal para o Estado de bem-estar social, quando o governo passou a coletar informações dos cidadãos com o objetivo de aprimorar a eficiência da administração e melhor distribuir seus recursos. Inicialmente, essa atividade era conduzida pelo Estado devido aos elevados investimentos e à infraestrutura que, na época, nem mesmo os grandes grupos empresariais

[130] Tradução: Regulamento Geral de Proteção de Dados (RGPD)
[131] COMISSÃO EUROPEIA. *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. COM(2012) 11 final.* Bruxelas, 25 jan. 2012. Disponível em: http://docplayer.com.br/3497609- Proposta-de-regulamento-do-parlamento-europeu-e-do-conselho.html. Acesso em: 20/11/2023.

possuíam, ou optavam por não utilizar, devido à incerteza em relação à utilidade desses dados[132].

Com os avanços recentes na tecnologia subjacente à rede mundial e sua crescente adoção pela sociedade, surgiu uma preocupação crescente em relação ao controle dessas informações. Uma vez que essas informações dizem respeito à vida pessoal do indivíduo, são consideradas derivadas do próprio conceito de privacidade. Foi nesse contexto que, a partir da década de 1970, começou a se desenvolver uma segunda interpretação do direito à intimidade: o direito à privacidade como o direito de controlar quais aspectos da vida privada e informações relacionadas devem ser mantidos em segredo e quais podem ser revelados, total ou parcialmente[133].

Abordando uma perspectiva mais radical, Juan Carlos Menéndez Mato e Maria Eugenia Gayo Santa Cecilia[134] argumentam que, embora tradicionalmente o direito à proteção de dados pessoais esteja associado ao direito à privacidade, ele começa a ser reconhecido como um direito autônomo, com conteúdo próprio, fundamentado em princípios específicos e protegido por mecanismos especializados.

Pedro Servera[135], por sua vez, identifica a ligação entre o direito à privacidade e o direito à proteção de dados pessoais no mecanismo fundamental que sustenta ambos os direitos: o consentimento. Tanto no caso dos dados pessoais quanto na ampla acepção da privacidade, cabe ao titular dos direitos decidir quem pode acessar sua esfera íntima, seja adentrando sua casa e convívio

---

[132] FERNANDES, Milton. *Proteção civil da intimidade*. São Paulo: Saraiva, 1977

[133] PUGLIESE, Giovanni. *Il diritto alla riservatezza nel quadro dei diritti della personalità.* In: STUDI in onore di Alberto Asquini. Padova: CEDAM, 1965

[134] MENÉNDEZ MATO, Juan Carlo; GAYO SANTA CECILIA, Maria Eugenia*. Derecho e informática: ética y legislación*. Barcelona: Bosch, 2014. p. 281

[135]O autor afirma: *Desglosando cada uno de los derechos con los que hemos conformado 'la protección de la vida privada', intimidade, honor, propria imagen y protección de datos personales, puede observar-se que en todos (salvo en el derecho al honor por sus propias peculiaridades) la primera línea de protección de la vida privada la determina el titular de los derechos a través de su derecho a decidir (a través de su consentimiento): es la persona la que decide quién puede entrar en su casa (es la persona la que decide si un tercero le puede seguir en facebook o no), es la persona quien decide si una información puede ser conocida por otros (es la persona la que decide qué información va transmitiendo a través de twitter) (…).* GRIMALT SERVERA, Pedro. La necessária reconducción del régimen jurídico de la protección de los datos personales desde la perspectiva de los conflitos y solapamentos com otros derechos y libertades en internet. In: VALEROS TORRIJOS, Julián (Org.). La protección de los datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica. Cizur Menor, Navarra: Thomson Reuters/Aranzadi, 2013

familiar ou tomando conhecimento de seus dados, como os disponíveis em seu perfil de uma rede social[136].

David Ordóñez Solís[137] coaduna com ambas as perspectivas: a proteção dos dados pessoais é ao mesmo tempo fundamentada na privacidade e constitui um direito autônomo. Não se busca aqui negar o valor fundamental desse novo direito, mas reconhecer que, apesar dessa identidade, a proteção de dados pessoais é uma garantia que demanda mecanismos específicos de tutela.

A partir de diversas abordagens ao direito à proteção de dados pessoais, observa-se que, embora tenha sua origem primordial no direito à privacidade - considerado seu fundamento axiológico -, a proteção de dados atualmente é reconhecida como merecedora de normatização específica, constituindo, assim, um direito fundamental independente. Essa tendência implica, na prática, que a proteção de dados, embora vinculada à privacidade, deve ser regulamentada por normas próprias, contendo princípios e regras específicos. Não é viável apenas realizar ajustes nas leis existentes por meio de modificações legislativas ou interpretações extensivas, dada a falta de menções claras sobre dados pessoais.[138]

Stefano Rodotà[139] e Arnaud Belleil[140] compartilham dessa posição, argumentando que questões emergentes em um novo contexto social devem ser abordadas dentro desse contexto, considerando os valores em conflito no cenário atual, em vez de buscar soluções com base em concepções de privacidade de épocas anteriores. Portanto, embora se reconheça a conexão entre os direitos, a proteção aos dados pessoais requer uma análise contemporânea, inserida nas

---

[136] Nesse sentido, António Barreto Menezes Cordeiro assevera que: “A necessidade de, por princípio, o titular ter de consentir no tratamento dos seus dados pessoais assume-se como uma das principais garantias de proteção dos interesses individuais de cada sujeito. A sua consagração no artigo 8.º/2 da Carta dos Direitos Fundamentais da União Europeia impossibilita que o consentimento venha, porquanto esta disposição se encontre em vigor, a ser ignorado pelo legislador europeu ou pelos legisladores nacionais. (CORDEIRO, A. Barreto Menezes. O *Consentimento do Titular dos Dados no RGPD*. Disponível em: https://blook.pt/publications/publication/e772e2d8f7b4/. Acesso em: 20/11/2023, p.01)

[137] ORDÓÑEZ SOLÍS, David*. Privacidad y protección judicial de los datos personales*. Barcelona: Bosch, 2011.

[138] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2016. P. 164

[139] RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Org., sel. e apres. de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.p.72.

[140] BELLEIL, Arnaud. *@-Privacidade: o mercado dos dados pessoais, proteção da vida privada na internet.* Lisboa: Instituto Piaget, 2002.

disputas entre os interesses presentes dos diversos atores envolvidos nas relações que envolvem dados pessoais.

Após a inicial conceituação dos dados pessoais e sua aceitação como elementos a serem protegidos juntamente com a vida privada no "novo direito à privacidade", a doutrina buscou sistematizar essa proteção. Inicialmente, dois fatores fundamentais foram identificados para avaliar a legalidade na coleta de dados, conforme Anderson Schreiber[141]: a dimensão procedimental, que abrange a legalidade do modo de coleta, e a dimensão substancial, que diz respeito à finalidade e uso efetivo dos dados. A legalidade de um procedimento de coleta e tratamento requer que ambos, o modo e o uso final dos dados, sejam legais e legítimos.

Stefano Rodotà[142], seguindo a linha de pensamento de Westin[143] e Canotilho[144], definiu esse posicionamento ativo como um "direito de autodeterminação informativa". Este direito não apenas confere direitos ao sujeito, mas também impõe deveres positivos aos usuários dos dados pessoais, incluindo a obrigação de obter autorização para a coleta de dados, a vinculação entre a autorização concedida e a finalidade informada da coleta, e o fornecimento de acesso ao banco de dados ao titular dos dados. Esses deveres, entre outros, foram consolidados como princípios orientadores na Convenção de Estrasburgo de 1981 para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais[145].

Essa convenção estabelece cinco princípios principais: o princípio da publicidade, que demanda que a existência de um banco de dados com dados pessoais seja de conhecimento público; o princípio da exatidão, que exige a precisão dos dados; o princípio da finalidade, que determina que a coleta de dados deve ter um propósito específico; o princípio do livre acesso, que garante ao titular o acesso aos dados inscritos no banco; e o princípio da segurança física e lógica, que assegura a proteção dos dados. Esses princípios visam garantir a

---

141 SCHREIBER, Anderson. *Direitos da Personalidade*. São Paulo: Editora Atlas, 2013

142 RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Org., sel. e apres. de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008. p.96.

143 WESTIN, Alan. *Privacy and Freedom*, New York: Atheneum, 1970

144 CANOTILHO, J.J. Gomes. *Direito constitucional e teoria da Constituição*. 7. ed. Coimbra: Almedina, 2003.

145 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2016, p. 171.

transparência, informação adequada ao titular dos dados e a proteção eficaz dos dados pessoais[146].

O princípio da finalidade, também conhecido como princípio da limitação dos propósitos, assume um papel preponderante nos debates atuais relacionados à legalidade do mercado de compra e venda de dados pessoais, especialmente nas redes sociais e outros serviços online considerados "gratuitos." Este princípio visa restringir o impacto da autorização concedida pelo indivíduo para a coleta de seus dados pessoais, evitando que esses dados sejam utilizados de maneira contrária à vontade inicial do indivíduo. Dessa forma, os dados só podem ser coletados, processados e utilizados para a finalidade explicitamente apresentada e aceita pelo usuário. Por exemplo, é inadmissível que um usuário autorize a exibição pública de sua imagem em uma rede social e, posteriormente, seus dados, como foto, nome e demais informações, sejam vendidos a terceiros para fins publicitários, uma vez que tal uso não foi previamente descrito na proposta inicial ao usuário[147].

Além disso, a finalidade declarada do tratamento serve como critério para avaliar se a coleta de dados é adequada e necessária, ou se configura excessiva ou ilegítima. Por exemplo, se um responsável pretende coletar dados para personalizar um serviço ao usuário, é imperativo informar ao usuário como esses dados serão utilizados. Simultaneamente, um responsável que oferece um serviço de correio eletrônico personalizado não pode coletar dados de saúde do usuário, pois esses dados seriam incompatíveis com a finalidade do tratamento. O princípio da finalidade desempenha, assim, um papel crucial na garantia de transparência e conformidade legal no tratamento de dados pessoais[148].

Por outro lado, o princípio do livre acesso é fundamental para que o usuário possa exercer controle sobre o tratamento de seus dados pessoais e garantir sua legalidade. Este princípio assegura ao usuário o direito de acessar seus dados, independentemente de sua localização, permitindo a obtenção de cópias, correção de informações e exclusão de dados obsoletos. Relacionado ao instituto brasileiro do habeas data, o princípio do livre acesso se estende além dos bancos de dados públicos, abrangendo também os privados. Sua integração com o princípio da

---

146 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2016, p. 171.
147 *Ibidem,* p. 212.
148 *Ibidem,* p.226.

exatidão garante que os dados pessoais sejam precisos, coletados de maneira correta e armazenados fielmente à realidade, conferindo ao indivíduo o direito de corrigir, modificar ou remover tais dados[149].

Por fim, o princípio da segurança física e lógica impõe a responsabilidade ao depositário das informações pela proteção dos dados contra destruição, alteração e acesso não autorizado, seja por meios físicos ou virtuais. Essa responsabilidade não se limita à compensação em casos de violação, exigindo também a implementação de medidas tecnológicas e organizacionais para mitigar os riscos inerentes ao processamento de dados pessoais. Se uma violação ocorrer devido à falta de implementação de medidas de segurança, o responsável pelo tratamento deve ser responsabilizado por não adotar tais precauções para reduzir o risco de violações[150].

2.2.2. A consolidação de um direito fundamental

O entendimento do percurso do direito à privacidade e à proteção de dados, até sua consolidação como um direito fundamental, é de suma importância no contexto legislativo ordinário. A obtenção desse status confere relevância e suscita questionamentos sobre suas limitações. Para elucidar a consolidação do direito à proteção de dados pessoais como um direito fundamental na União Europeia, é essencial analisar sucintamente o histórico do Direito Internacional, destacando convenções que exerceram influência até a consolidação da Carta de Direitos Fundamentais da UE.

O surgimento do direito à privacidade no Direito Internacional contemporâneo, conforme já abordado anteriormente, remonta à Declaração Universal dos Direitos Humanos de 1948. Esta, como resposta às atrocidades da Segunda Guerra Mundial, assegura, em seu artigo 12, o direito à proteção da intimidade, vida privada e familiar, bem como o sigilo de correspondência, protegendo contra interferências arbitrárias. De maneira relacionada, o artigo 19 garante a liberdade de opinião e expressão, correlacionando-se, em certos

[149] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2016, p. 226.
[150] *Ibidem*, p. 172.

aspectos, à proteção da intimidade do indivíduo. Apesar de aparente contradição, o artigo 29 reconhece a necessidade de equilíbrio entre os direitos, sem afirmar a absoluta irrevogabilidade de nenhum deles[151].

O pós-Segunda Guerra Mundial impulsionou a criação da Convenção Europeia sobre Direitos Humanos em 1950[152], fortalecendo o arcabouço de direitos delineado pela Declaração. Ao contrário desta, a Convenção estabelece uma obrigação objetiva para que seus membros instituam e garantam os direitos e liberdades nela previstos, com a criação de legislação interna compatível com o tratado.

Além da simples obrigação, a Convenção conta com um sistema de aplicação e fiscalização pela Corte Europeia de Direitos Humanos, independente da União Europeia. Essa corte, embora frequentemente associada à União Europeia, tem jurisdição mais ampla, julgando casos relacionados a violações da Convenção, com efeitos vinculantes aos Estados-Membros. O artigo 12 da Convenção Europeia de Direitos Humanos estabelece o direito à intimidade e à vida privada, permitindo violações justificadas por finalidades legais, como persecução penal e segurança nacional.

Apesar de a privacidade ter obtido status de direito fundamental, o reconhecimento do direito à proteção de dados foi um processo mais demorado. Somente com a Carta de Direitos Fundamentais da União Europeia, em 2000[153], é que o direito à proteção de dados pessoais foi elevado à categoria de garantia fundamental, conforme consta no artigo 8º da Carta:

> 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessa ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam

[151] NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos*. Adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos.Acesso em: 20/11/2023

[152] CONSELHO DA EUROPA. *Convenção Europeia dos Direitos do Homem*. Disponível em: https://www.echr.coe.int/documents/d/echr/convention_por. Acesso em: 20/11/2023

[153] PARLAMENTO EUROPEU. CONSELHO DA EUROPA. *Carta de Direitos Fundamentais da União Europeia (2000/C 364/01*). Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 20/11/2023

> respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente[154].

O destaque reside no fato de que a Constituição não adotou uma abordagem simplista em sua salvaguarda. Em vez de meramente elevar o direito a um patamar fundamental dentro do sistema jurídico, a Carta incorporou outros três elementos como indispensáveis para a efetiva observância do direito fundamental à proteção de dados[155].

O primeiro ponto crucial é que, para considerar o direito atendido, o tratamento de dados pessoais deve ser (i) leal, (ii) com finalidades específicas e (iii) fundamentado em uma base legal adequada, seja ela o consentimento ou outro fundamento jurídico. O tratamento leal implica em uma abordagem verdadeiramente apropriada, ou seja, realizada de acordo com as expectativas do titular dos dados e em conformidade com as informações fornecidas a ele. Portanto, se os dados do titular são tratados de maneira diferente do que foi informado inicialmente, tal direito seria imediatamente violado[156].

A restrição do tratamento a "fins específicos" reflete o princípio da finalidade, já discutido, pelo qual os dados pessoais devem ser coletados e tratados apenas para finalidades específicas, sem a possibilidade de acumulação simples de dados na esperança de que tal conjunto se torne valioso[157].

Além disso, quando se afirma que o tratamento de dados deve ser baseado no consentimento ou em outro fundamento legal aplicável, a Carta explicita, em resumo, que o tratamento de dados pessoais é a exceção e não a regra. Ao contrário de alguns países, o tratamento de dados é, por padrão, proibido, a menos que haja uma justificativa legal para tal tratamento[158].

Em outras palavras, na ausência de uma base legal, o tratamento de dados pessoais é proibido. Esse aspecto será crucial para nossa análise, uma vez que

---

[154] PARLAMENTO EUROPEU. CONSELHO DA EUROPA. *Carta de Direitos Fundamentais da União Europeia (2000/C 364/01)*. Disponível em: https://www.europarl.europa.eu/ charter/pdf/text_ pt.pdf. Acesso em: 20/11/2023

[155] *Ibidem*.

[156] *Ibidem*.

[157] *Ibidem.*

[158] *Ibidem.*

não se trata apenas de uma regra procedimental, mas sim de um princípio elevado à categoria de garantia fundamental[159].

Em segundo lugar, o artigo estabelece como condição primária para a observância do direito fundamental a garantia de acesso ao titular, acompanhada do direito de retificação caso os dados estejam incorretos. Apesar de existirem outros direitos assegurados no RGPD, os direitos de acesso e retificação foram elevados ao status de direitos fundamentais pela Carta[160].

Ademais, em terceiro lugar, conforme a Carta, é necessário que os direitos relacionados a dados pessoais sejam supervisionados por uma autoridade independente para considerar o texto totalmente cumprido[161].

Portanto, essa disposição tem um impacto significativo, ao estabelecer como elemento fundamental da disciplina a presença das chamadas Autoridades de Proteção de Dados e, mais ainda, sua independência, o que, como observado, tem sido um ponto de conflito ao longo da implementação da Diretiva de Proteção de Dados.

2.3 Desenho Normativo

O sistema de proteção de dados pessoais da União Europeia (UE) é atualmente reconhecido como um dos mais avançados e tem servido como referência para a criação de leis em diversas partes do mundo. Não apenas o modelo europeu é considerado um ponto central nas discussões sobre a regulamentação dos dados pessoais, mas também exerce uma influência significativa sobre diversas legislações no mundo, entre elas a lei brasileira de Proteção de Dados.

A complexidade do quadro legislativo em vigor no contexto europeu exige atenção especial, pois incorpora tanto o Direito comunitário, com suas diretrizes, regulamentos, orientações e jurisprudências específicas, quanto se integra ao âmbito nacional por meio de leis, decretos e jurisprudências próprias. Essa

---

[159] PARLAMENTO EUROPEU. CONSELHO DA EUROPA. *Carta de Direitos Fundamentais da União Europeia* (2000/C 364/01). Disponível em: https://www.europarl.europa.eu/ charter/pdf/text _pt.pdf. Acesso em: 20/11/2023

[160] *Ibidem*.

[161] *Ibidem*.

integração revela notáveis variações nos espaços discricionários criados pelo direito comunitário, buscando proporcionar maior flexibilidade na adoção das normas pelos Estados-membros, visando, assim, uma adesão e efetividade mais amplas das garantias e regras estabelecidas.

Dentro do escopo deste estudo, a análise se concentrará, neste momento, no Regulamento Geral de Proteção de Dados, conhecido como RGPD. No entanto, também abordaremos brevemente outras normativas relevantes, como a Convenção nº 108 do Conselho da Europa, a Diretiva sobre e-*Privacy* e o programa denominado *Privacy Shield*. Essa abordagem visa proporcionar uma compreensão abrangente das diferentes facetas das normas de proteção de dados adotadas pela União Europeia, considerando a diversidade e a interconexão desses instrumentos legais.

2.3.1. A Convenção 108 do Conselho da Europa

Em primeira instância, a Convenção nº 108 do Conselho da Europa, de 1981, conhecida como "Convenção para a Proteção de Indivíduos em relação ao Tratamento Automatizado de Dados Pessoais" ou, simplificadamente, Convenção de Estrasburgo, destaca-se como a norma internacional mais relevante no âmbito europeu para a proteção de dados pessoais[162].

Diferentemente de outros dispositivos internacionais já mencionados, a Convenção de Estrasburgo foi pioneira ao abordar diretamente o desafio de estabelecer regras para qualquer tipo de tratamento de dados pessoais. Em contraste com instrumentos da época, a Convenção já demandava que os signatários adotassem internamente medidas necessárias para implementar e aplicar os princípios delineados em seu texto[163].

O fundamento da Convenção partiu do reconhecimento de que aqueles que fazem uso de dados pessoais têm responsabilidades específicas para evitar danos ou impactos negativos nos indivíduos a quem esses dados se referem. Entretanto, a Convenção reconhece que a proteção dos indivíduos não pode ser o único valor defendido nesse contexto, considerando também a promoção do livre trânsito dos

[162] MIGUEL ASENSIO, Pedro Alberto de. *Derecho privado de internet*. 4. ed. Madrid: Civitas, 2011.
[163] *Ibidem*.

dados pessoais dentro de certos limites como um valor a ser impulsionado. Pela primeira vez, estabeleceu-se um mecanismo de controle sobre transferências internacionais: enquanto o fluxo de dados entre os países signatários deve ser incentivado, uma vez que cada país se comprometeu a promover os mesmos valores sobre proteção de dados em suas legislações, a transferência de dados para outros países é, em princípio, proibida ou minimamente desencorajada.

Do ponto de vista substantivo, como já mencionado anteriormente, a Convenção normatizou os princípios da publicidade, exatidão, finalidade, livre acesso e segurança física e lógica[164]. Embora tenha sido superada por legislações mais recentes, a Convenção ainda representa um marco normativo para a proteção de dados, especialmente devido à sua abrangência internacional. Notavelmente, a Convenção está aberta à adesão de países não pertencentes à União Europeia, contando atualmente com 51 países que a ratificaram.

Por fim em 2018, a Convenção de Estrasburgo foi reformada por meio de um Protocolo de Alteração, modernizando-a e expandindo-a em diversos aspectos. Além dos princípios já previstos, a versão atualizada consolida disposições sobre transparência no tratamento, proibição do tratamento de dados sensíveis, garantias aos titulares (como acesso, retificação, objeção ao tratamento e objeção a decisões automatizadas) e regulamentações sobre a atuação das autoridades de proteção de dados pessoais[165].

2.3.2. Regulamento Geral de Proteção de Dados

Em 2016, o sistema europeu de proteção de dados pessoais passou por uma significativa transformação, resultante de uma abrangente reforma concebida desde o ano de 2010. Esta reforma foi principalmente instaurada pela aprovação

---

[164] EUROPEAN COMISSION. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108)*.1981. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Acesso em: 17 jan. 2024

[165] EUROPEAN COMMISSION. Council of Europe. *128th Session of the Committee of Ministers*. (Elsinore, Denmark, 17-18 May 2018). Ad hoc Committee on Data Protection (CAHDATA) - Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108). Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e. Acesso em: 20/11/2023

do Regulamento nº 679/2016 do Parlamento e do Conselho, substituindo a Diretiva nº 95/46/CE e unificando as disposições relativas à proteção de dados pessoais[166].

O Regulamento é aplicado diretamente como norma interna, eliminando a necessidade de incorporação do texto supranacional por meio de legislação interna. Denominado como Regulamento Geral de Proteção de Dados (RGPD), este conjunto normativo é reconhecido por sua abrangência e representa possivelmente um dos sistemas de proteção mais complexos em vigor globalmente.

O RGPD, com sua extensa coleção de 173 considerandos, fornece um valioso material para a interpretação das disposições normativas. O texto do regulamento, organizado em 11 capítulos, abrange: disposições gerais, princípios, direitos dos titulares de dados, responsável pelo tratamento e subcontratante, transferências internacionais de dados, autoridades de supervisão independente, mecanismos de cooperação e consistência entre autoridades, remédios, responsabilidade e penalidades, disposições sobre processamentos específicos, implementação e medidas delegadas aos Estados-Membros, e disposições finais.

Entre os temas mais relevantes destacam-se os princípios e condicionantes para o tratamento de dados, os direitos dos titulares, as responsabilidades dos responsável pelo tratamento e subcontratante, bem como as atribuições das autoridades de proteção de dados. Esta análise tem como objetivo sistematizar os principais pontos de comparação entre os sistemas, apresentando uma visão concisa do conteúdo do RGPD.

No que concerne aos princípios e condicionantes, é imprescindível salientar que o Regulamento Geral de Proteção de Dados (RGPD) estipula que, para que o tratamento de dados seja considerado lícito, deve estar fundamentado no consentimento do titular dos dados ou em outras bases legais, como o cumprimento de contratos ou obrigações legais, dispensando-se o consentimento em tais circunstâncias. Mesmo quando o tratamento se baseia no consentimento, o RGPD estabelece critérios rigorosos, exigindo que esse consentimento seja livre, informado e inequívoco. O tratamento de dados sensíveis, como informações sobre

---

[166] UNIÃO EUROPEIA. *Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Jornal Oficial L. 119/1008, 04 de maio de 2016. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023 .

saúde e opinião política, está sujeito a restrições mais rigorosas, assim como o tratamento de dados de crianças e adolescentes.

A despeito dos direitos dos titulares de dados, o RGPD enumera uma série de direitos que devem ser assegurados, abrangendo a recepção de informações transparentes e claras sobre o tratamento de dados, o acesso aos dados tratados, a retificação de dados incorretos ou desatualizados, a eliminação dos dados (também conhecido como "direito ao esquecimento"[167]), a solicitação de restrição ao tratamento de dados, a portabilidade dos dados para outro provedor de serviços semelhantes, a objeção a decisões automatizadas baseadas no tratamento de dados pessoais, e a objeção ao tratamento, entre outras variantes asseguradas na legislação vigente.

Quanto às responsabilidades do responsável pelo tratamento e subcontratante, o RGPD impõe uma extensa lista de obrigações, incluindo a designação de um Encarregado ou *Data Protection Officer* para supervisionar os tratamentos de dados, a implementação de medidas adequadas de segurança física, técnica e administrativa para garantir a segurança e confidencialidade dos dados pessoais, e a adoção de práticas responsáveis no tratamento de dados. Esta última é geralmente interpretada pelo mercado como a obrigação de estabelecer regras e procedimentos internos para garantir que o tratamento de dados seja conduzido em estrita conformidade com a legislação, seguindo um modelo de programa de compliance similar ao utilizado em áreas como prevenção à lavagem de dinheiro e combate à corrupção.

Além disso, é relevante destacar que o RGPD, refletindo os preceitos da Carta de Direitos Fundamentais de 2000, da Diretiva de Proteção de Dados de 1995 e da Convenção de Estrasburgo de 1981, detalha a obrigação de cada Estado-Membro criar uma autoridade independente de supervisão para fiscalizar o cumprimento do regulamento e de outras normativas relacionadas à proteção de dados. A independência dessas autoridades é particularmente crucial, visto que as disposições do RGPD se aplicam não apenas ao tratamento de dados pelo setor

[167] Note-se que o direito ao esquecimento europeu não é exatamente equivalente ao direito ao esquecimento brasileiro. Sobre esse tema, confira-se GUIDI, Guilherme Berti de Campos. O Caso Costeja v. Google Spain e o direito ao esquecimento: para além da implementação e rumo ao diálogo global. In: MENEZES, Wagner (Org.) Tribunais internacionais e a implementação procedimental de suas decisões. Belo Horizonte: Arraes, 2018.

privado, mas também pelos órgãos públicos de cada Estado-Membro. Tais autoridades devem possuir amplos poderes para investigar e sancionar, bem como intervir em conflitos entre particulares, seja por meio de reclamações individuais, ou em processos judiciais e administrativos dentro de suas competências.

Desse modo, naturalmente, as autoridades detêm competências consultivas e normativas, capacitando-as a estabelecer recomendações ou normativas secundárias para interpretar e regulamentar pontos específicos da legislação aplicável sobre proteção de dados. Essa prerrogativa permite um aprofundamento nos princípios e regras gerais contidos no RGPD, assim como em outras normas de amplo alcance.

2.3.3. Diretiva 2002/58/CE e a *e-Privacy Directive*

A Diretiva 2002/58/CE[168], posteriormente emendada pela Diretiva 2009/136/CE, abrange áreas insuficientemente tratadas pelo Regulamento Geral de Proteção de Dados (RGPD) no âmbito específico das comunicações eletrônicas, englobando serviços que implicam na transmissão de sinais através de redes de telecomunicação ou radiodifusão. Esta legislação explicita sua finalidade como a especificação e complementação das normas de proteção de dados estabelecidas pelo RGPD[169].

Com o intuito de atingir tal propósito, a diretiva apresenta regras especialmente relevantes ao setor devido às peculiaridades dos serviços prestados aos usuários, incluindo a abordagem de práticas específicas como o spam. Além disso, determina que os Estados-Membros da União Europeia devem promulgar leis nacionais para internalizar tais regras.

Para alcançar seus objetivos, a Diretiva opera em duas frentes, impondo obrigações tanto aos Estados quanto aos responsáveis pelo tratamento de dados. Aos responsáveis pelo tratamento de dados pessoais, são exigidas as seguintes

---

[168] UNIÃO EUROPEIA. *Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas.* Jornal Oficial L. 201, 31 de julho de 2002. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32002L0058. Acesso em: 20/11/2023

[169] Artigo 1º, 2: Para os efeitos do nº 1, as disposições da presente diretiva especificam e complementam a Diretiva 95/46/CE. Além disso, estas disposições asseguram a proteção dos legítimos interesses dos assinantes que são pessoas coletivas.

obrigações: assegurar que os dados em processamento sejam acessados apenas por pessoas autorizadas, inclusive dentro de sua organização; proteger os dados contra perda, destruição ou alteração acidental, e contra qualquer forma de tratamento ilegal ou não autorizado; garantir a implementação de uma política de segurança no tratamento dos dados pessoais; notificar todas as violações de dados pessoais à autoridade nacional no prazo de 24 horas; eliminar ou tornar anônimos dados desnecessários para comunicação ou faturamento de serviços prestados, a menos que o titular consinta na continuidade do uso para fins de comercialização; cessar imediatamente a utilização de dados mantidos exclusivamente para fins de comercialização caso o titular retire seu consentimento.

No que diz respeito aos Estados-Membros, a Diretiva estipula as seguintes obrigações: assegurar, de maneira geral, a confidencialidade das comunicações realizadas por redes públicas; proibir a instalação de escutas e outras formas de vigilância e interceptação de comunicações e dados em tráfego sem a autorização do titular, exceto por decisão judicial; garantir que informações só sejam armazenadas no dispositivo do titular ou acessadas por provedores de serviços de comunicação eletrônica quando o titular for devidamente informado e der seu consentimento.

Por fim, apesar das regras de derrogação no RGPD em relação ao consentimento do titular dos dados, a Diretiva 2002/58/CE estabelece casos específicos nos quais o consentimento permanece como requisito para a legalidade do uso dos dados. Exige-se o consentimento expresso do titular antes do envio de comunicações não solicitadas por qualquer meio de comunicação, antes da inserção de informações no equipamento pessoal do usuário ou do acesso a essas informações pelo provedor (por meio de cookies), e antes da inclusão de dados de contato do titular em listas públicas[170].

[170] CASTETS-RENARD, Céline. *Droit de l'internet: droit français et européen*. 2. éd. Paris: Montchrestien, 2012.

2.3.4. O Tribunal de Justiça da União Europeia

A União Europeia desempenha um papel crucial como um dos principais fóruns de discussão no que diz respeito às novas tecnologias[171]. Este papel pioneiro, tanto em nível supranacional quanto por meio de seus Estados-Membros, destaca-se na regulamentação de aspectos fundamentais, notadamente a privacidade e a proteção de dados pessoais. Após décadas de experiência prática, a UE oferece um ambiente maduro para debates substanciais sobre essas questões.

Uma característica particularmente interessante desse contexto é a singularidade do modelo de organização regional adotado pelo bloco. A presença de um nível de integração sem precedentes possibilita a existência e atuação de um Tribunal internacional regional, o Tribunal de Justiça da União Europeia (TJUE). Este Tribunal desempenha um papel crucial na atividade adjudicatória e consultiva da União, decidindo sobre diversas questões, incluindo pedidos de anulação de atos das instituições da União e interpretação ou validade das disposições do direito da União. Essa atuação contribui significativamente para a coesão e coerência do sistema jurídico da UE, promovendo uniformidade na aplicação da lei em seu território[172].

Como era de se esperar, o papel do Tribunal de Justiça da União Europeia tem sido fundamental tanto na experiência da Diretiva nº 95/46/CE[173] quanto na implementação do Regulamento Geral de Proteção de Dados (RGPD). Algumas decisões recentes do Tribunal destacam-se pela relevância em questões de grande

---

[171] GUIDI, Guilherme Berti de Campos. *A proteção dos dados pessoais na internet: contribuições da experiência europeia ao modelo brasileiro.* 2016. Dissertação (Mestrado) – Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade de São Paulo, São Paulo, 2016.

[172] CASELLA, Paulo Borba. *União Europeia: instituições e ordenamento jurídico*. São Paulo: LTr, 2002

[173] Com a entrada em vigor do Regulamento Geral de Proteção de Dados Pessoais em maio de 2018, a competência do Tribunal foi expandida. Na vigência da Diretiva, a competência do Tribunal lhe permitia conhecer de questões relacionadas a falhas de transposição da Diretiva para o direito interno de cada Estado Membro ou de conflitos interpretativos da lei local, que seriam então solucionados com base no texto da Diretiva. Isso ocorre porque a Diretiva é norma que atribui aos Estados-Membros a obrigação de adotar leis internas em determinado sentido, não sendo diretamente aplicável, no que se diferencia do Regulamento, que constitui norma supranacional diretamente aplicável aos governos, empresas e indivíduos.

alcance, como a revogação da Diretiva nº 2006/24/CE, que abordava a retenção de dados de conexão pelos provedores de acesso[174].

Essa Diretiva, que tratava da retenção de dados como nomes de usuários, endereços IP e localização para fins de investigação criminal, enfrentava inconsistências na regulamentação regional, motivando a busca por uniformização.

Em 2014, o Tribunal de Justiça da União Europeia declarou a Diretiva inválida, considerando-a desproporcional, uma vez que não estabelecia claramente a gravidade dos crimes justificadores do acesso a esses dados, não exigia decisão judicial para tal acesso e não impunha garantias suficientes para a proteção dos dados retidos. Além disso, a diretiva não demandava que esses dados fossem armazenados no território da União Europeia, prejudicando a supervisão das autoridades independentes competentes em proteção de dados pessoais[175].

Em uma outra oportunidade, o Tribunal proferiu uma decisão de extrema relevância relacionada às transferências internacionais de dados pessoais de cidadãos europeus. A Decisão da Comissão 2000/520/CE[176], datada de 26 de julho de 2000, estabeleceu um programa de "porto seguro" em conjunto com o Departamento de Comércio dos Estados Unidos da América. Contudo, diante de revelações sobre a devassa de dados pessoais por órgãos governamentais, a reação do Tribunal foi severa.

A disparidade de abordagens entre os Estados Unidos e a União Europeia, notadamente no que se refere à percepção econômica dos dados pessoais nos EUA, onde são tratados mais como mercadoria do que como aspectos pessoais a serem protegidos, foi destacada. Essa discrepância levou à possibilidade de proibição das transferências de dados pessoais para os Estados Unidos, com base

---

[174] MENEZES, Wagner. *Tribunais internacionais: jurisdição e competência.* São Paulo: Saraiva, 2013.

[175] UNIÃO EUROPEIA. Corte de Justiça da União Europeia. Casos conjuntos C-293/12 e C 594/12. DigitalRights Ireland Ltd. v. Ireland, julgados em 8 de abril de 2014. Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=fi rst&part=1&text=&doclang=PT&cid=513860. Acesso em: 20/11/2023

[176] COMISSÃO EUROPEIA. Decisão 2000/520/CE. Decisão da Comissão de 26 de julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípios de “porto seguro” e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América. Jornal Oficial L 215, 25 de agosto de 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32000D0520. Acesso em: 20/11/2023

no artigo 25 da Diretiva 95/46/CE, que veda transferências para países sem níveis adequados de proteção[177].

Na tentativa de evitar a interrupção no fluxo de dados entre a União Europeia e os Estados Unidos, foi instituído um programa de conformidade. Esse programa envolvia o registro de empresas norte-americanas junto ao Departamento de Comércio dos EUA, exigindo que tais empresas declarassem publicamente sua adesão ao programa, adotassem e apresentassem uma Política de Privacidade em conformidade com as normas da União Europeia e obtivessem certificação anual junto ao Departamento de Comércio[178].

Entretanto, em uma decisão datada de 6 de outubro de 2015, o Tribunal de Justiça da União Europeia invalidou a Decisão 2000/520/CE, motivado por denúncias feitas por Edward Snowden, ex-agente da Agência de Segurança Nacional dos EUA. O Tribunal argumentou que os dados transferidos estavam sujeitos a acesso e processamento pela NSA sem conformidade com os princípios do "Safe Harbour", representando uma grave violação à intimidade dos titulares desses dados. Além disso, destacou a falta de meios para que os indivíduos buscassem seus direitos e protegessem sua intimidade e dados pessoais contra violações ou uso indevido[179].

Após essa decisão, foram iniciadas discussões entre os Estados Unidos e a União Europeia para criar um novo programa que garantisse o intercâmbio de informações. O resultado dessas negociações foi a Decisão de Execução 2016/1250/CE[180], que estabeleceu o programa "*Privacy Shield*" como uma melhoria do anterior.

No entanto, semelhante ao desfecho do "Safe Harbour", um novo processo foi instaurado perante o TJUE para analisar a validade do "*Privacy Shield*", conhecido como "o caso Schrems II". Nesse novo processo, questionava-se não

---

[177] MENEZES, Wagner. *Tribunais internacionais: jurisdição e competência*. São Paulo: Saraiva, 2013.
[178] *Ibidem.*
[179] GREENWALD, G; MACASKILL, E. *NSA Prism program taps in to user data of Apple Google and others.* The Guardian Online, June 7, 2013. Disponível em: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Acesso em: 20/11/2023
[180] UNIÃO EUROPEIA. Decisão de Execução (UE) 2016/1250 da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho. Jornal Oficial L. 207/1, 01 de agosto de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016D1250. Acesso em: 20/11/2023

apenas o programa, mas também o mecanismo de cláusulas contratuais padrão. Em conformidade com o RGPD, o responsável pelo tratamento dos dados pessoais deve assegurar um nível adequado de proteção ao transferir dados para países fora da União, ou, alternativamente, demonstrar que, mesmo em países sem garantias legislativas suficientes, os dados serão protegidos por medidas contratualmente impostas[181].

Assim, a União Europeia estabeleceu conjuntos de Cláusulas Contratuais Padronizadas, aprovadas pela Comissão Europeia, como um meio pelo qual os responsável pelo tratamento podem assegurar a transferência internacional de dados, presumivelmente autorizada e devidamente garantida. Anteriormente, o *Privacy Shield* se baseava no reconhecimento de adequação, onde a Comissão reconhecia que os dados sob o programa recebiam um "nível de proteção adequado", permitindo assim as transferências. No entanto, em outros casos, os responsável pelo tratamento muitas vezes aplicavam as cláusulas-padrão de maneira indiscriminada, sem considerar adequadamente se essas cláusulas eram suficientes para garantir a segurança do tratamento de dados.

O Tribunal de Justiça da União Europeia, ao analisar a reclamação sobre a continuidade dos programas de vigilância estatal nos Estados Unidos, particularmente os baseados no *Foreign Intelligence Surveillance Act* (FISA), concluiu que o *Privacy Shield* não oferecia proteção adequada para transferências internacionais. Isso se deveu à falta de garantias processuais adequadas no FISA, especialmente em relação aos direitos básicos (como o direito de acesso) e à insuficiência dos recursos judiciais disponíveis para abusos desses programas de vigilância.

Além disso, a decisão do tribunal estabeleceu que as cláusulas contratuais padrão aprovadas pela Comissão não eram automaticamente consideradas "garantias adequadas". Em vez disso, sua adequação dependeria da conformidade efetiva com o tratamento específico dos dados em questão. Isso significava que o

[181] COURT OF JUSTICE OF THE EUROPEAN UNION (CJEU). Case C-311/18. Data Protection Commissioner v Facebook Ireland and Maximillian Schrems. Judgment from the Court of Justice of the European Union (CJEU) relating to the transfer of personal data by a private company from a European Union (EU) Member State to a private company in a third country for commercial purposes. It concerns specifically the legality of standard contractual clauses (SCCs) as a mechanism to transfer personal data outside the EU. The judgment became known as the Schrems II judgment. Disponível em: https://www.europeansources.info/record/cjeu-case-c-311-18-data-protection-commissioner-v-facebookireland-and-maximillian-schrems/. Acesso em: 20/11/2023

uso das cláusulas contratuais padrão não mais conferiria automaticamente uma presunção de legalidade às transferências internacionais.

Portanto, a utilização do *Privacy Shield* para fundamentar transferências internacionais não é mais permitida, pois não atende aos requisitos do RGPD, e a eficácia das cláusulas contratuais padrão foi condicionada à sua adequação específica para cada operação, removendo a presunção de legalidade previamente existente.

2.4 Considerações sobre proteção de dados no sistema europeu

As disposições normativas mencionadas representam a base do sistema europeu de proteção de dados pessoais, abrangendo também os subsistemas nacionais. O conjunto de normas supranacionais formado por diretivas, regulamentos e decisões é notável em virtude de sua ambição intrínseca.

Assim, o Regulamento Geral de Proteção de Dados (RGPD) destaca-se como o documento central, visando a proteção no tratamento de qualquer dado pessoal, independentemente de ser automatizado ou não, e tanto na esfera pública quanto privada. Embora existam outros instrumentos normativos de igual relevância, é pertinente salientar que, para os propósitos desta análise, são as disposições do RGPD que estabelecem o parâmetro para comparação com o sistema presente no ordenamento jurídico brasileiro.

É crucial para este estudo compreender a estrutura do conjunto normativo, que permite uma certa segmentação enquanto mantém uma unidade mínima aplicável a todos os setores regulamentares. Dentro dessa estrutura, a Convenção de Estrasburgo de 1981 emerge como a principal fonte dos valores a serem protegidos, ocupando o topo do conjunto e servindo como fundamento filosófico para os demais esforços normativos nessa matéria. Desde o ano 2000, a Carta dos Direitos Fundamentais da União Europeia consolidou sua posição como garantia fundamental da proteção dos dados pessoais, tornando-se parte integral do núcleo axiológico do tema.

Desta feita, quatro aspectos principais demandam atenção para estabelecer pontos comuns de comparação: a amplitude das normativas, as restrições e condições relativas ao tratamento de dados em si, os direitos dos titulares de dados

e o modo de tutela, além das obrigações impostas aos responsáveis pelo tratamento de dados.

2.4.1 Abrangência

Em relação à amplitude, as normas europeias de proteção de dados conseguem abranger uma vasta gama de atividades, tanto de natureza pública quanto privada. Esse alcance é ampliado pela definição aberta do que constitui o tratamento de dados pessoais. Inicialmente, o Regulamento Geral de Proteção de Dados (RGPD) aplica-se ao tratamento de dados pessoais, independentemente de ser realizado por meios automatizados ou não, de forma física ou digital. O conceito de tratamento abrange diversas ações, como discutido anteriormente, considerando qualquer tipo de utilização ou interação com dados pessoais. Da mesma forma, o conceito de dado pessoal, como também mencionado anteriormente, é abrangente e refere-se a qualquer informação relacionada a uma pessoa física identificada ou identificável.

No tocante às exceções à aplicação do RGPD, conforme estabelecido no artigo 2º, estão excluídos os tratamentos realizados pelos Estados-Membros para finalidades ligadas à segurança pública, segurança nacional, persecução penal e fins militares[182]. Além disso, são excluídos os tratamentos efetuados por uma pessoa física para finalidades exclusivamente pessoais ou domésticas. No entanto, é importante ressaltar que essa última exclusão é bastante restrita, abrangendo apenas usos de dados considerados absolutamente comuns. Qualquer desvio dessa norma comum estaria sujeito ao escopo do RGPD, mesmo se realizado por uma pessoa individual.

Quanto ao escopo territorial, a aplicação do RGPD é ampla e pode gerar questões de ordem internacional devido à sua aplicação extraterritorial em certos

[182] UNIÃO EUROPEIA. *Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Art. 2º. Jornal Oficial L. 119/1008, 04 de maio de 2016. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023.

casos[183]. Resumidamente, estão sujeitos ao RGPD: (i) todos os tratamentos ocorridos no território da União ou em locais onde as leis da União são aplicáveis, (ii) todos os tratamentos realizados no contexto da operação de entidades estabelecidas na União, e (iii) todos os tratamentos realizados por entidades estabelecidas fora da União, mas que oferecem bens e serviços a pessoas na União Europeia ou monitoram o comportamento de pessoas localizadas na União Europeia. Destaca-se que essas definições não impõem limitações à aplicação da legislação a tratamentos sem fins lucrativos ou realizados por pessoas individuais, tampouco consideram o tamanho do tratamento ou o faturamento mínimo decorrente dessa operação.

É importante observar que o critério de aplicação considera, em geral, pessoas localizadas na União Europeia, não sendo relevante sua residência ou cidadania. Assim, mesmo uma pessoa que esteja apenas de passagem por esse território tem a garantia de que seus dados serão tratados conforme as disposições do RGPD. Além disso, como mencionado anteriormente, teoricamente, o RGPD pode ser aplicável fora do território da União Europeia, caso uma empresa estabelecida fora desse território, ao oferecer bens e serviços ao mercado europeu, realize o tratamento de dados em conformidade com o Regulamento. Isso evidencia que a preocupação do RGPD é em parte desconsiderar o aspecto territorial, reconhecendo que a eficácia da lei está centrada no tratamento de dados, independentemente do local onde ocorre ou da localização do responsável.

Em relação à aplicação no âmbito dos Estados-membros, distintamente da Diretriz n. 95/46/CE, o RGPD não indica os critérios de determinação do direito interno aplicável em cada caso concreto. Segundo Cordeiro, a omissão de uma norma que possa reger as situações de conflitos, deixa espaço para o surgimento de dúvidas principalmente no que concerne cláusulas de abertura, visto também não ser pacífica a possibilidade de as leis de execução nacionais tomarem tal decisão[184].

---

[183] CORDEIRO, António Barreto Menezes. *Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*. Coimbra: Almedina, 2020. ISBN 978-972-40-8952-2. p. 102

[184] Cordeiro assevera: “Para efeitos de aplicação deste preceito é indiferente se o tratamento em concreto ocorre dentro ou fora do espaço territorial da União, ou seja, o titular dos dados objeto de tratamento não tem de ser cidadão europeu, nem tem de se encontrar em território da União no momento em que o tratamento ocorre. Trata-se de uma decorrência lógico-jurídica do espírito do RGPD e da natureza do direito (fundamental) à proteção de dados.” António Barreto Menezes.

Nesse sentido vale citar a lei n.º 58/2019, de 8 de agosto, através da qual o legislador português assegura a execução, na ordem jurídica interna, do RGPD, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[185]. Cordeiro afirma que o diploma nacional deve ser interpretado à luz do conteúdo do RGPD.[186]

2.4.2. Princípios e condicionantes do Tratamento de Dados

O sistema europeu de proteção de dados apresenta distintivas condicionantes e restrições ao tratamento de dados. Essas restrições são estabelecidas por meio de hipóteses legais que autorizam o tratamento, estando este, em princípio, proibido na ausência de uma hipótese legal aplicável. Além disso, princípios e regras sobre a legalidade do tratamento limitam como o mesmo deve ser conduzido, incluindo sua medida, especificações, finalidades e meios. Em contraste com um sistema simplista, no qual o tratamento é condicional à incidência de uma hipótese legal específica, no sistema europeu, mesmo quando o tratamento é viável, ele pode ser considerado amplamente desleal e, portanto, ilegal.

Um dos principais condicionantes refere-se às bases legais de tratamento, sendo o consentimento do titular dos dados uma delas. Se o titular consente que seus dados sejam coletados e processados, há, em tese, uma base legal para o tratamento. No entanto, a legislação europeia reconhece a limitação do consentimento como uma base legal adequada em todas as situações. Por exemplo, em casos como o de uma vítima de um acidente que chega desacordada a um hospital, o tratamento de dados (abertura de um prontuário médico) é necessário para fornecer o atendimento necessário, mas a vítima pode não estar em condições de consentir conscientemente para o tratamento de seus dados pessoais.

Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019. Coimbra: Almedina, 2020. ISBN 978-972-40-8952-2. p. 102

[185] PORTUGAL. Lei n.º 58/2019, de 08 de Agosto. LEI DA PROTEÇÃO DE DADOS PESSOAIS, 2019. Disponível em https://www.pgdlisboa.pt/leis/ lei_mostra_articulado.php?artigo_id =3118A0001&nid=3118&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=#artigo. Acesso em: 14/01/2024

[186] CORDEIRO, António Barreto Menezes, Op.cit., p. 103

Da mesma forma, a obtenção do consentimento específico de todos os clientes de uma empresa para cumprir suas obrigações legais, como registros de vendas para administração tributária, é desafiadora. O RGPD reconhece, portanto, hipóteses legais que autorizam o tratamento de dados sem depender exclusivamente do consentimento do titular. Isso inclui tratamentos destinados ao cumprimento de obrigações legais, prestação de serviços de saúde e/ou proteção à vida do titular ou de terceiros, exercício regular de direitos (por exemplo, em processos judiciais, nos quais não é razoável esperar autorização da parte contraposta) e execução de um contrato.

Além disso, uma consideração relevante no contexto da comparação a ser efetuada é a hipótese do Interesse Legítimo[187]. Conforme delineado pelo RGPD, é permitido ao responsável pelo tratamento de dados processar informações pessoais quando houver um interesse legítimo considerável, desde que tal processamento não cause desproporcional prejuízo aos direitos fundamentais do titular dos dados. O legislador, ao adotar essa abordagem, demanda essencialmente uma análise de proporcionalidade entre o interesse do responsável pelo tratamento e os direitos do titular, assegurando que o tratamento proposto seja equitativo.

A amplitude do interesse legítimo se justifica pela necessidade de adaptar o sistema a situações não antecipadas na elaboração do Regulamento. Contudo, é importante observar que, devido à sua flexibilidade, o interesse legítimo é criteriosamente monitorado pelas autoridades, com o intuito de regulamentar seu emprego e restringir suas aplicações, evitando prejudicar injustamente os titulares de dados.

Além da avaliação da viabilidade do tratamento, é imperativo considerar as restrições e condições aplicáveis à forma como os dados são processados. Nesse contexto, os princípios de proteção de dados, desempenham um papel crucial, pois impões limitações à maneira como os dados são tratados. Os princípios, contidos

[187] UNIÃO EUROPEIA. *Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Art. 6º. Jornal Oficial L. 119/1008, 04 de maio de 2016. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023.

no art. 5º do RGPD são: i) licitude, lealdade e transparência; ii) limitação das finalidades; iii) minimização dos dados; iv) exatidão; v) limitação conservação; vi) integridade e confidencialidade; vii) responsabilidade[188].

O princípio da licitude, lealdade e transparência estabelece que o tratamento de dados deve ser feito de acordo com os regramentos da RGPD e demais legislações aplicáveis[189], a lealdade como conceito aberto confere mais amplitude à licitude, e impõe limitações à comportamentos contrários aos interesses do titular e ao espírito do RGPD, e a transparência, por sua vez engloba a comunicação tanto do conteúdo das informações, quanto como os procedimentos da transmissão[190].

O princípio da limitação da finalidade estabelece que os dados devem ser processados para finalidades legítimas, específicas e explicitamente comunicadas ao titular. É vedado o tratamento posteriormente de uma forma incompatível com a finalidade previamente informada[191].

O princípio da minimização dos dados estipula que o dado só pode ser tratado se for adequado, necessário e pertinente[192] para alcançar a finalidade definida. Já o princípio da exatidão[193] veda o armazenamento de dados inexatos, e estabelece a atualização ou o apagamento dos mesmos sempre que necessário.

No princípio da limitação da conservação[194] é imposto, com exceções, que os dados devem ser conservados de uma forma que permita a identificação dos titulares dos dados estritamente durante a janela temporal necessária para as finalidades para as quais são tratados.

---

188 UNIÃO EUROPEIA. *Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Art. 5º. Jornal Oficial L. 119/1008, 04 de maio de 2016. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023.

189 CORDEIRO, António Barreto Menezes. *Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*. Coimbra: Almedina, 2020. ISBN 978-972-40-8952-2. p. 152.

190 FRENZEL Apud CORDEIRO, António Barreto Menezes. Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019. Coimbra: Almedina, 2020. ISBN 978-972-40-8952-2. p. 154.

191 UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE Regulamento Geral sobre a Proteção de Dados). Jornal Oficial L. 119/1008, 04 de maio de 2016. Art. 5º. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023.

192 CORDEIRO, António Barreto Menezes. *Op. cit.* p. 159.

193 UNIÃO EUROPEIA. *Op. cit.* Art. 5º.

194 Ibidem.

O princípio da integridade e confidencialidade impõe o tratamento de forma segura, com as medidas técnicas adequadas, e o princípio da responsabilidade atribui ao responsável a responsabilidade em duas dimensões, como afirma o prof. Dr. Cordeiro Menezes, vejamos: *"[...] O preceito prevê dois deveres distintos: (i) o responsável pelo tratamento deve atuar sempre no estrito cumprimento dos princípios elencados no artigo 5.o/1; e (ii) o responsável pelo tratamento deve conseguir demonstrar, maxime às autoridades de controlo e aos tribunais, o cumprimento desses mesmos princípios."*[195]

Estes princípios, relevantes não apenas para o RGPD, têm importância central especialmente quando em comparação com a Lei Geral de Proteção de Dados brasileira. Se por um lado os princípios constituem um desafio prático considerável na precisa gestão das finalidades e informações fornecidas para evitar uso e manipulação descabida, por outro viés oferecem as diretrizes necessárias que possibilitam a realização do tratamento de dados no sistema europeu.

2.4.3. Direitos do titular e tutela

A salvaguarda dos direitos do titular de dados representa um dos pilares fundamentais da legislação referente à proteção de dados pessoais na União Europeia. Como discutido anteriormente, mesmo os direitos de acesso e retificação foram consagrados como direitos fundamentais, incorporados no artigo 8º da Carta de Direitos Fundamentais da União Europeia.

Os direitos do titular são assegurados principalmente pelo artigo 8º da Carta, pelo artigo 9º da Convenção de Estrasburgo e pelo capítulo III do Regulamento Geral de Proteção de Dados (RGPD). Dentre esses, o capítulo III do RGPD se destaca por fornecer uma abordagem mais minuciosa desses direitos, englobando até mesmo aqueles garantidos pelos outros dois instrumentos jurídicos. Nossa análise se concentrará, portanto, no capítulo III do RGPD.

Uma primeira ênfase desses direitos diz respeito à informação sobre o tratamento de dados. O RGPD estabelece critérios detalhados sobre quais informações devem ser comunicadas ao titular, seja quando o tratamento de dados

---

[195] CORDEIRO, António Barreto Menezes. *Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*. Coimbra: Almedina, 2020. ISBN 978-972-40-8952-2. p.161.

pessoais ocorre imediatamente após a coleta direta dos dados pelo próprio titular (por exemplo, através de um questionário ou formulário de cadastro), ou quando os dados são obtidos de terceiros que tiveram contato prévio com o titular. Isso se aplica, por exemplo, a uma empresa que adquire dados de outra empresa que teve contato direto com o titular.

Desse modo, mesmo em casos de coleta indireta, a primeira empresa, que não teve contato direto com o titular, deve disponibilizar meios para que este obtenha informações detalhadas sobre o tratamento, podendo incluir a divulgação pública dessas informações[196].

A legislação não apenas estipula que o responsável pelo tratamento deve fornecer informações, mas também determina o conteúdo dessa comunicação. Em suma, o responsável pelo tratamento é obrigado a informar: (i) a identidade e os detalhes de contato do responsável pelo tratamento, (ii) as informações de contato do encarregado de proteção de dados, (iii) os propósitos e fundamentos jurídicos do tratamento, (iv) os dados efetivamente processados, (v) os destinatários dos dados pessoais, quando compartilhados, (vi) detalhes sobre a transferência internacional de dados, (vii) o período de retenção dos dados pessoais, (viii) os direitos garantidos ao titular dos dados, (ix) se o tratamento e compartilhamento de dados resultam de uma obrigação legal ou contratual, e (x) se o titular estará sujeito a decisões automatizadas, incluindo a definição de perfis, com informações relevantes sobre os critérios dessas decisões automatizadas[197].

Desse modo, o direito de acesso, assemelhando-se ao direito à informação, viabiliza que o titular tenha acesso não apenas aos dados efetivamente tratados, mas também a informações abrangentes sobre o tratamento em geral, incluindo aquelas mencionadas anteriormente e a origem dos dados, caso não tenham sido diretamente obtidos do titular. Este direito é fundamental para a autodeterminação informática, pois permite ao titular, de maneira informada e ponderada, avaliar a licitude do tratamento, decidir sobre a apresentação de reclamações ao

[196] UNIÃO EUROPEIA. *Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Jornal Oficial L. 119/1008, 04 de maio de 2016. Art. 14. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023

[197] *Ibidem*.

responsável ou à autoridade de supervisão, e optar por exercer outros direitos garantidos pela legislação.

Além do direito de acesso, são garantidos acessoriamente os direitos de eliminação e correção. O direito de correção concede ao titular a prerrogativa de atualizar ou corrigir dados incorretos sobre si, enquanto o direito de eliminação permite solicitar o apagamento de dados pessoais em circunstâncias específicas, respeitando as limitações legais e não sendo um direito absoluto.

Dentre outros direitos assegurados pela legislação da União Europeia, incluem-se o direito à restrição ao tratamento de dados, geralmente aplicável em situações de decisões pendentes sobre o tratamento em razão de reclamação ou solicitação do titular, o direito à portabilidade de dados, que possibilita a transferência de dados pessoais a outro prestador de serviços, o direito de oposição ao tratamento para certas finalidades como e-mail marketing, e o direito de se opor a decisões automatizadas, requerendo que decisões não se baseiem exclusivamente no tratamento automatizado de dados pessoais.

A diversidade de direitos consagrados pela legislação denota um fortalecimento da autocomposição para a resolução de conflitos, atribuindo ao titular a responsabilidade primordial de fiscalizar o uso de seus dados. Este papel contribui para a autodeterminação informativa, capacitando o titular com os instrumentos necessários para tomar decisões informadas sobre seus dados pessoais. Embora a via judicial não seja obrigatória, é preferível, inclusive para o titular, que certas demandas sejam inicialmente tratadas de forma particular, permitindo a resolução eficiente de conflitos. Esse mecanismo requer que o responsável pelo tratamento exponha sua justificativa para o tratamento em análise.

Na ausência desses direitos, o responsável não teria a obrigação legal de responder a uma solicitação do titular, conferindo-lhe vantagens em uma possível demanda judicial ou administrativa. Quando esses direitos são garantidos, o responsável não apenas deve responder em prazo determinado, mas sua justificativa vincula suas estratégias de defesa.

Assim, a garantia de direitos ao titular é uma ferramenta crucial para assegurar o cumprimento adequado das obrigações de tratamento e a resposta correta às solicitações, sendo uma fonte de responsabilidade e prestação de

contas. Esses direitos também capacitam o titular a obter informações sobre tratamentos irregulares e submetê-las ao escrutínio das autoridades, tornando-se essenciais para a efetividade da tutela de direitos no âmbito do Regulamento Geral de Proteção de Dados (RGPD).

2.4.4. Responsabilidade, *accountability* e segurança

Em última análise, e de maneira igualmente significativa, é imperativo destacar as responsabilidades relacionadas à responsabilização dos responsáveis pelo tratamento, prestação de contas (*accountability*) e segurança dos dados. Em um primeiro contexto, os responsáveis pelo tratamento, comumente referidos como agentes de tratamento, assumem papéis distintos como responsável pelo tratamento (controlador) ou subcontratante (operador)[198].

O responsável pelo tratamento, de forma simplificada, é a entidade primariamente responsável pelo tratamento, determinando finalidades e meios, além de colher possíveis benefícios advindos do tratamento de dados.[199]

O subcontratante, por outro lado, é a entidade que executa o tratamento, estritamente sob as diretrizes do responsável pelo tratamento. Essa distinção é crucial, pois influencia as responsabilidades contratuais em situações como vazamento de dados.

O impacto prático dessa diferenciação é evidenciado na necessidade dos responsável pelo tratamento estabelecerem relações contratuais detalhadas para assegurar que as ações dos subcontratantes estejam sempre em conformidade com a legislação. Uma prática decorrente do Regulamento Geral de Proteção de Dados (RGPD), por exemplo, é a negociação de cláusulas robustas de proteção de

---

[198] O art. 4º do RGPD dispõe sobre o assunto. Em inglês os termos utilizados são “controller” e “processor”. Traduzidos como “responsável pelo tratamento” ou “controlador” e “subcontratante” ou “operador”. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023

[199] UNIÃO EUROPEIA. *Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Jornal Oficial L. 119/1008, 04 de maio de 2016. Art. 4º. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023

dados, mesmo quando não explicitamente exigidas por lei, tornando-se uma prática comum em diversos países, inclusive no Brasil[200].

Esse impacto também se manifesta nos princípios de *accountability*. O RGPD estipula não apenas que os agentes de tratamento devem obedecer à lei, mas também devem fazer esforços ativos para demonstrar tal conformidade. Essa responsabilização pós-fato surge da transição de um sistema que demandava autorização prévia para o tratamento de dados para um modelo de controle posterior, onde a conformidade com a lei é predominantemente fiscalizada após o início do tratamento de dados.

A obrigação de *accountability* evoluiu para abranger programas complexos de governança em dados pessoais, assemelhando-se a programas de compliance anti-corrupção, que incluem o estabelecimento de políticas internas sobre tratamento de dados, práticas contratuais responsáveis, treinamento contínuo dos colaboradores e gestão proativa de riscos em proteção de dados.

Por fim, e não menos relevante, encontram-se as obrigações de segurança dos dados. O RGPD, seguindo a linha da Diretiva de Proteção de Dados, adotou uma abordagem similar quanto à segurança dos dados pessoais. Reconhecendo a constante evolução do campo tecnológico relacionado à proteção de dados, a legislação procura ser tecnicamente neutra.

Assim, o RGPD estabelece que os agentes de tratamento devem adotar as medidas adequadas, sejam técnicas, físicas ou administrativas, para garantir a segurança dos dados[201]. Embora não detalhe medidas específicas, o regulamento fornece critérios a serem considerados, incluindo a confidencialidade, integridade, disponibilidade e resiliência dos dados, bem como as características e riscos do tratamento, a tecnologia disponível e os custos associados.

---

[200] Sobre este assunto, confira-se: ALVES, Carla Segala; GUIDI, Guilherme Berti de Campos. *Cláusulas contratuais e dados pessoais: controladores, operadores, cocontroladores e transferências internacionais*. In: BLUM, R.O.; VAINZOF, R.; MORAES, H.F. Data protection officer (encarregado): teoria e prática de acordo com a LGPD e o RGPD. São Paulo: Thomson Reuters Brasil, 2020.

[201] UNIÃO EUROPEIA. *Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Jornal Oficial L. 119/1008, 04 de maio de 2016. Art. 22. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023

Essa flexibilidade é um aspecto notável, alinhando-se às práticas estabelecidas no campo da segurança da informação em relação à gestão de riscos de segurança.

2.5 Dados sensíveis, e a proteção à saúde no RGPD

O Regulamento Geral de Proteção de Dados distingue os dados sensíveis[202] dos demais dados. Isto pois, os dados sensíveis se distinguem dos demais na medida em que por possuir uma natureza especialmente sensível em relação a direitos e liberdades fundamentais, no contexto do seu tratamento, podem implicar riscos para os direitos e liberdades fundamentais[203].

Em relação a esses dados, têm-se que, por regra geral, eles não devem ser objeto de tratamento, salvo se a operação for permitida em casos específicos presente no próprio regulamento, ou nos regramentos dos estados-membro, que podem determinar condições específicas com fins de adaptação para cumprimento de obrigação legal, ou exercício de funções de interesse público, ou exercício de autoridade pública[204].

A natureza dos dados sensíveis é esclarecida pelo art. 9º, que consagra dois grandes blocos, primeiramente os *"dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical"*[205], assim como os *"dados genéticos, dados biométricos para efeitos de identificação exclusiva de uma pessoa singular, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa singular"*[206].

---

[202] Cordeiro afirma que o legislador europeu "dados sensíveis" ou "dados especiais" indistintamente, como sinónimos. CORDEIRO, António Barreto Menezes. *Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*. Coimbra: Almedina, 2020. ISBN 978-972-40-8952-2. 132.

[203] UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Considerando 51. Jornal Oficial L. 119/1008, 04 de maio de 2016. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023

[204] UNIÃO EUROPEIA, *op. Cit*., art. 9º.

[205] *Ibidem.*

[206] *Ibidem*.

Cordeiro admoesta que a escolha dessa categoria de dados não é arbitrária, mas que por si reconhece a soberania da proibição da não discriminação, constante no art. 21 da Carta, bem como no art. 26/1 da CRP. Além disso, afirma também que esse raciocínio se fortalece a medida em que se leva em consideração a natureza do direito envolvido, o qual poderia colocar em uma situação de vulnerabilidade extrema o titular dos dados, além dos possíveis impactos prejudiciais que poderiam resultar do seu tratamento[207].

2.5.1 Dados relativos à saúde

Desta feita, tendo em vista o escopo do presente trabalho, a seguir serão apresentados esclarecimentos mais pormenorizados acerca dos dados sensíveis relativos à saúde.

O art. 4º define dados relativos à saúde como *"todos os dados que facultam informações sobre a saúde física ou mental de uma pessoa singular*"[208].Nessa esteira, à luz da jurisprudência do TJEU deve-se conferir sentido lato a expressão. No caso *Lindqvist*[209], relacionado à violação de dados pessoais, o Tribunal de Justiça considerou que a expressão "dados relativos à saúde' deve ser objeto de uma interpretação ampla, de modo a incluir informações relativas a todos os aspectos, tanto da saúde física como mental de um indivíduo. Nessa oportunidade, a referência ao fato de uma pessoa ter lesionado o pé foi considerado um dado pessoal relativo à saúde.

O art. 4º é complementado também pelo considerando 35, que detalha e exemplifica elementos que são considerados dados pessoais relativos à saúde, a saber todos os dados relativos ao estado de saúde de um titular que revelem

---

[207] CORDEIRO, António Barreto Menezes. *Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*. Coimbra: Almedina, 2020. ISBN 978-972-40-8952-2. p. 133.
[208] UNIÃO EUROPEIA, *op. Cit*., art. 4º.
[209] O caso referenciado foi remetido pelo Tribunal de Recurso de Gota (Suécia) ao Tribunal de Justiça Europeu para uma decisão sobre questões relativas ao âmbito e à interpretação da Diretiva de Proteção de Dados. O caso dizia respeito ao processo penal contra a Sra. *Lindqvist*, que foi acusada de violação da legislação sueca sobre a proteção de dados pessoais por manter uma página na Internet contendo informações de seus colegas sem o seu consentimento. Disponível em Bodil Lindqvist (ccgnlud.org). Acesso em 10/01/2024.

informações sobre "a sua *saúde física ou mental no passado, no presente ou no futuro"*[210]. A definição também inclui:

> "as informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação, conforme referido na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho (9), a essa pessoa singular; qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro."[211]

Cabe ressaltar ainda que, diretamente associados aos dados relativos à saúde, também estão os dados genéticos, que são protegidos da mesma maneira. O regramento afirma que eles são *"os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa"*[212], e o considerando 34 ainda completa dispondo que a amostra em questão é "*nomeadamente da análise de cromossomas, ácido desoxirribonucleico (ADN) ou ácido ribonucleico (ARN), ou da análise de um outro elemento que permita obter informações equivalentes"* [213].

2.5.2 O Tratamento dos dados sensíveis

[210]UNIÃO EUROPEIA. *Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Considerando 51. Jornal Oficial L. 119/1008, 04 de maio de 2016. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023

[211] UNIÃO EUROPEIA, *op. Cit*., considerando 35.

[212] UNIÃO EUROPEIA, *op. Cit*., art. 4º.

[213] UNIÃO EUROPEIA, *op. Cit.*, considerando 34.

Apesar de ser categórico ao se referir que é expressamente proibido o tratamento de dados relativos à saúde, há uma série de exceções que podem se verificar nos mais diversos casos. A primeira delas, constante na alínea a) do artigo 9º é no caso de consentimento explícito. É necessário que o consentimento seja livre, informado, específico, e inequívoco, além disso, ele tem que poder ser retirado a qualquer momento, sem prejuízos para o titular. Gonçalves[214] afirma que no contexto da saúde pública a avaliação de consentimento livre necessita ser realizada cautelosamente, visto que há potencial de consequências negativas significativas quando os titulares de dados recusam a dar o seu consentimento, e o consentimento sob ameaça de não tratamento não pode ser considerado um consentimento livre.

Outra exceção, prevista na alínea b), é quando o tratamento é indispensável para o cumprimento de obrigações, bem como o exercício de direitos específicos do responsável pelo tratamento, ou do titular dos dados em matéria de legislação laboral, segurança social e de proteção social. Isso tudo na medida em que permitido pelo direito, ou por convenção coletiva.

Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou, de outra pessoa singular, no caso do titular está incapacitado de dar os seus consentimentos, também é possível realizar o tratamento de dados relativos à saúde[215]. O tratamento de dados pessoais com base no interesse vital de outra pessoa só é possível quando ele não puder se fundamentar em qualquer outro fundamento jurídico[216], do que só é aplicável em casos muito vitais, como por exemplo caso em que o titular dos dados está inconsciente e é necessário o acesso aos dados a fim de saber informações acerca de alergias a medicamentos que podem ser vitalmente decisivos no sucesso do tratamento, deve-se considerar também a existência de representantes legais que poderia suprir a falta de

---

[214] GONÇALVES, Anabela Susana de Sousa. *O tratamento de dados pessoais relativos à saúde no âmbito do RGPD. Cidades Inteligentes e Direito, Governação Digital e Direitos.* Coimbra: Almedina, p. 251-269, nov. 2023 978-989-40-1598-7. P. 260.

[215] UNIÃO EUROPEIA. *Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Jornal Oficial L. 119/1008, 04 de maio de 2016. art. 9º, alínea c. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023.

[216] UNIÃO EUROPEIA, *op. Cit*, considerando 46.

consentimento do titular[217] . Cordeiro afirma que a necessidade deve ser medida no sentido em que a não realização do tratamento levará, ou não impedirá a produção de danos gravosos[218].

A alínea d) do art. 9º cita uma derrogação no âmbito de atividades legítimas por uma fundação viva associação ou qualquer outro organismo sem fins lucrativos. Para tanto os dados devem ser dos membros, antigos ou atuais, ou pessoas que mantenham contatos com estas entidades, possivelmente doadores ou voluntários.

Quando os dados forem manifestamente tornados públicos pelo próprio titular o tratamento também é permitido. Isso pois, quando decidida pelo próprio titular tal divulgação pública é interpretada como uma renúncia a proteção do artigo nono. Afinal se o próprio titular reconhece que é exposição viro e o tratamento desses dados não lhe é prejudicial não há porquê a proteção ser perpetuada imotivadamente[219]. Cabe ressaltar nesse ponto, toca-se apenas nas manifestações tornadas públicas pelo próprio titular, partindo de uma decisão livre e esclarecida do mesmo, e não difundidas por terceiros.

Outra exceção é a necessidade do tratamento para defesa dos direitos em processo judicial, ou sempre que os tribunais atuem no exercício das suas funções jurisdicionais[220]. A alínea g) do art. 9º também dispõe acerca da possibilidade do tratamento de dados relativos à saúde quando a motivação for interesse público importante, sempre que previstos na legislação europeia ou nacional. Além disso é mister que seja proporcional ao objetivo, preveja medidas adequadas e específicas que salvaguardem os direitos e interesses dos titulares de dados, e respeite o direito à autodeterminação informacional. Segundo Gonçalves, proporcionalidade nesse caso é sempre que não houver outra medida menos prejudicial[221]. Destaca-

---

[217] WEICHERT, Anotação ao artigo 9.o do RGPD em *Kühling/Buchner*, Rn. 68. *Apud*, CORDEIRO, António Barreto Menezes. Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019. p. 243.

[218] CORDEIRO, António Barreto Menezes. *Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*. Coimbra: Almedina, 2020. ISBN 978-972-40-8952-2, p. 243.

[219] *Ibidem*, p. 245.

[220] UNIÃO EUROPEIA. *Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Jornal Oficial L. 119/1008, 04 de maio de 2016. art. 9º, alínea g. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023.

[221] GONÇALVES, Anabela Susana de Sousa, *O tratamento de dados pessoais relativos à saúde no âmbito do RGPD. Cidades Inteligentes e Direito, Governação Digital e Direitos.* Coimbra: Almedina, p. 251-269, nov. 2023 978-989-40-1598-7.p. 260.

se que o processamento de dados sensíveis com base em interesses públicos significativos pode ser estabelecido pelo Direito da União Europeia ou pelas legislações internas dos Estados-Membros. Cordeiro, por sua vez, afirma que, nesses casos, devido à natureza especial desses dados sensíveis, é necessário um cuidado especial durante a elaboração legislativa correspondente, o que inclui esclarecimentos detalhados sobre o interesse público específico que está sendo buscado e a identificação precisa dos dados que serão objeto desse tratamento[222].

Também pode-se justificar o tratamento de dados pessoais relacionado à saúde justamente em situações de "*necessidade para fins de cuidados médicos ou sociais que devem ser necessariamente para: medicina preventiva; medicina ocupacional; diagnóstico médico; prestação de cuidados ou tratamentos de saúde ou de ação social; gestão de sistemas e serviços de saúde; ação social com base no direito da união ou dos estados-membros"[223].* A referida exceção também comporta os casos de tratamento por força de um contrato com o profissional de saúde, sendo que só podem ser tratados por esse fim se o profissional estiver legalmente sujeito obrigação de sigilo profissional, ou uma obrigação de confidencialidade[224].

À alínea i) do artigo nono afirma que o tratamento se for necessário por motivos de interesse público no domínio da saúde pública, ainda exemplifica citando a proteção contra ameaças transfronteiriças as graves para a saúde, a exemplo da pandemia de COVID-19, ou para assegurar o elev.ado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos. O conceito de saúde é definido no 3.o/1, c) do Regulamento (CE) n.o 1338/2008, de 16 de dezembro como:

> "Todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o

[222] CORDEIRO, António Barreto Menezes. *Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*. Coimbra: Almedina, 2020. ISBN 978-972-40-8952-2, p. 246.
[223]UNIÃO EUROPEIA. *Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Jornal Oficial L. 119/1008, 04 de maio de 2016. art. 9º, alínea h. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023.
[224] UNIÃO EUROPEIA, op. Cit, art. 9º/3.

> acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade."[225]

Segundo cordeiro é necessário que se compreenda que apesar de qualquer um desses elementos justificar o tratamento de dados sensíveis é estritamente necessário que ele seja motivado por interesse público[226].

Por fim é possível realizar o tratamento se indispensável para fins de arquivo de interesse público, investigação científica ou histórica ou para fins estatísticos[227]. Ressalta o princípio da necessidade e o da proporcionalidade na medida em que o tratamento deve ser necessário e proporcional ao objetivo visado. Sendo que está sujeito as garantias adequadas querem seguramente medidas técnicas e organizativas a fim de assegurar o respeito do princípio da minimização dos dados, ou seja, os dados a tratar devem ser adequados, pertinentes e limitados ao que é exigido pelas finalidades que determinam o tratamento[228].

Insta ressaltar que em relação aos dados genéticos e relativos à saúde os estados membros podem manter ou estabelecer novas condições e até mesmo limitações[229]. Gonçalves afirma que devido a natureza dos dados, é justificável a possibilidade dos estados membros conferem proteções adicionais ao seu tratamento, apesar disso, se revela incoerente pois autoriza demasiada fragmentação decorrente dos diferentes níveis de proteção de dados, conferida por cada estado membro[230].

É importante ressaltar que, apesar das considerações realizadas, o objetivo aqui não é apresentar um histórico normativo completo e detalhado, visto que isso

---

225 UNIÃO EUROPEIA. *Regulation (ec) no 1338/2008 of the european parliament and of the council* of 16 December 2008 on Community statistics on public health and health and safety at work (Text with EEA relevance). [s.l: s.n.]. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R1338&from=PT. Acesso em: 20 jan. 2024.

226 CORDEIRO, António Barreto Menezes. *Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*. Coimbra: Almedina, 2020. ISBN 978-972-40-8952-2, p. 247.

227 UNIÃO EUROPEIA. *Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Jornal Oficial L. 119/1008, 04 de maio de 2016. art. 9º, alínea j. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023.

228 UNIÃO EUROPEIA, *op. Cit*, Art. 89.

229 UNIÃO EUROPEIA, *op. Cit*, art. 9º, alínea

230 GONÇALVES, Anabela Susana de Sousa, *O tratamento de dados pessoais relativos à saúde no âmbito do RGPD. Cidades Inteligentes e Direito, Governação Digital e Direitos.* Coimbra: Almedina, p. 251-269, nov. 2023 978-989-40-1598-7.p. 268.

já foi realizado em inúmeras obras, mas estabelecer as bases para demonstrar que foram essas regulações estabeleceram um mecanismo capaz de estabelecer limites no processamento de dados pessoais na crise de saúde pública da Covid-19, permitindo tanto que se evitasse resultados negativos em relação à pandemia, quanto a proteção de direitos fundamentais.

3. EVOLUÇÃO DO DIREITO DE PRIVACIDADE NA ESTRUTURA CONSTITUCIONAL BRASILEIRA

O objetivo deste capítulo é fazer uma breve descrição do desenvolvimento da proteção de dados pessoais no Brasil, que possui como importante marco legal a Lei Geral de Proteção de Dados Pessoais LGPD, conforme será demonstrado nas subseções a seguir.

3.1 Principais especificidades sobre dados pessoais e categoriais especiais de informação

A importância da proteção legal dos dados pessoais reside no fato de que tanto esses como outros dados deles obtidos quase representam uma pessoa perante a sociedade, o que representa uma parte real de sua personalidade. Portanto, embora nem sempre de uso prático óbvio, uma explicação da diferença entre os conceitos de dados pessoais e informações pessoais pode ser útil para uma discussão aprofundada sobre o assunto.[231]

3.1.1 Dados pessoais X Informações pessoais

Quando se utilizam os termos dados pessoais e informações pessoais, é inegável que os dois se sobrepõem em diferentes circunstâncias e representam certos aspectos do fato, da realidade. Em termos de detalhes, dados podem ser vistos como um termo primitivo e fragmentado, que pode ser entendido como

[231] BOFF, Salete Oro; FORTES, Vinícius Borges. *A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil.* Sequência (Florianópolis) [online]. 2014, n.68.

informação em estado potencial, que se torna informação somente quando é transmitida, recebida e compreendida.[232]

Segundo Souza[233], esse conhecimento é anterior ao processo interpretativo e criativo. Assim, aparece como uma conjuntura de eventos, ações humanas que tendem a mudar as pessoas, conteúdos, entre outras coisas, segundo a personalidade, afetividade.

Normalmente, os objetos devem ser identificados ou pelo menos identificáveis, mas nem sempre é esse o caso, por exemplo, nos casos em que a informação se refere a pessoas de natureza não especificada. Em tais situações, segundo Souza:

> As informações são mantidas anônimas e utilizadas para fins estatísticos e protegem as pessoas cujas informações foram previamente coletadas e armazenadas. Ressalta-se que, por serem esses dados anônimos e tratados de forma a impossibilitar a identificação, deixam de estar sujeitos à disciplina e proteção da proteção de dados pessoais, uma vez que não violam a natureza protetiva desse direito: a privacidade e personalidade humana.[234]

Dados pessoais são algo que vão além de seu mero conteúdo e requerem um procedimento prévio para sua análise. Eles podem ser compartilhados de inúmeras formas, sejam fotos, vídeos, e diversas situações, inclusive coisas relacionadas a valores.[235]

Com base na Convenção de Strasbourg, uma boa forma de conceituar a terminologia seria a seguinte: "qualquer informação sobre uma pessoa natural identificada ou identificável".[236]

Desse modo as informações pessoais, diferem das demais por um viés mais objetivo entre o indivíduo e as informações relevantes, independentemente das questões que lhes dizem respeito. Segundo Doneda[237], essa conexão subjetiva

---

[232] CAVALCANTI, José Carlos. *"The new ABC of ICTs (analytics +big data + cloud computing: a complex trade-off between IT and CT costs"*. Hershey: IG Global, 2016.
[233] SOUZA, Carlos Affonso Pereira de. *Contornos atuais do direito à imagem*. Brasília: Fundação Getúlio Vargas, 2018.p.42
[234] *Ibidem.*
[235] GARCIA, Lara Rocha. Lei Geral de Proteção de Dados Pessoais (LGPD: guia de implantação. São Paulo: Edgard Blücher Ltda, 2020.
[236] SOUZA, Carlos Affonso Pereira de. *Op. cit.*p.42
[237] DONEDA, Danilo. *A proteção de dados pessoais como direito fundamental.* Revista Espaço Jurídico 12/103. Joaçaba: Unoese, 2011. P. 98

seria “além de outras categorias de informações que, embora possam ter alguma relação com a pessoa, não seriam exatamente informações pessoais”

Diante disso, é muito importante esclarecer que o objetivo da proteção de dados ou informações pessoais é proteger a pessoa e sua personalidade, e não o dano em si.[238]

Com isso em mente, o tópico a seguir discute categorias de dados específicas que representam uma categoria de dados que representa uma ameaça maior à personalidade do indivíduo.

3.1.2 Categorias especiais de informação: eventuais riscos de discriminação

A análise desta categoria de dados desenvolve-se a partir do conhecimento de que o tratamento de determinados dados pode constituir uma ameaça maior, e mais grave, à personalidade e à liberdade da pessoa do que outros, o que pode conduzir a uma nova questão de igualdade, que se fora infringida pode levar a ações potencialmente discriminatórias, por exemplo.[239]

A questão é tratada de forma diferenciada nas normativas, além de costumar vir acompanhada de normativas gradativamente mais rígidas, visando a melhor proteção dos cidadãos e da sociedade.[240]

É muito importante proteger todo tipo de informação, mesmo aquelas que não são consideradas tão importantes, pois mesmo que pareça algo insignificante, pode se tornar sensível ao longo do tempo.[241]

Nesse sentido, Oliveira[242] acrescenta que: “É com tratamento de dados sensíveis que é capaz de transformar dados inofensivos em dados potencialmente

---

[238] CAVALCANTI, Natália Peppi; SANTOS, Luiza Mendonça da Silva Belo. *A lei geral de proteção de dados do brasil na era da big data.* In: Tecnologia Jurídica & Direito Digital - II Congresso Internacional de Direito, Governo e Tecnologia, 2., 2018, Belo Horizonte. Anais [...]. Belo Horizonte: Fórum, 2018, v.1, p. 351-366.

[239] BOFF, Salete Oro; FORTES, Vinícius Borges. *A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil.* Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2013v35n68p109/26949. Acesso em: 04/01/2024. P.120.

[240] DONEDA, Danilo. *Op.cit*.,p.100.

[241] BOFF, Salete Oro; FORTES, Vinícius Borges. *Op. cit., p.122.*

[242] OLIVEIRA, Ana Paula de. *A LGPD brasileira na prática empresarial*. Revista Jurídica da Escola Superior de Advocacia da OAB-PR, ano 4, n.1, p. 172-200, 2019.

discriminatórios". Segundo Martins[243], "informações insignificantes podem adquirir um novo valor. Dessa forma, deixarão de ser gerados dados irrelevantes no tratamento eletrônico de dados. "

Certamente não deveria haver proibição absoluta de acesso e uso de dados pessoais, pois tal prática colocaria em risco a segurança necessária para a execução das ações judiciais e seria contrário à autonomia da negociação. Não só nestes casos, mas também quando a utilização é legal e necessária, por exemplo em atividades de investigação ou mesmo médicas, não cabe a recusa total no tratamento de dados pessoais.[244]

Por último, importa ressaltar que, como já abordado nesse trabalho, o artigo 6.º do RGPD (Regulamento Geral de Proteção de Dados), que regula a matéria na União Europeia, não impede a plena utilização desta informação, apenas em alguns casos.

Nesse sentido, merecem discriminação específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Além disso, deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, questões relacionadas a sexualidade, bem como ao direito a saúde, pontos que serão mais profundamente abordados no capítulo 4 desta pesquisa.

3.2 Evolução da proteção de dados no brasil

A respeito do contexto da proteção à privacidade no Brasil, Salete Oro Boff e Vinicius Borges Fortes[245], no texto "A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil", explicam a evolução da tecnologia principalmente na questão da comunicação e informação, também analisam sob a realidade brasileira, as legislações, marcos pontos de princípio de

[243] MARTINS, Guilherme Magalhães. *O direito ao esquecimento na Internet*. In: Direito Privado e Internet. Coord: Guilherme Magalhães Martins. São Paulo: Editora Atlas, 2014.
[244] *Idem.*
[245] BOFF, Salete Oro; FORTES, Vinícius Borges. *A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil*. Sequência (Florianópolis) [online]. 2014, n.68

proteção ,como instrumentos normativos e controle da distribuição das informações pessoais, visando o asseguramento de proteção de forma jurídica aos direitos a privacidade e inviolabilidade dos dados.

Os autores com a proposta de pesquisa no Brasil, país que deu, tardiamente, a devida relevância sociocultural, jurídica para esse tema de privacidade em contemporaneidade com o advento de novas tecnologias e de que forma deve ser feita a proteção jurídica do direito à privacidade e proteção dos dados, as principais propostas e instrumentos, contextualização e delimitar as dimensões das violações desses direitos para o estudo.[246]

Com o conceito de ciberespaço, para noções de base do estudo, sociedade da informação, demonstra o histórico do surgimento da internet, com base em estudos e pesquisas de novas formas de comunicação e informação, a criação dos primeiros softwares para navegação nas World Wide Web, por conta da Guerra Fria, onde não há um confronto direto, mas de guerra de informações, narrativas ideológicas. Com o tempo, finda a guerra fria, ocorreu uma democratização da informação, o acesso a população e processos de inclusão digital para a população e citam, por reflexos pela chegada das novas tecnologias a época.[247]

A partir de então, surgem problemas jurídicos decorrente da popularização do uso das redes, promovendo questões referentes ao direito à privacidade e proteção dos dados pessoais, com isso surgem diretrizes e marcos regulatórios em escala global, com os objetivos de criar normas para o uso da rede e regulação das redes sociais.[248]

Assim, o direito à privacidade é reconhecido constitucionalmente pelo Brasil. Tal direito abrange a preservação da intimidade, vida privada, inviolabilidade e assegura o direito a indenização pelo dano material ou moral, decorrente dessas violações.

No entanto, apesar do resguardo jurídico existente, até o ano de 2014 não havia no ordenamento jurídico brasileiro uma legislação abrangente que tratasse das violações de garantias e direitos fundamentais na internet. Questões

---

[246] BOFF, Salete Oro; FORTES, Vinícius Borges. A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil. Sequência (Florianópolis) [online]. 2014, n.68. p.119

[247] *Ibidem*, p.120.

[248] *Ibidem*.

relacionadas à proteção de dados, infraestrutura tecnológica para acessibilidade da internet para toda a população e outros aspectos essenciais ao pleno exercício da cidadania careciam de regulamentação específica[249]. As garantias como sigilo das comunicações, não suspensão da conexão e inviolabilidade, embora consideradas direitos essenciais, não eram devidamente contempladas por normativas jurídicas.[250]

Essa lacuna, no entanto, foi endereçada com o advento do Marco Civil da Internet, que foi introduzido para preencher esse vácuo normativo. Esse marco legal não apenas supriu a ausência de regulamentações, mas também estabeleceu princípios fundamentais para o uso e controle da internet no Brasil. Dentre esses princípios, destacam-se a Neutralidade da Rede, que visa garantir tratamento igualitário a todo o tráfego de dados, e a preservação da liberdade de expressão e privacidade[251]. O Marco Civil da Internet, portanto, representa um avanço significativo ao proporcionar diretrizes claras para a proteção dos direitos fundamentais no ambiente digital.[252]

No Brasil se há o entendimento da privacidade como direito fundamental e prevê a possibilidade de indenização pelo dano causado. Contudo, só houve uma regulamentação da matéria, propriamente dita, a partir de meados de 2000, antes eram usadas legislações de formas subsidiarias para os determinados casos concretos.[253]

Um dos exemplos do uso de forma subsidiaria para a proteção de privacidade dos dados é com o Código de Defesa do Consumidor[254], o qual prevê artigos como o art.43, que dispõe em suma sobre a possibilidade de acesso pelo consumidor a qualquer espécie de dados cadastrados no banco de dados da empresa. Além disso, também há a lei de habeas data[255] que permite o

---

[249] NADER, Paulo. *Curso de direito civil: parte geral*. 10. ed. Rio de Janeiro: Forense, 2016.
[250] BRASIL. *Lei n. 12.965,* de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 20/11/2023.
[251] NADER, Paulo. *Curso de direito civil: parte geral*. 10. ed. Rio de Janeiro: Forense, 2016.
[252] BRASIL. Lei n. 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20/11/2023
[253] BOFF, Salete Oro; FORTES, Vinícius Borges. *A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil.* Sequência (Florianópolis) [online]. 2014, n.68. p.122
[254] BRASIL. *Lei n. 8.078*, de 11 de setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 20/11/2023
[255] BRASIL. *Lei n. 9.507*, de 12 de novembro de 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm. Acesso em: 20/11/2023.

conhecimento ou retificação de informações em bancos de dados de entidades governamentais ou de caráter público.

Contudo, apesar da aparente abrangência das proteções legislativas, observa-se uma contradição recente com a aprovação da Lei do Cadastro Positivo[256]. Esta legislação autoriza a troca de dados entre instituições financeiras, incluindo informações sobre a adimplência ou inadimplência de débitos.

Tal intercâmbio visa a criação de um histórico de crédito, permitindo, por conseguinte, a oferta de linhas de crédito diferenciadas com juros variados, dependendo do histórico de pagamento do consumidor[257]. Este movimento contraditório é evidente em relação à Lei de Acesso à Informação, respaldada pelo inc. XXXIII do Art. 5 da Constituição Federal:

> Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.[258]

Além disso, vale mencionar a Lei Carolina Dieckmann[259], que surgiu em um momento de ocorrência de diversos crimes cibernéticos, de informática, como invasões bancarias, divulgação sem autorização de fotos pessoais, hackeamentos e então com a necessidade de tutelar bens jurídicos como privacidade e sigilo da informação e responsabilizar as infrações do mundo virtual.

Referido diploma legal, trouxe para o ordenamento jurídico brasileiro a criminalização da conduta de invasão de dispositivo informático, inserindo ao Código Penal brasileiro o artigo 154-A, que atualmente detém a seguinte disposição:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

---

[256] BRASIL. *Lei n. 12.414*, de 09 de junho de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm Acesso em: 20/11/2023
[257] NADER, Paulo. *Curso de direito civil: parte geral.* 10. ed. Rio de Janeiro: Forense, 2016.
[258] BRASIL, Constituição (1998). Constituição da República Federativa do Brasil. Brasília, DF, Senado, 1998.
[259] BRASIL. *Lei n. 12.737*, de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em: 20/11/2023

> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.[260]

Por fim, é relevante destacar novamente o Marco Civil[261] da Internet, sancionado em 2014. Tal lei desempenha um papel fundamental como a principal regulamentação para a utilização da internet, fundamentando-se em três princípios essenciais. São eles: o Princípio da Neutralidade da Rede, que busca garantir um tratamento equitativo para todo o tráfego de dados; o Princípio da Privacidade, assegurando a inviolabilidade e o sigilo das trocas de informações entre os usuários, bem como a liberdade de expressão. Este último prevê, de maneira responsável, a quebra do sigilo de dados mediante intimação judicial nos casos em que essas informações possam contribuir para a descoberta de atividades ilícitas.

Diante da rápida evolução dos meios tecnológicos, a tendência tem sido o progresso das leis para acompanhar esse avanço, integrando o ordenamento jurídico de forma condizente[262]. Nesse contexto, o Marco Civil da Internet representa um ponto de partida crucial para a modernização da legislação brasileira, adaptando-se aos desafios trazidos pela revolução digital. Diante disso,

---

[260] BRASIL. *Decreto-Lei nº 2.848*, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União, Poder Executivo, Brasília, DF, 31 dez. 1940. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-publicacaooriginal-1-pe.html. Acesso em: 20/11/2023
[261] BRASIL. *Lei n. 12.965*, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 20/11/2023
[262] NADER, Paulo. *Curso de direito civil: parte geral*. 10. ed. Rio de Janeiro: Forense, 2016.

a próxima seção fornecerá uma breve contextualização sobre a relevância deste marco legal para a temática que está sendo abordada.

3.2.1 O marco civil da internet

Desde o ano de 1999, por meio da apresentação, no Senado Federal, do Projeto Lei 84/99, a qual ficou conhecida como Lei Azeredo, que buscava uma ampla punição penal para crimes cometidos virtualmente, observa-se a preocupação em se regular, juridicamente, as ações no mundo virtual, no Brasil. Diversas foram as reações a tal projeto, que a época fora motivo de críticas, tendo em vista seu potencial de "vigilantismo"[263], o qual levaria aos usuários da rede a expor e punir os criminosos virtuais.[264]

Entretanto, muitas foram as reações favoráveis ao projeto, as quais viam a importância de se criar uma lei civil, para dispor sobre o assunto, nesse sentido Lemos, aduz que:

> O Marco Civil surgiu como uma alternativa à chamada 'Lei Azeredo', projeto de lei que propunha o estabelecimento de uma ampla legislação criminal para a internet, e assim batizada por conta do seu relator e mais assíduo defensor, o deputado Eduardo Azevedo (PSDB-MG). A percepção de um amplo espectro da sociedade brasileira é que a Lei Azeredo, se aprovada, provocaria um grande retrocesso no ambiente regulatório da internet no país.[265]

O Marco Civil da internet é visto como um marco, para o ordenamento jurídico brasileiro, pois sua criação, além de ter gerado um profundo debate, com a participação de diversos membros da sociedade civil, principalmente os usuários

---

[263] O Vigilantismo digital, cibervigilantismo ou Digilantes é conhecido pela prática de internautas que se utilizam dos recursos da internet e outras tecnologias digitais para combater alguma prática criminosa ou socialmente recriminada. O vigilantismo pode englobar os mais diversos temas, de golpes na rede à exploração sexual de crianças, passando por questões de proteção ambiental, direitos sexuais e corrupção. Nem sempre é claro o limite do vigilantismo como prática de combate aos crimes, pois há casos de justiceiros que cometem crimes para combater outros crimes, o que pode gerar problemas na justiça. (LEMOS, Ronaldo. *Direito, tecnologia e cultura: desafios jurídicos da comunicação digital.* Editora Atlas, 2014.)

[264] LEMOS, Ronaldo. *Direito, tecnologia e cultura: desafios jurídicos da comunicação digital*. Editora Atlas, 2014.

[265] LEMOS, Ronaldo. Direito, tecnologia e cultura: desafios jurídicos da comunicação digital. Editora Atlas, 2014.

das redes sociais, buscou tornar mais justo e democrático o tráfico na internet, demonstrando que esta não é mais “terra sem lei”[266].

Ainda em 2010, quando a lei ainda se encontrava em discussão, a Desembargadora Letícia Santos inovou ao utilizar dos fundamentos contidos em tal diploma legal, a fim de embasar a decisão do Agravo de Instrumento número 0013822-08.2010.8.19.0000, ao afirmar que:

> APLICABILIDADE. MULTA DIÁRIA EXCLUÍDA. PARCIAL PROVIMENTO DO RECURSO. 1. No caso dos autos, alegando violação de sua conta de e-mail, o agravado quer que a agravante lhe forneça os dados necessários para identificação dos invasores de sua conta de e-mail. 2. Haja vista a fase embrionária jurídica em relação ao assunto, ainda não se concretizaram definitivamente as posições no tocante à matéria. 3. Contudo, ainda que existam muitos nichos desconhecidos em relação à internet, esse mesmo argumento não pode servir para justificar ou escusar a não aplicação da legislação que se tem à mão. 4. O Marco Civil da Internet no Brasil, submetido à segunda consulta pública, estabelece os direitos dos cidadãos brasileiros na internet.5. Ponto muito importante e positivo do Marco Civil é a forma como propõe regular os direitos e deveres relativos aos vários dados gerados pelo usuário quando navega. 6. Os registros relativos à conexão (data e hora do início e término, duração e endereço IP vinculado ao terminal para recebimento dos pacotes) terão que ser armazenados pelo provedor de acesso à internet. 7. Em relação ao registro de acesso aos serviços de internet (e-mails, blogs, perfil nas redes sociais etc.), o provedor não tem obrigação de armazenar os dados. Mas, se o fizer, terá que informar o usuário, discriminando o tempo de armazenamento. 8. Assim, resta claro que a simples alegação de impossibilidade técnica de cumprimento à decisão, tendo em vista não mais possuir armazenados os logs de acesso com as informações das operações realizadas no mês de setembro de 2009 não tem o condão de afastar a determinação judicial concedida nos autos da Medida Cautelar. 9. Além disso, medida não trará nenhum prejuízo ao agravante já que este estará apenas fornecendo os dados necessários para identificar os possíveis violadores da conta de e-mail do autor da ação. 10. Por outro lado, em se tratando de ação de exibição de documentos, aplica-se ao caso a S. 372, STJ. 11. Mantémse, contudo, a decisão recorrida que determinou o fornecimento dos nomes, endereços e todos os dados que a NET tiver em seus arquivos, relativos a seus contratantes que das 22:00 horas do dia 19.09.2009 às 00:44 horas do dia 20.09.2009, se utilizaram dos IPs indicados no item 1 da petição inicial (cf. fls. 60), especificando os horários de inicio e fim da utilização, bem como os sites na internet que foram acessados no curso da utilização. 12. Parcial provimento do agravo de instrumento para excluir a imposição da multa di ria para caso de descumprimento.[267]

---

[266] *ibidem*.

[267] BRASIL. TJ RJ – 0013822-08.2010.8.19.0000 – Agravo de instrumento des. Leticia Sardas – julgamento: 30/06/2010 – vigésima câmara cível. Disponível em: http://www1.tjrj.jus.br/gedcacheweb/default.aspx?UZIP=1&GEDID=0003DF4E08AC8C662E2A188DDB4DF5BAB71F35C403071562. Acesso em: 20/11/2023

O Marco Civil da internet, lei 12.965/2014, fora aprovado na Câmara dos Deputados no dia 25 de março de 2014, sendo sancionado um mês depois, pela então presidente Dilma Rousseff, na Conferência NET Mundial, em São Paulo[268].

Desse modo, conforme já aduzido, anteriormente, tal lei fora o primeiro diploma legal elaborado, colaborativamente, entre a sociedade e o Poder Executivo, sendo que a própria internet fora o instrumento utilizado para debate.

A partir de sua promulgação, as relações virtuais passaram a ser, especificamente, reguladas, tendo em vista que, o Código Civil, lei utilizada anteriormente para tratar sobre o tema, dispunha de diversas lacunas.

Por fim, o Marco Civil da Internet trata de diversos direitos, deveres, dos usuários e prestadores de serviço, sendo um diploma normativo, ao mesmo tempo, criticado e amado pela sociedade.

Portanto, a tutela da privacidade, em todas as suas perspectivas, deve garantir, antes de tudo, a liberdade da pessoa para a construção e desenvolvimento de sua identidade e esfera íntima. Nesse sentido, importante se faz abordar a despeito da Lei Geral de Proteção de Dados Pessoais (LGPD), que é um importante marco no ordenamento jurídico brasileiro para o tema em questão, conforme será demonstrado a seguir.

3.3 A lei geral de proteção de dados: principais aspectos

A Lei Geral de Proteção de Dados é a Lei Ordinária nº 13.709, aprovada em agosto de 2018 e com vigência a partir de 18 de setembro de 2020. É o marco legal que rege o uso, proteção e transferência de dados pessoais no Brasil. Ele cria padrões para a coleta e processamento de dados corporativos. O objetivo da lei é garantir a privacidade e proteção dos dados pessoais e promover a transparência nas relações entre pessoas físicas e jurídicas. Além de garantir maior controle sobre o controle dos cidadãos sobre seus dados pessoais, é necessário o consentimento explícito para a coleta e uso dos dados, sendo ainda necessário fornecer ao usuário opções para visualizar, corrigir e excluir seus dados.[269]

---

[268] LEMOS, Ronaldo. *Direito, tecnologia e cultura: desafios jurídicos da comunicação digital*. Editora Atlas, 2014

[269] MALDONADO, V. N.; BLUM, R. O. *LGPD: Lei Geral de Proteção de Dados comentada.* 1. ed. São Paulo: Revista dos Tribunais, 2019.

A LGPD tem origem no Projeto Lei nº 53/2018, que foi aprovada por unanimidade e rapidez pelo plenário do Senado em julho de 2018. O texto também vale para empresas com sede no exterior, desde que o tratamento de dados ocorra no território do país.[270]

A seguir, abordar-se-á a respeito dos principais fundamentos da Lei Geral de Proteção de Dados.

3.3.1 Principais fundamentos da LGPD

A LGPD fornece uma estrutura com princípios e regras que regem todo o ordenamento jurídico. É uma lei relativamente pequena, dividida em dez capítulos e seções. Os regulamentos preliminares declaram os limites legais de aplicação, local de atuação, conceitos e princípios.

O artigo 1.º prevê o tratamento de dados pessoais, incluindo recursos digitais, por qualquer pessoa singular ou coletiva (pública ou privada) com vista à proteção dos direitos fundamentais, com destaque para a privacidade. O artigo 2.º, título I, descreve os fundamentos disciplinares para obter a proteção de dados de forma a respeitar a privacidade. Esse fundamento corrobora o que se encontra na Carta Magna, no art. 5, inciso X.[271]

O próximo fundamento é a autonomia informacional, que é bastante consistente porque é um alerta de que representa a capacidade de todos controlarem suas informações pessoais de alguma forma. Isso garante que uma pessoa possa decidir em determinadas circunstâncias se os dados podem ser processados (recolhidos, usados, transferidos) por terceiros, acessar bancos de dados para solicitar correção ou cancelamento de dados, porque todos os dados

---

[270] TEFFÉ, Chiara Spadaccini de. MAGRANI. Eduardo. VIOLA, Mario. *Artigo "5 pontos sobre a importância de uma autoridade nacional de proteção de dados".* Disponíve¬lem:https://medium.com/@ITSriodejaneiro/5-pontos-sobreaimport%C3%A2ncia-de-uma-autoridade-nacionaldeprote%C3%A7%C3%A3ode-dados-4cf8137cf59e. Acesso em 20/11/2023.

[271] MALDONADO, V. N.; BLUM, R. O. *LGPD: Lei Geral de Proteção de Dados comentada.* 1. ed. São Paulo: Revista dos Tribunais, 2019

estão relacionados à vida de uma pessoa. Portanto, seu proprietário deve revisá-lo para decidir se deve ou não permitir o acesso e a quem conceder acesso.[272]

Posteriormente, a Seção III afirma a liberdade de expressão, informação, comunicação e opinião porque reconhece que o abuso da informação do titular também pode levar à violação daqueles direitos que são justificados por direitos e garantias constitucionais. Sabe-se que os primeiros fundamentos mostram uma preocupação com a proteção do indivíduo, e os demais incisos (V, VI e VII) indicam a preocupação do legislador com a livre iniciativa e o desenvolvimento econômico do país.[273]

Embora a proteção de dados pessoais seja discutida, é útil reconhecer a mudança de paradigma no desenvolvimento da tecnologia e da livre iniciativa do ponto de vista do desenvolvimento das pessoas e da sociedade. As normas de proteção à privacidade não podem, portanto, impedir o desenvolvimento econômico, tecnológico e inovador, pois se relacionam com os princípios da ordem econômica do art. 170 e seguintes da Constituição Federal, pois o objetivo da LGPD é proteger contra possíveis abusos do Estado ou de outros cidadãos em relação ao direito ao trabalho e ao engajamento.[274]

Além disso, o dispositivo da mesma constituição prevê indenização por danos causados pela violação da privacidade, amparo legal também se encontra no art. 21 do Código Civil/2002, que dá às vítimas de violações de privacidade a oportunidade de recorrer ao tribunal para garantir seu direito constitucional à privacidade.[275]

A partir disso, pode-se observar que a LGPD detém relevantes fundamentos no que diz respeito a proteção de dados pessoais. Nesse sentido, relevante se faz conhecer alguns dos principais princípios, contido nessa norma, de maneira a compreender como esta buscou resguardar o direito à privacidade nos meios digitais, o que será feito a seguir.

---

[272] SÁ JUNIOR, Sergio Ricardo C. *A regulação jurídica da proteção de dados pessoais no Brasil.* 2019. Monografia de especialização – Pontífica Universidade Católica do Rio de Janeiro, Rio de Janeiro.
[273] *Ibidem.*
[274] MALDONADO, V. N.; BLUM, R. O. *LGPD: Lei Geral de Proteção de Dados comentada*. 1. ed. São Paulo: Revista dos Tribunais, 2019
[275] *Ibidem.*

3.3.2 Princípios contidos na Lei Geral de Proteção de Dados

Os princípios são o fundamento necessário do sistema jurídico. Nada pode ser determinado até que se verifique que corresponde a esta raiz fundamental, pois são parte necessária da interpretação dos textos legais. No entanto, a interpretação especial da norma LGPD leva em consideração apenas seu significado e aplicação específica.[276]

Robert Alexy ajuda a distinguir as regras dos princípios:

> Crucial para a diferença entre regras e princípios é que os primeiros são padrões que exigem que algo seja aplicado o mais amplamente possível, dentro das possibilidades legais e factuais disponíveis. Os princípios são, portanto, comandos de otimização caracterizados pelo fato de que podem ser cumpridos de diferentes maneiras e a medida exata de sua satisfação depende não apenas de possibilidades fáticas, mas também jurídicas. O escopo das opções legais é determinado por princípios e regras conflitantes[277].

Assim, os princípios são sempre aplicados, mais ou menos, ao contrário das regras que se aplicam ou não a um caso particular. Por isso, Robert Alexy segue definindo melhor as regras para dirimir dúvidas:

> [...] padrões que são sempre atendidos ou rejeitados. Se a regra se aplicar, faça exatamente o que ela diz; nem mais nem menos. Portanto, as regras envolvem determinar o que é factual e juridicamente possível. Isso significa que a diferença entre regras e princípios é uma diferença qualitativa, não uma diferença de grau. Toda norma é uma regra ou um princípio[278].

O princípio da finalidade atribui ao órgão administrativo o dever de praticar o ato administrativo de acordo com a concretude da finalidade almejada pela lei. Enfatizando a LGPD, pretende dar ao titular dos dados o direito de analisar se há um motivo e uma necessidade para os dados coletados. Considerando que os dados só podem ser tratados com autorização do titular, sendo ainda necessário

---

[276] TEFFÉ, Chiara Spadaccini de. MAGRANI. Eduardo. VIOLA, Mario. *Artigo "5 pontos sobre a importância de uma autoridade nacional de proteção de dados".* Disponível em:https://medium.com/@ITSriodejaneiro/5-pontos-sobreaimport%C3%A2ncia-de-uma-autoridade-nacionaldeprote%C3%A7%C3%A3ode-dados-4cf8137cf59e. Acesso em 20/11/2023.
[277] ALEXY, Robert. *Teoria dos Direitos Fundamentais*. 1. ed. São Paulo: Malheiros Editores, 2016. P.88.
[278] *Idem,*

assegurar que não haja desvio da finalidade de recolha e tratamento acordada na legislação.[279]

A concretude da boa-fé evita que as sentenças sejam vagas ou criem dúvidas quando se referem a um princípio, pois considerando que o titular deve avaliá-las para aprovar a medida, deixa claro que ele pode não concordar para a proteção dos dados que você usa divulgados a terceiros. Assim, o dado deve estar completamente convencido do que ele transmite, confirmando.

O princípio da adequação está diretamente relacionado ao princípio da finalidade, pois segundo ele a finalidade deve ser seguida no tratamento de dados pessoais para evitar o uso indevido. É claro que informa o titular de outra garantia e dúvida se é garantido que os dados serão utilizados mais ou menos do que o acordado na legislação.[280]

O princípio da necessidade também está relacionado ao princípio da finalidade, pois define os dados a serem coletados e tratados, ou seja, a menor quantidade possível de dados que seja suficiente para um determinado propósito.[281]

Esse princípio permite que os dados sejam transparentes para seu titular sendo chamado de acesso aberto. Seria inconsistente se o titular dos dados não tivesse livre acesso às informações relacionadas aos seus dados. Este princípio cria uma obrigação que é sólida porque um terceiro é responsável por abrir o arquivo para que o proprietário possa avaliar se foi feito corretamente. A integridade inclui a integridade dos dados vinculados, o que significa que o controlador não pode processá-los ou excluí-los arbitrariamente.[282]

A transparência torna as atividades diárias e as informações delas derivadas disponíveis para o público em geral. Este princípio não é um fim em si mesmo, mas um meio pelo qual a população controla a administração pública.

---

[279] SÁ JUNIOR, Sergio Ricardo C. *A regulação jurídica da proteção de dados pessoais no Brasil. 2019.* Monografia de especialização – Pontífica Universidade Católica do Rio de Janeiro, Rio de Janeiro.

[280] TEFFÉ, Chiara Spadaccini de. MAGRANI. Eduardo. VIOLA, Mario. Artigo *"5 pontos sobre a importância de uma autoridade nacional de proteção de dados".* Disponíve¬lem:https://medium.com/@ITSriodejaneiro/5-pontos-sobreaimport%C3%A2ncia-de-uma-autoridade-nacionaldeprote%C3%A7%C3%A3ode-dados-4cf8137cf59e. Acesso em 20/11/2023.

[281] MALDONADO, V. N.; BLUM, R. O. *LGPD: Lei Geral de Proteção de Dados comentada*. 1. ed. São Paulo: Revista dos Tribunais, 2019

[282] ALEXY, Robert. *Teoria dos Direitos Fundamentais.* 1. ed. São Paulo: Malheiros Editores, 2016

O princípio ausento impossibilita a eficácia de uma disposição legal, pois deve ser observado com especial atenção antes da anuência do titular. Afinal, isso está diretamente relacionado ao fato de que o titular deve estar plenamente ciente das condições de coleta, finalidade, tratamento, afirmação, tratamento e exclusão dos dados, com exceção dos segredos industriais e comerciais.[283]

A proteção de dados é essencial para a conformidade de segurança. A responsabilidade comum dos agentes de processamento de dados é um dispositivo técnico à disposição do titular dos dados capaz de impedir o acesso não autorizado e o fluxo de dados, ou seja, usar todos os meios possíveis para manter a segurança dos dados durante o processamento. Portanto, a responsabilidade por eventuais danos causados por eventos é apurada após vistoria técnica, quando não há culpa.[284]

Assim como a segurança define o padrão para a concepção do projeto, a prevenção deve ser o tom da segurança, pois na velocidade do potencial tecnológico, a falha pode significar danos inimagináveis, pois a capacidade de transmissão e armazenamento potencializam seus efeitos adversos.[285]

De acordo com o princípio da responsabilização e prestação de contas, o controlador ou operador deve demonstrar todas as medidas eficazes que podem ser utilizadas para demonstrar o cumprimento da LGPD, bem como a eficácia das medidas implementadas. Refere-se às consequências de infringir a lei. Ou seja, o tratamento dos dados é lícito e de acordo com as normas, se cumprir os regulamentos exigidos por lei, a negligência e os danos causados ao titular acarretarão responsabilidade.[286]

Com base no exposto, observa-se que a lei deve alertar os processadores e operadores de dados de que são responsáveis pelo cumprimento de todos os

---

[283] MALDONADO, V. N.; BLUM, R. O. LGPD: *Lei Geral de Proteção de Dados comentada*. 1. ed. São Paulo: Revista dos Tribunais, 2019

[284] TEFFÉ, Chiara Spadaccini de. MAGRANI. Eduardo. VIOLA, Mario. *Artigo "5 pontos sobre a importância de uma autoridade nacional de proteção de dados".* Disponíve¬lem:https://medium.com/@ITSriodejaneiro/5-pontos-sobreaimport%C3%A2ncia-de-uma-autoridade-nacionaldeprote%C3%A7%C3%A3ode-dados-4cf8137cf59e. Acesso em 20/11/2023.

[285] SÁ JUNIOR, Sergio Ricardo C. *A regulação jurídica da proteção de dados pessoais no Brasil.* 2019. Monografia de especialização – Pontífica Universidade Católica do Rio de Janeiro, Rio de Janeiro.

[286] MALDONADO, V. N.; BLUM, R. O. *LGPD: Lei Geral de Proteção de Dados comentada*. 1. ed. São Paulo: Revista dos Tribunais, 2019

requisitos decorrentes de suas disposições, para assegurar os objetivos, bases e demais princípios básicos definidos na lei. Em caso de violação do contido na norma tais agentes podem vir, até mesmo, a ser responsabilizados civilmente, conforme será analisado no tópico que segue.

3.3.3 Responsabilidade civil na LGPD

Do ponto de vista da responsabilidade dos operadores, a proteção de dados é de extrema importância. Com o desenvolvimento da tecnologia, o mercado da informação faz parte do cotidiano, e por isso o prejuízo causado ao titular dos dados é consequência direta e relativa do tamanho da importância econômica e abrangência.[287]

A LGPD inova ao estabelecer um conjunto de condições de tratamento de forma consistente, uniforme e legal. No entanto, esta é uma atividade que envolve riscos e pode causar danos (patrimonial ou moral) ao proprietário.

Nos casos em que o dano tenha sido causado pelo tratamento de dados, há, portanto, regras estabelecidas em lei sobre como a compensação deve ocorrer.

Com relação à responsabilidade civil prevista na LGPD, há clara distinção entre relações civis e relações de consumo. Nas relações civis, o âmbito é o aspecto contratual e aplica-se a regra geral do direito civil – a responsabilidade. Isso deve levar em conta a negligência do agente e, se houver responsabilidade objetiva, deve ser explicitamente apontado. No que diz respeito às relações de consumo, a reparação pode ser realizada em relação a uma determinada pessoa ou comunidade, dependendo da natureza da atividade de processamento de dados. Isso se torna mais preciso e informativo à medida que as medições aumentam.[288]

Outro ponto importante que deve ser abordado na LGPD é que a solidariedade entre controladores e operadoras em sua responsabilidade por danos nos termos inciso I, §1º, do art. 42, pois é relevante para todos os agentes de

---

[287] *Ibidem.*

[288] TEFFÉ, Chiara Spadaccini de. MAGRANI. Eduardo. VIOLA, Mario. *Artigo "5 pontos sobre a importância de uma autoridade nacional de proteção de dados".* Disponíve¬lem:https://medium.com/@ITSriodejaneiro/5-pontos-sobreaimport%C3%A2ncia-de-uma-autoridade-nacionaldeprote%C3%A7%C3%A3ode-dados-4cf8137cf59e. Acesso em 20/11/2023.

processamento o cumprimento das leis e segurança operacional, independentemente, de um seguir as ordens do outro. Isso significa que uma ou ambas as partes podem ser responsabilizadas por danos.

A responsabilidade civil objetiva aplica-se por previsão legal quando o legislador constatar fragilidade estrutural de uma das partes. No caso da LGPD, isso está previsto em duas situações: tratamento de dados no âmbito das relações de consumo de acordo com o artigo 45 da lei, e tratamento de dados pelo poder público, conforme art. 37, §6º da Constituição.[289]

Segundo o Supremo Tribunal Federal, não há responsabilidade objetiva, especialmente por atos comissivos. Esse é um entendimento que ainda não abordou as idiossincrasias do processamento de dados e deve ser observado em estudos futuros.[290]

Portanto, já se sabe que a LGPD traz um novo paradigma para a gestão de dados pessoais, garantindo a liberdade e a privacidade dos titulares dos dados pessoais. E para atingir seu objetivo principal, esta norma impõe restrições, obrigações a todas as pessoas, sejam elas pessoas físicas ou jurídicas, sejam elas pessoas físicas ou jurídicas, que tratem dados pessoais digitalmente ou de outra forma, e imponha penalidades.

Na prática, porém, as obrigações e a responsabilidade pelos danos causados ao titular dos dados cabem aos processadores, ou seja, o processador responsável e o mantenedor. A fim de cumprir efetivamente as diretrizes da LGPD e minimizar o risco de um evento gerar passivos, os processadores de dados responsáveis devem zelar para que seja assegurada a segurança dos dados sob controle de terceiros

Embora essas medidas temporárias não protejam os processadores de todos os problemas futuros, elas garantem que o processamento de dados seja mais compatível com as disposições da LGPD, o que garante que os riscos aos dados que possam prejudicar o titular dos dados sejam minimizados.

---

[289] SÁ JUNIOR, Sergio Ricardo C. *A regulação jurídica da proteção de dados pessoais no Brasil.* 2019. Monografia de especialização – Pontífica Universidade Católica do Rio de Janeiro, Rio de Janeiro.

[290] MALDONADO, V. N.; BLUM, R. O. *LGPD: Lei Geral de Proteção de Dados comentada*. 1. ed. São Paulo: Revista dos Tribunais, 2019

Por conseguinte, pelo exposto, infere-se a relevância do instituto da responsabilidade civil no ordenamento jurídico brasileiro, especialmente no que diz respeito à proteção da vida humana, da honra e da reputação e do direito à privacidade na internet.

A questão da proteção de dados pessoais mostra-se tão atual e de suma importância, que o próprio legislador, por meio da Emenda Constitucional 115/2022, deu a este direito status de direito e garantia fundamental, conforme será analisado no tópico que segue.

3.4 A Emenda Constitucional 115/2022 e a Questão da Privacidade

A Emenda Constitucional nº 115[291], promulgada em 11 de fevereiro de 2022, representa um marco significativo ao elevar a proteção de dados pessoais ao status de direito fundamental. Essa transformação impulsiona de forma contundente a necessidade de resguardar a privacidade, constituindo, por conseguinte, a preservação da dignidade humana por meio do livre desenvolvimento da personalidade individual.

Anteriormente, o artigo 5º da Constituição da República Federativa do Brasil já abarcava princípios fundamentais, como a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade. Contudo, a EC 115/2022[292] introduziu uma alteração crucial, acrescentando, no inciso LXXXIX desse artigo, o direito à proteção dos dados pessoais, inclusive nos meios digitais. Essa inclusão reflete uma significativa mudança na configuração sistêmica de proteção à privacidade, conferindo aos dados pessoais um abrigo expresso na Constituição, agora posicionado hierarquicamente no rol dos direitos fundamentais[293].

---

[291] BRASIL. *Emenda Constitucional nº 115,* de 11 de fevereiro de 2022. Altera o texto do art. 156 da Constituição Federal, para determinar que a União legislará sobre a competência tributária em relação aos impostos sobre serviços de qualquer natureza, de competência dos Municípios e do Distrito Federal, definidos em lei complementar. Diário Oficial da União, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 20/11/2023

[292] *Ibidem.*

[293] TIBÚRCIO L. *Emenda Constitucional 115/2022: direito à proteção de dados pessoais*. 2022. Disponível em: https://www.estrategiaconcursos.com.br/blog/emenda-constitucional-115-2022/. Acesso em: 20/11/2023

Essa atualização constitucional não apenas reconhece a importância crescente da privacidade em um mundo digitalizado, mas também reforça a necessidade de uma proteção mais robusta diante dos desafios contemporâneos. A partir desse novo panorama legal, o direito à privacidade não é apenas um componente intrínseco da liberdade individual, mas também um alicerce essencial para a preservação da autonomia e da integridade pessoal[294].

Ao adentrar o terreno digital, a EC 115/2022[295] sinaliza para a complexidade das questões relacionadas à privacidade online. O agasalho constitucional conferido aos dados pessoais reconhece que, em uma sociedade cada vez mais interconectada, a proteção da informação pessoal[296] torna-se vital para a manutenção de uma esfera de intimidade e segurança para os cidadãos[297].

Essa emenda não apenas legitima a preocupação crescente com a privacidade, mas também estabelece um alicerce robusto para a legislação infraconstitucional. Ao inserir a proteção de dados pessoais na Carta Magna, ela orienta a interpretação e elaboração de normas e regulamentos futuros, consolidando a importância desse direito no arcabouço jurídico nacional[298].

A partir disso, observa-se que a EC 115/2022 não apenas reflete a evolução da sociedade em direção a uma maior consciência sobre a privacidade, mas também confere uma base jurídica sólida para enfrentar os desafios emergentes no cenário digital. Essa mudança constitucional não é apenas um reconhecimento da importância dos dados pessoais, mas também um compromisso com a proteção

---

[294] *Ibidem.*

[295] BRASIL. *Emenda Constitucional nº 115,* de 11 de fevereiro de 2022. Altera o texto do art. 156 da Constituição Federal, para determinar que a União legislará sobre a competência tributária em relação aos impostos sobre serviços de qualquer natureza, de competência dos Municípios e do Distrito Federal, definidos em lei complementar. Diário Oficial da União, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 20/11/2023

[296] Para Barreto Menezes Cordeiro, "o conceito de informação pessoal abrange, consequentemente, todos os aspetos relativos à nossa pessoa, quer sejam familiares ou sociais, privados ou públicos, físicos ou mentais." (CORDEIRO, A. Barreto Menezes Cordeiro. Dados pessoais: conceito, extensão e limites. Disponível em: https://blook.pt/publications/publication/e38a9928dbce. Acesso em: 20/11/2023, p.07). A partir disso, observa-se que ao consagrar a proteção de dados como um Direito e uma Garantia Fundamental, o legislador brasileiro visou proteger de forma ampla a privacidade individual, resguardando, assim, a dignidade da pessoa humana.

[297] TIBÚRCIO L. *Emenda Constitucional 115/2022: direito à proteção de dados pessoais*. 2022. Disponível em: https://www.estrategiaconcursos.com.br/blog/emenda-constitucional-115-2022/. Acesso em: 20/11/2023

[298] TIBÚRCIO L. Emenda Constitucional 115/2022: direito à proteção de dados pessoais. 2022. Disponível em: https://www.estrategiaconcursos.com.br/blog/emenda-constitucional-115-2022/. Acesso em: 20/11/2023

dos direitos fundamentais dos cidadãos em um mundo cada vez mais interconectado[299].

Uma grande influência no campo da proteção de dados, advém do fator econômico, porque diante das inúmeras notícias de vazamentos e exposições de dados pessoais, passou-se a exigir maior comprometimento das empresas para a proteção dos dados que coletavam ou compartilhavam. A boa imagem da empresa passou a ser associada ao grau de comprometimento com a guarda dos dados elevando a confiança do público, gerando perdas ou ganhos econômicos, conforme os meios que adota para garantir a proteção.

A Diretiva 95/46/CE[300] do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, destacou-se como um instrumento relevante ao exigir sistemas mais robustos de proteção da privacidade no âmbito europeu.

Posteriormente, o Regulamento Geral de Proteção de Dados 2016/67940[301] (RGPD), norma crucial da União Europeia (UE) que sucedeu a Diretiva 95, intensificou a obrigatoriedade de uma governança mais robusta para garantir a proteção e segurança da privacidade. O RGPD reverberou globalmente, impondo condições e requisitos de conformidade para contratos estabelecidos com a UE, influenciando significativamente países, incluindo o Brasil, que mantêm relações comerciais com a UE.

Desse modo, a Emenda 115/2022[302], ao tornar o direito à proteção de dados pessoais um direito fundamental, inscrito hierarquicamente, no ápice da pirâmide constitucional visou consagrar a proteção integral do indivíduo, principalmente, no que diz respeito a honra e imagem da pessoa, sob os aspectos digitais.

---

[299] *Ibidem.*

[300] UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 20/11/2023

[301] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 20/11/2023

[302] BRASIL. *Emenda Constitucional* nº 115, de 11 de fevereiro de 2022. Altera o texto do art. 156 da Constituição Federal, para determinar que a União legislará sobre a competência tributária em relação aos impostos sobre serviços de qualquer natureza, de competência dos Municípios e do Distrito Federal, definidos em lei complementar. Diário Oficial da União, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 20/11/2023

De acordo com Tibúrcio[303] “o fato de a Proteção de Dados ser agora uma cláusula pétrea impede que se tramite no Legislativo proposta de emenda tendente a suprimir ou reduzir a proteção constitucional conferida a esse direito”.

Para melhor compreender essa nova configuração exige-se, necessariamente, um novo olhar que vislumbre a nova configuração dimensão do livre desenvolvimento da personalidade da pessoa natural, que existe no direito à privacidade daqueles que atuam no setor público, em especial no que diz respeito aos componentes das Forças Armadas[304].

O livre exercício dos direitos da personalidade e seu desenvolvimento implicam em tornar compatível a proteção de dados pessoais às novas exigências da sociedade digital. Para que isto ocorra, deve-se realizar um exercício constante de moldar a situação fática para transparecer suas formas e, assim, encontrar os meios adequados à proteção integral da dignidade humana[305].

Nesse diapasão Bioni pontua que:

> O direito à proteção dos dados pessoais deve ser alocado como uma nova espécie do rol aberto dos direitos da personalidade, dando elasticidade à cláusula geral da tutela da pessoa humana. Caso contrário, corre-se o risco de ele não se desprender das amarras conceituais e da dinâmica do direito à privacidade e, em última análise, inviabilizar uma normatização própria para regular o fluxo informacional como fator promocional da pessoa humana[306].

Portanto, a proteção de dados pessoais, como um direito fundamental do indivíduo, sendo essa regulamentada pela EC 115/22 oferece mais um instrumento de proteção ao direito da personalidade.

Nesse contexto, torna-se evidente que as alterações na legislação concernente à proteção de dados geraram significativos impactos na sociedade, com especial destaque para setores intimamente ligados ao manejo de informações pessoais, como é o caso da área da saúde. Diante desse cenário, o próximo segmento discorrerá sobre os impactos predominantes nesse setor e os desafios

---

[303] TIBÚRCIO L. *Emenda Constitucional 115/2022: direito à proteção de dados pessoais.* 2022. Disponível em: https://www.estrategiaconcursos.com.br/blog/emenda-constitucional-115-2022/. Acesso em: 20/11/2023

[304] *Ibidem.*

[305] *Ibidem.*

[306] BIONI,Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Forense, 2019. P.99.

enfrentados para a plena implementação da Lei Geral de Proteção de Dados (LGPD) no contexto brasileiro.

4. DIREITO FUNDAMENTAL A SAÚDE E A APLICABILIDADE DA LGPD

O propósito deste capítulo é realizar uma análise abrangente dos elementos fundamentais do Direito à Saúde à luz da Lei Geral de Proteção de Dados. Em particular, será dedicada atenção especial à proteção de dados sensíveis, que requerem consentimento específico para seu processamento, conforme será explorado ao longo desta seção. Este estudo é crucial para a futura compreensão dos impactos e repercussões da coleta e tratamento de dados pessoais no contexto da pandemia de Covid-19.

4.1 Do direito à saúde

Sabe-se que a promulgação da Constituição Federal de 1988, em 5 de outubro, foi um grande marco, principalmente, por ter sido promulgada após o fim de um longo período ditatorial em que o Brasil se encontrava, o qual ficou evidenciado pela grande repressão e retirada de direitos dos cidadãos. Sua formulação iniciou-se em 1987, momento em que o país passava por um processo de redemocratização. Deste modo, a Constituição surgiu como o marco de devolução e consagração dos direitos sociais, econômicos, políticos, culturais[307].

Consolidando-se a nova ordem constitucional proposta pela Carta da República de 1988, o Estado Democrático de Direito também fora constituído no Brasil, estando presente no artigo primeiro, de referido diploma legal, que trata sobre os princípios fundamentais, dentre eles a soberania, cidadania, dignidade da pessoa humana. Firmando-se assim, na ordem jurídica brasileira, o princípio democrático, dispondo que “todo poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição”.[308]

A Constituição de 1988, foi apelidada de Constituição Cidadã, pois além de devolver os direitos retirados pela Ditadura Militar, ampliou a proteção aos direitos fundamentais, individuais e coletivos, dentre eles, o direito a saúde, consagrando-o como um direito social de suma importância, sendo dever do Estado garanti-lo a

[307] FIGUEIREDO, Luciano. *Curso de Direito Constitucional*. 14. ed. São Paulo: Saraiva, 2017.
[308] *Ibidem.*

todos, pois, este é tão importante quanto o direito à vida, e medidas devem ser recepcionadas para que se consigam concretizar tal direito.

Com o transcorrer dos anos, as alterações na definição do que seria saúde ajudaram ainda mais na efetivação deste direito, segundo Figueiredo, mencionada evolução permitiu um entendimento mais abrangente do que realmente seria essa garantia hodiernamente. Constituindo-se com um direito humano e fundamental, o Direito a Saúde é fruto de uma longa e expressiva jornada na formulação não somente de um direito, porém também de uma ideia mais própria do que seria a saúde[309].

Para Pilau Sobrinho a garantia à saúde pode ser vista de diferentes formas:

> Tudo depende da titularidade e da divisibilidade do bem tutelado. Não há como questionar a existência de um direito individual a saúde, enquanto um direito restrito a incolumidade ou segurança individual, porém a tendência da contemporaneidade deve ser centralizada na dimensão de proteção dos direitos metaindividuais da sociedade[310].

Tendo em vista a importância global deste direito, fora firmada pela Declaração Universal dos Direitos Humanos, de 1948, em seu artigo XXV, a garantia a todo indivíduo a um padrão de vida que fosse capaz de assegurar a si e sua família saúde e bem-estar[311].

Apenas, como já mencionado, com a Constituição Federal de 1988, que fora efetivado o direito a saúde no Brasil, garantindo-o, em seu artigo sexto, como um direito social e no artigo 196, um direito de todos.

---

[309] FIGUEIREDO, Luciano. *Curso de Direito Constitucional*. 14. ed. São Paulo: Saraiva, 2017.

[310] PILAU SOBRINHO, Liton Lanes. *Direito à Saúde: uma perspectiva constitucionalista*. Passo Fundo, Universidade de Passo Fundo, 2003. ISBN: 8575151150. p. 100.

[311] A carta dispõe: “Toda a pessoa tem direito a um nível de vida suficiente para lhe assegurar e à sua família a saúde e o bem-estar, principalmente quanto à alimentação, ao vestuário, ao alojamento, à assistência médica e ainda quanto aos serviços sociais necessários, e tem direito à segurança no desemprego, na doença, na invalidez, na viuvez, na velhice ou noutros casos de perda de meios de subsistência por circunstâncias independentes da sua vontade. 2.A maternidade e a infância têm direito a ajuda e a assistência especiais. Todas as crianças, nascidas dentro ou fora do matrimônio, gozam da mesma proteção social.”.ONU. *Declaração Universal dos Direitos Humanos.* Adotada e proclamada pela resolução 217 A (III) da Assembleia Geral das Nações Unidas em 10 de dezembro de 1948. Disponível em: http://unesdoc.unesco.org/images/0013/001394/139423por.pdf. Acesso em: 15 de dezembro de 2023.

De acordo com Sarlet[312], a Carta da república de 1988 elevou o direito a saúde a um patamar irrevogável, agasalhando-o não apenas como um bem jurídico digno de tutela, porém indo mais além, dando a este um status de direito fundamental, reconhecendo-lhe maior proteção jurídica.

Observando-se os entendimentos jurisprudenciais de diversos tribunais, desde o Supremo Tribunal Federal até os Tribunais Estaduais, pode-se denotar que o entendimento unânime é o de que o direito à saúde, além de qualificar-se como Direito Fundamental que assiste a todas as pessoas, representa consequência constitucional indissociável do direito à vida[313].

O Desembargador Nelson Schaefer Martins do TJ- SC em julgamento de uma apelação dispôs que é direito de todos e dever do Poder Público, a garantia do tratamento da saúde, que, segundo a *Lex Fundamentalis*, inclui o fornecimento gratuito de medicamento, a fim de garantir a conservação da saúde de quem não tiver condições de fazê-lo.[314]

A Suprema Corte possui inúmeros julgados sobre o assunto, em um destes, o Ministro Celso de Mello, julgando um caso de um paciente com HIV, dependente de medicamentos do Sistema Único de Saúde, garantiu que tal direito representa ônus constitucional, indissociável do direito à vida.[315]

O ministro Ayres Britto, do Supremo Tribunal Federal, julgando a ação cautelar 2.836, expos que “a saúde é constitucionalmente qualificada como direito fundamental de dupla face (direito social e individual indisponível).”[316]

Na decisão de um Recurso Extraordinário o Ministro Lewandowski disse que o julgador ao ser confrontado entre proteger o direito à vida e à saúde ou fazer prevalecer um interesse financeiro e secundário do Estado, entende que por razões de ordem ético-jurídica impõem ao julgador uma só e possível opção: aquela que privilegia o respeito indeclinável à vida e à saúde humanas.[317]

---

[312] SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 13. ed. rev. e atual. Porto Alegre: Livraria do Advogado, 2019. P.147.
[313] Ibidem.
[314] BRASIL. Tribunal de Justiça de Santa Catarina. Apelação Cível n. 2012.089245-5, da capital, Rel. Des. Nelson Schaefer Martins, SC, 29 de janeiro de 2013.
[315] BRASIL. Supremo Tribunal Federal. Recurso Extraordinário 271286. RS, Relator: Celso de Mello. Data de Julgamento: 11/09/2000, Segunda Turma.
[316] BRASIL. Supremo Tribunal Federal. Ação cautelar 2.836. SP, Relator: Ayres Britto. Data de Julgamento: 27/03/2012, Segunda Turma.
[317] BRASIL. Supremo Tribunal Federal. Recurso Extraordinário 706931. RN, Relator: Ricardo Lewandowski. Data de Julgamento: 15/05/2013.

Além disso, a ministra Carmen Lúcia considerou a distribuição de fraldas descartáveis a uma criança doente, um real fim terapêutico, não se configurando mera comodidade, afirmando ainda:

> o direito à saúde de crianças e adolescentes detêm absoluta prioridade com respaldo nos artigos. 196 e 198 da CRFB/88 e no artigo 11, § 2º do ECA que atribui ao Poder Público o dever de fornecer gratuitamente àqueles que necessitem os medicamentos, próteses e outros recursos relativos a tratamento, habilitação ou reabilitação.[318]

Ante ao exposto, fica claro que é obrigação do Poder Público cumprir e avocar o direito que positivou, independentemente da forma utilizada para que tal direito seja concretizado, pois, de acordo com o artigo 23, inciso II, da Constituição Federal, cuidar da saúde é competência de todos os entes federados[319].

De acordo Schwartz[320], ainda que o direito a saúde necessite dos meios materiais necessários para sua efetivação, o Poder Público tem responsabilidade na área da saúde, e nenhum dos entes federados componentes da República Brasileira pode eximir-se de tal obrigação. E o entendimento dos tribunais não é diferente.

A responsabilidade pelo atendimento à saúde é solidária entre União, Estados e Municípios. Eventual deliberação a respeito da repartição de responsabilidade compete unicamente aos entes federativos, a ser realizada em momento oportuno, não podendo o particular ter limitado seu direito à saúde, garantido constitucionalmente, por ato da Administração Pública.[321]

Portanto, resguardar o direito a saúde é o mínimo que o Poder Público deve fazer ao cidadão[322], haja vista, que este é próprio do ser humano, sendo intrínseco ao mínimo existencial e se o Governo não garante de maneira administrativa, cabe ao judiciário o fazer, por meio da tutela jurisdicional.

A partir disso, uma das formas de proteger tal direito seria por meio da proteção de dados referentes a saúde, que ganhou especial contorno após a

---

[318] BRASIL. Supremo Tribunal Federal. Recurso Extraordinário com Agravo 741583. RS, Relator(a): Cármen Lúcia. Data de Julgamento: 17/05/2013

[319] FIGUEIREDO, Luciano. *Curso de Direito Constitucional*. 14. ed. São Paulo: Saraiva, 2017.

[320] SCHWARTZ, Germano. *Curso de Direito Constitucional*. 4. ed. rev. e atual. Rio de Janeiro: Forense, 2016.

[321] BRASIL. Tribunal de Justiça do Rio Grande do Sul. Agravo de Instrumento n. 70051324309, de Sapucaia do Sul, Rel. Ricardo Moreira Lins Pastl, SC. Julgamento em 02/10/2012

[322] FIGUEIREDO, Luciano. *Curso de Direito Constitucional*. 14. ed. São Paulo: Saraiva, 2017.

promulgação da LGPD, visto que além de exporem o paciente, muitas vezes, sem consentimento, tratam-se de dados sensíveis, os quais necessitam de consentimento especial para seu tratamento, conforme será abordado no tópico que segue.

4.2 Dados sensíveis e a LGPD

Conceituam-se os dados pessoais sensíveis como aqueles diretamente relacionamentos aos aspectos mais íntimos da personalidade de um indivíduo. Assim, são dados pessoais sensíveis aqueles relativos à 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 um indivíduo[323].

A Lei Geral Proteção Dados expõe em seu artigo 5º, II, o que vem a ser dados sensíveis, entre estes estão os referentes à saúde, visto que apresentam a extensão da personalidade do indivíduo, relevantes em sua privacidade, identidade, merecendo uma maior proteção jurídica. Segundo Dallari e Monaco[324] tomando em conta o artigo 35 da RGPD, consideram-se informações pertinentes a saúde as que se referem “ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro.”

Desta feita, questões envolvendo a saúde ganham uma relevância maior, visto que atingem, diretamente, a vida privada, intimidade do indivíduo, assim consideram-se sensíveis. Outra questão importante de ser frisada seria o fato de que a divulgação destes dados poderia vir a causar uma possível discriminação a um indivíduo, justificando assim a relevância de sua maior proteção, visto que detém um grande potencial de atingir os direitos humanos. Desse modo, o compartilhamento não autorizado destas informações pode vir a causar discriminação e estigmatização social aos seus titulares.[325]

---

[323] DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos e coordenação. LGPD na saúde. São Paulo: Thomson Reuters Brasil, 2021.
[324] *Ibidem.*
[325] VIEIRA, Fabio Alonso; COSTA, Carolina Barbosa Cunha. *Data Privacy and Protection Relating to Healthcare in Europe, the United States and Brazil.Latin Lawyer*. August 2021. Disponível em:

O setor médico coleta e processa grandes quantidades de dados pessoais com base nos serviços prestados aos pacientes e tem grande responsabilidade pela proteção desses dados.

No entanto, Tinto[326] defende que o problema das violações de dados sensíveis em hospitais é agravado quando são considerados “devassáveis”. Diante disso, as organizações de saúde precisam proteger melhor a confidencialidade dos dados do paciente por meio de fortes políticas de privacidade que possam garantir transparência, simplicidade e acessibilidade do paciente. Entende-se, portanto, que as instituições médicas devem zelar pela validade dos direitos de confidencialidade do paciente e entender que são meras guardiãs das informações pertencentes aos pacientes. Os pacientes são, portanto, muito importantes porque são proprietários dos dados e devem ser informados sobre como eles são usados.

A partir disso, a LGPD conceitua em seu art. 5º, inciso V, que o titular é a “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”. É relevante destacar que os direitos do titular dos dados, sensíveis ou não, estão previstos no artigo 18 da LGPD e garantem a toda pessoa física a titularidade plena dos dados a que se referem. Juntamente com a propriedade, seguem os seguintes direitos: confirmação da existência do tratamento; acesso aos dados; informações sobre compartilhamento; correção de dados; eliminação de dados; portabilidade de dados; possibilidade de não consentimento; e retirada do consentimento (BRASIL, 2018).

Os titulares dos dados estão no centro dos debates sobre proteção de dados, pois, as disposições normativas tratam especialmente de garantir seus direitos, visto que são os verdadeiros detentores dos dados. Assim, a LGPD conferiu a estes um protagonismo, um conjunto de direitos que devem ser respeitados durante o processo de tratamento de dados, como o direito de solicitar a anonimização e a exclusão de dados desnecessários ou tratados com base no consentimento.[327]

---

https://latinlawyer.com/guide/the-guide-corporate-compliance/secondedition/article/24-data-privacy-and-protection-relating-healthcare-in-europe-the-united-statesand-brazil. Acesso em: 20/11/2023

[326] TINTO, Ana Rita Ramos Y Rio. *Proteção de dados de saúde Percepção e conhecimento dos Administradores Hospitalares acerca do novo Regulamento Geral de Proteção de Dados da União Europeia.* 2018. Dissertação (Mestrado). Escola Nacional de Saúde Pública. Universidade Nova de Lisboa, Lisboa, 2018.

[327] DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos e coordenação. *LGPD na saúde*. São Paulo: Thomson Reuters Brasil, 2021.

Conforme Aragão e Schiocchet[328] a LGPD está amparada na ideia central de que as pessoas tenham conhecimento e controle sobre a coleta e o processamento de suas informações, principalmente daquelas que as identificam, possibilitando a limitação desse processo. Assim, para a efetividade do tratamento de dados pessoais é necessária ter uma finalidade determinada, com medidas necessárias para prevenir danos e proteger os dados, armazenando os quando necessários, como o consentimento do titular durante todo o processo, que tem o direito a acessá-los e ainda solicitar sua exclusão.[329]

Uma relevante questão, trata do consentimento, visto que o artigo 7º, I, da LGPD afirma que o tratamento de dados pessoais apenas pode ocorrer com o consentimento de seu titular. Desse modo, o ordenamento normativo dá maior privilégio a participação ativa de seu titular, mediante a prioridade de seu consentimento.[330]

A autorização do titular se manifesta de forma livre, informada e de forma inequívoca, passando a concordar que seus dados pessoais sejam tratados, para um fim específico, como bem explica o artigo 5º, XII, da LGPD.

Para Albuquerque[331], o consentimento informado é uma escolha voluntária e informada que visa promover a autonomia, a autodeterminação, a integridade física do paciente. Entende-se que os pacientes têm direito a: participar nas decisões sobre os seus cuidados de saúde; de participar ativamente no aconselhamento sobre seus cuidados; de retirar o consentimento sem retaliação e ao consentimento informado sem coerção ou influência indevida. A partir disso, o autor obtém o direito de respeitar sua vida privada:

> Tem uma ampla gama de aplicações no atendimento ao paciente, incluindo o direito de recusar qualquer tipo de tratamento, o direito de fazer escolhas quanto a visitas e exames físicos por profissionais médicos e o direito à confidencialidade das informações de saúde que eles respeitam. Direito de consentir em qualquer tipo de procedimento.[332]

---

[328] ARAGÃO, A. L.; SCHIOCCHET, T. R. *Lei Geral de Proteção de Dados: Comentários à Lei nº* 13.709/2018. Editora Juspodivm, 2020.
[329] GREGORI, Maria Stella. *Os impactos da lei geral de proteção de dados pessoais na saúde suplementar.* Revista de Direito do Consumidor. v. 127, p. 171– 196, jan./fev. 2020.
[330] BRASIL. *Lei n. 13.709*, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm Acesso em: 20/11/2023
[331] ALBUQUERQUE, Aline. *Direitos humanos dos pacientes*. Curitiba: Juruá, 2016. P.108.
[332] ALBUQUERQUE, Aline. *Direitos humanos dos pacientes*. Curitiba: Juruá, 2016. P.108.

Portanto, no âmbito da LGPD, os titulares devem ser notificados sobre o uso e a divulgação de seus dados de forma clara e compreensível. A finalidade declarada para o uso e processamento da informação deve ser clara e específica, sendo proibida a permissão geral e o uso fora do contexto.

Segundo Dove e Taylor[333], a divulgação de dados pessoais sempre acarreta riscos, os dados pessoais de saúde podem ser considerados mais arriscados do que outros, pois, há uma suposição de os dados pessoais não podem ser usados para colocar o paciente em risco, o que os autores discordam.

Assim, o consentimento, portanto, respeita os indivíduos como atores e tem uma função protetora, pois, os indivíduos têm o direito de assumir, voluntariamente, os riscos de divulgação e uso de seus dados com base nessas características. Dessa forma, o consentimento funciona como uma proteção, pois evita erros que constituem um processo contínuo no qual uma pessoa pode mudar de ideia[334].

Neste contexto, enfatiza-se que os pacientes são os verdadeiros proprietários de suas informações e, portanto, devem desempenhar um papel na proteção de seus dados. Portanto, fica claro que ter processos e ferramentas para proteger esses dados é essencial para garantir a confidencialidade dos dados do paciente. Porque sem proteção de dados, não se pode falar sobre a confidencialidade dos dados do paciente.

4.3 O tratamento dos dados de saúde

No tocante à guarda dos prontuários, os profissionais ou a instituição que assistem o paciente são responsáveis por armazená-los de modo seguro (Art. 87 §2º, da Resolução CFM 2.227/2018), seja em meio físico ou digital, de modo a preservar-lhes o conteúdo e, consequentemente, o segredo e a não violação à esfera de privacidade e intimidade do assistido[335].

---

[333] DOVE, Edward S; TAYLOR. Mark J. Signalling *Standards for Progress: Bridging the Divide Between a Valid Consent to Use Patient Data Under Data Protection Law and the Common Law Duty of Confidentiality.* Medical Law Review, v. 29, Issue 3, Summer, p. 411–445, 2021.
[334] *Ibidem*.
[335] CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.227, de 13 de dezembro de 2018. Regulamenta a prática da telemedicina no país. Disponível em: https://abmes.org.br/legislacoes/detalhe/2694#:~:text=Resolu%C3%A7%C3%A3o%20CFM%20n%C2%BA%202.227%2C%20DE%2013%20DE%20DEZEMBRO%20DE%202018&text=Define%20e

Na área da saúde, portanto, a noção de que os dados de saúde são espécies de dados sensíveis encontra respaldo na regulamentação ética e administrativa. O profissional da saúde, para atuar conforme a ética, deve partir da premissa de que o histórico médico de um paciente contém informações sensíveis cujo vazamento acidental ou voluntário pode ser catastrófico para a vida dele e de seus familiares e com efeitos irreversíveis[336].

Dados os riscos envolvidos no tratamento de dados de saúde, tem se formado uma legislação setorial robusta para impor obrigações e padrões mínimos de segurança no dever de guarda e manuseio dos registros dos pacientes. Processo este que vem se intensificando com o surgimento de tecnologias da informação e comunicação para mediar a atenção à saúde, as denominadas “e-Saúde”, que englobam serviços como tele consultorias, telediagnóstico, segunda opinião formativa, tele cirurgia, tele monitoramento, teleducação e prontuário eletrônico[337].

A iniciar pelo prontuário médico, trata-se de documento único que reúne todos os dados da assistência prestada ao paciente, a permitir uma prestação continuada. A Resolução CFM nº 1.638/2002[338], além de trazer o conceito de prontuário médico, traz informações sobre seu conteúdo essencial e as atribuições de responsabilidade sobre preenchimento, guarda e manuseio, bem como torna obrigatória a criação de Comissão de Revisão de Prontuários, a quem compete observar a qualidade dos dados inseridos no prontuário e verificar a presença dos seguintes requisitos mínimos:

> a. Identificação do paciente nome completo, data de nascimento (dia, mês e ano com quatro dígitos), sexo, nome da mãe, naturalidade (indicando o município e o estado de nascimento), endereço completo (nome da via pública, número, complemento, bairro/distrito, município, estado e CEP);

%20disciplina%20a%20telemedicina,servi%C3%A7os%20m%C3%A9dicos%20mediados%20por%20tecnologias.&text=Revoga%3A,07%20de%20agosto%20de%202002. Acesso em: 20/11/2023

[336] BRAGANÇA, Luciano; TESTA, Marco. TIC Saúde e Privacidade: Uma Leitura Atualizada. In: Livro Verde Sociedade da Informação no Brasil: Dimensões e Propostas. CGI.br, 2011

[337] KAMEDA, Paulo Pazello. *Segurança em e-Saúde: Desafios e Propostas.* Tese de Doutorado, Universidade Estadual de Campinas, 2015.

[338] CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 1.638, de 29 de maio de 2002. Define e disciplina os procedimentos concernentes às Comissões de Revisão de Prontuários nos Conselhos Federal e Regionais de Medicina e dá outras providências. Disponível em: https://www.mpgo.mp.br/portal/arquivos/2019/09/11/15_40_13_481_Consulta_09_2019_comissão_revisora_em_unidades_de_saúde_1_pj_mineiros201900491013.pdf. Acesso em: 20/11/2023

> b. Anamnese, exame físico, exames complementares solicitados e seus respectivos resultados, hipóteses diagnósticas, diagnóstico definitivo e tratamento efetuado;
> c. Evolução diária do paciente, com data e hora, discriminação de todos os procedimentos aos quais o mesmo foi submetido e identificação dos profissionais que os realizaram, assinados eletronicamente quando elaborados e/ou armazenados em meio eletrônico;
> d. Nos prontuários em suporte de papel é obrigatória a legibilidade da letra do profissional que atendeu o paciente, bem como a identificação dos profissionais prestadores do atendimento. São também obrigatórios a assinatura e o respectivo número do CRM;
> e. Nos casos emergenciais, nos quais seja impossível a colheita de história clínica do paciente, deverá constar relato médico completo de todos os procedimentos realizados e que tenham possibilitado o diagnóstico e/ou a remoção para outra unidade[339].

Por sua vez, a Resolução CFM nº 1.821/2007[340], que revogou a Resolução CFM nº 1.639/2002, trouxe respaldo legal ao uso cada vez mais frequente de sistemas informatizados de guarda e manuseio dos prontuários, o chamado prontuário eletrônico do paciente (PEP) ou ainda prontuário médico eletrônico (PME). A legislação veio a tornar possível a eliminação total de prontuários em suporte de papel, desde que garantidos padrões mínimos de segurança aos sistemas informatizados aptos a garantir a preservação integral dos dados, o que compreende o uso de certificação digital e método de indexação que permita criar arquivo organizado, possibilitando a pesquisa de maneira simples e eficiente.[341]

Cientes da complexidade de aprofundamento dos aspectos técnicos sobre o tema, o Conselho Federal de Medicina (CFM) e a Sociedade Brasileira de Informática em Saúde (SBIS) firmaram um convênio de cooperação técnica científica para a elaboração de requisitos e avaliação da conformidade de sistemas de informação, mediante a edição contínua de manuais de certificação e expedição de selos de qualidade. O SBISCFM mantém em seu site cartilhas explicativas sobre

---

[339] CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 1.638, de 29 de maio de 2002. Define e disciplina os procedimentos concernentes às Comissões de Revisão de Prontuários nos Conselhos Federal e Regionais de Medicina e dá outras providências. Disponível em: https://www.mpgo.mp.br/portal/arquivos/2019/09/11/15_40_13_481_Consulta_09_2019_comissão_revisora_em_unidades_de_saúde_1_pj_mineiros201900491013.pdf. Acesso em: 20/11/2023

[340] CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 1.821, de 27 de setembro de 2007. Dispõe sobre a digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes/resolucao-cfm-no-1-821-de-11-de-julho-de-2007. Acesso em: 20/11/2023

[341] KAMEDA, Paulo Pazello. *Segurança em e-Saúde: Desafios e Propostas*. Tese de Doutorado, Universidade Estadual de Campinas, 2015

a utilização de PEPs, bem como lista atualizada dos sistemas ativos certificados e auditados pelo convênio, com informações detalhas sobre o grau de segurança e as funcionalidades de cada sistema, o que denota a preocupação do setor em garantir o tráfego seguro de informações sensíveis de pacientes.[342]

No que tange aos prontuários, a migração para sistemas de informação eletrônicos apresenta inúmeras vantagens que contribuem para a eficiência na prestação dos serviços de saúde e qualidade dos dados: maior legibilidade, acurácia, compartilhamento remoto, capacidade de processar grande volume de dados, entre outros. Porém, apesar do ganho de eficiência da redução de custos no longo prazo, a migração demanda um complexo e custoso processo de implementação, já que os dados sensíveis não podem estar sujeitos ao armazenamento em bases de dados vulneráveis[343].

Pesquisas indicam que a migração para prontuários eletrônicos ainda enfrenta uma série de desafios, os quais são descritos por Serpa Neto[344] como: a falta de interoperabilidade entre os PME e outros sistemas de informação, não apenas entre diferentes sistemas, mas até dentro de um mesmo hospital ou clínica; o alto custo de sua implementação e de sua manutenção; e o impacto negativo real e/ou observado no fluxo de trabalho dos profissionais.

Apesar das barreiras técnicas e financeiras à plena migração dos estabelecimentos para sistemas eletrônicos, entende-se que a utilização das Tecnologias da Informação e Comunicação permitirão significativo salto qualitativo na prestação da saúde, de modo que há um esforço legislativo contínuo no sentido da implantação de padrões de informação e interoperabilidade entre sistemas, a permitir a melhoria e modernização dos atendimentos em saúde, bem como uma maior segurança no tratamento de dados de saúde[345].

---

[342] BRAGANÇA, Luciano; TESTA, Marco. *TIC Saúde e Privacidade: Uma Leitura Atualizada*. In: Livro Verde Sociedade da Informação no Brasil: Dimensões e Propostas. CGI.br, 2011

[343] KAMEDA, Paulo Pazello. *Segurança em e-Saúde: Desafios e Propostas*. Tese de Doutorado, Universidade Estadual de Campinas, 2015

[344] SERPA NETO, Ary. *Desafios para a Implementação de Prontuário Eletrônico do Paciente em Unidades de Terapia Intensiva Brasileiras.* Dissertação de Mestrado, Universidade de São Paulo, 2017.

[345] SERPA NETO, Ary. *Desafios para a Implementação de Prontuário Eletrônico do Paciente em Unidades de Terapia Intensiva Brasileiras.* Dissertação de Mestrado, Universidade de São Paulo, 2017.

O início foi dado pelo Ministério da Saúde, por meio da Portaria 2.073/2011[346], que definiu parâmetros de estruturação dos dados de saúde para a implementação de um Registro Eletrônico de Saúde (RES) e a interoperabilidade entre sistemas de informação do Sistema Único de Saúde (SUS) operantes em municípios, estados e União, e de saúde suplementar, com vistas ao compartilhamento de dados "em meio seguro e com respeito ao direito de privacidade" (art. 2º, II).

Do ponto de vista da privacidade no uso dos RES, enquanto a Portaria 2.073/2011[347] promove a utilização de uma arquitetura de dados e tem como escopo principal a promoção da segurança no compartilhamento de informações, a Portaria nº 940/2011[348], que regulamenta a criação do Sistema Cartão no âmbito do SUS, traz medidas expressas sobre garantia de sigilo no tratamento de dados. Além de abordar expressamente a privacidade ao colocar como um dos objetivos do cartão SUS: “Art. 4º, III segurança tecnológica da base de dados, respeitando--garantir a se o direito constitucional à intimidade, à vida privada, à integralidade das informações e à confidencialidade”.

Em consonância com a Portaria 2.073/2011[349], a Agência Nacional de Saúde (ANS), mediante as Resoluções Normativas nº 305/2012[350] e 341/2013[351], criou o

---

[346] BRASIL. Ministério da Saúde. Portaria nº 2.073, de 31 de agosto de 2011. Define os parâmetros de interoperabilidade para Registro Eletrônico de Saúde (RES) no âmbito do Sistema Único de Saúde (SUS). Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2073_31_08_2011.html. Acesso em: 20/11/2023

[347] *Ibidem*.

[348] BRASIL. Ministério da Saúde. Portaria nº 940, de 28 de abril de 2011. Institui o Sistema Cartão Nacional de Saúde (Sistema Cartão no âmbito do Sistema Único de Saúde (SUS), revoga a Portaria nº 1.206/GM/MS, de 9 de junho de 2000, e a Portaria nº 2.489/GM/MS, de 21 de outubro de 2005, e estabelece normas para o funcionamento do Sistema Cartão e a emissão do Cartão Nacional de Saúde. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt0940_28_04_2011.html. Acesso: 20/11/2023

[349] BRASIL. Ministério da Saúde. Portaria nº 2.073, de 31 de agosto de 2011. Define os parâmetros de interoperabilidade para Registro Eletrônico de Saúde (RES) no âmbito do Sistema Único de Saúde (SUS). Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2073_31_08_2011.html. Acesso em: 20/11/2023

[350] BRASIL. AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR (ANS). Resolução Normativa nº 305, de 9 de outubro de 2012. Institui o Padrão para Troca de Informação em Saúde Suplementar (TISS). Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/ans/2012/res0305_09_10_2012.html. Acesso em: 20/11/2023

[351] BRASIL. AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR (ANS). Resolução Normativa nº 341, de 29 de novembro de 2013. Atualiza o Padrão para Troca de Informação em Saúde Suplementar (TISS). Disponível em:

padrão TISS (Troca de Informação de Saúde Suplementar) como padrão obrigatório para troca de dados de beneficiários de planos privados de assistência à saúde no âmbito da saúde suplementar, com vistas a permitir a interoperabilidade entre os sistemas de informação das operadoras de saúde e à adoção de “normas nacionais de informação, terminologia única e identificadores unívocos” .

Em relação ao tratamento de dados e requisitos de segurança para equipamentos médicos, a Agência Nacional de Vigilância Sanitária (ANVISA) editou medidas regulatórias exigindo certificação compulsória de equipamentos que visam garantir a presença de mecanismos de segurança da informação, tendo em vista a importância dos dados sensíveis que trafegam em softwares médicos, bem como a interoperabilidade entre sistemas (RDC nº 40/2015).

O fato é que o debate acerca da proteção de dados de saúde tem se intensificado com o surgimento de redes de telessaúde e desenvolvimento da telemedicina, que surgem como ferramentas importantes para o enfrentamento dos desafios contemporâneos dos sistemas de saúde universais[352].

No tocante à proteção dos dados produzidos em atividades de telessaúde no SUS, compete à Coordenação Nacional de Telessaúde Brasil Redes garantir a interoperabilidade e segurança das informações:

> Art. 7º Compete à Coordenação Nacional do Telessaúde Brasil Redes: [...] V definir os padrões tecnológicos de interoperabilidade, conteúdo e segurança que permitirão a troca de informações entre os sistemas que viabilizam a operação do Telessaúde Brasil Redes e os diferentes sistemas de informação do SUS, incluídos o Cartão N acional de Saúde e o Sistema de Cadastro Nacional de Estabelecimentos de Saúde (SCNES); VI definir o conjunto de dados que fará parte do Registro Eletrônico de Saúde (RES) a partir das Teleconsultorias realizadas, visando à implementação de um registro nacional e longitudinal, conforme Portaria nº 2.073/GM MS, 2073/GM/MS de 31 de agosto de 2011; e (Retificado no DOU nº 209 de 31.10.2011, Seção 1, página 74)[353]

https://bvsms.saude.gov.br/bvs/saudelegis/ans/2013/res0341_27_11_2013.html. Acesso em: 20/11/2023

[352] SERPA NETO, Ary. *Desafios para a Implementação de Prontuário Eletrônico do Paciente em Unidades de Terapia Intensiva Brasileiras*. Dissertação de Mestrado, Universidade de São Paulo, 2017.

[353] BRASIL. *Ministério da Saúde. Portaria nº 2.073, de 31 de agosto de 2011. Define os parâmetros de interoperabilidade para Registro Eletrônico de Saúde (RES) no âmbito do Sistema Único de Saúde (SUS).* Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2073_31_08_2011.html. Acesso em: 20/11/2023

Para além das inovações na comunicação entre profissionais da saúde, as tecnologias da informação e comunicação trouxeram possibilidades inovadoras para uso da telemedicina diretamente na relação profissional e paciente, tais como a teletriagem médica, a teleconsulta, telediagnóstico, telecirurgia, teleconferência de ato cirúrgico.

A atividade, que está em pleno desenvolvimento na prática, chegou a ser regulamentada pelo CFM na Resolução CFM nº 2.227[354], no dia 13 de dezembro 2018, cujo objetivo era permitir e regulamentar a prática da modalidade no país, entretanto, devido a um elevado número de críticas e propostas de alteração por diversas entidades médicas, além do impacto social envolvido na medida, o órgão voltou atrás e revogou seu próprio ato, a fim de amadurecer a discussão e chegar a um novo texto, que segue em debate.

É relevante salientar, por último, que a prática crescente da telemedicina adicionará uma camada adicional de complexidade e exigirá regulamentação mais específica no que diz respeito aos dados de saúde. Isso se tornou especialmente crucial no contexto da pandemia de Covid-19, onde a coleta e tratamento de dados pessoais, como imagens, textos e áudios de pacientes, tornaram-se massivos. A magnitude dessa coleta demandou protocolos de registro e transmissão altamente seguros, cuja implementação bem-sucedida dependeu de garantias operacionais, como a estabilidade no fornecimento de energia elétrica e medidas eficazes de segurança contra vírus e invasões de hackers.

Nesse sentido, a complexidade emergente na regulamentação dos dados de saúde, impulsionada pela expansão da telemedicina, estabelece uma transição natural para o próximo capítulo. No capítulo subsequente, serão analisados os impactos e repercussões da coleta e tratamento massivo de dados pessoais durante a pandemia de Covid-19. A discussão abordará questões relacionadas ao rastreamento de contatos, monitoramento de movimento e coleta massiva de dados de saúde e os desafios enfrentados na manutenção da integridade e confidencialidade desses dados, fomentando uma compreensão mais aprofundada sobre o tema em questão.

---

[354] CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.227, de 13 de dezembro de 2018. Regulamenta a prática da telemedicina no país. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2018/2227\. Acesso em:20/11/2023.

5. IMPACTOS E REPERCUSSÕES DA COLETA E TRATAMENTO DE DADOS PESSOAIS NO CONTEXTO DA PANDEMIA DE COVID-19

A pandemia de COVID-19, que emergiu no final de 2019[355], introduziu uma nova dinâmica no cenário global, transformando significativamente a forma como a sociedade interage e como as instituições operam. Nesse contexto, a coleta e o tratamento de dados pessoais assumiram um papel central nas estratégias de contenção da propagação do vírus e na gestão da crise de saúde pública. A utilização intensiva de dados se tornou uma ferramenta essencial, mas também suscitou preocupações sobre privacidade, segurança e governança.

A coleta massiva de dados pessoais ganhou destaque em resposta à pandemia, sendo utilizada para rastreamento de contatos, monitoramento de movimentações e implementação de medidas de distanciamento social. Governos e autoridades de saúde, em colaboração com empresas de tecnologia, lançaram mão de aplicativos e sistemas que permitem o rastreamento eficiente de indivíduos infectados e a notificação de potenciais exposições. Essas iniciativas, embora fundamentais para conter a disseminação do vírus, desencadearam debates éticos e legais sobre o equilíbrio entre o bem coletivo e a proteção da privacidade individual.

A rápida adoção de tecnologias de vigilância levantou questões sobre a extensão do poder estatal e a preservação dos direitos fundamentais dos cidadãos. As transparências no uso dessas ferramentas, bem como garantias robustas de anonimato e segurança dos dados, tornaram-se imperativos para mitigar preocupações legítimas da sociedade em relação à invasão da privacidade. Instituições e empresas tiveram que enfrentar o desafio de desenvolver e implementar práticas éticas de coleta e tratamento de dados, alinhadas aos princípios de proteção à privacidade.

Além disso, o contexto da pandemia evidenciou a necessidade de marcos regulatórios mais adaptáveis e abrangentes para lidar com situações de emergência. As legislações existentes muitas vezes não estavam preparadas para

[355] Primeiro contágio pelo coronavírus teria acontecido em novembro, diz jornal, UOL. 13 de mar. 2020.Disponível em: https://noticias.uol.com.br/ultimas-noticias/efe/2020/03/13/jornal-afirma-que-primeiro-contagioda-covid-19-na-china-ocorreu-em-novembro.htm. Acesso em: 20/11/2023

lidar com as demandas específicas da coleta e tratamento de dados em um cenário de crise global. A revisão e aprimoramento desses marcos regulatórios tornaram-se cruciais para garantir que as medidas adotadas não apenas fossem eficazes na contenção da pandemia, mas também respeitassem os direitos individuais e a privacidade.

A interseção entre saúde pública e tecnologia colocou em evidência a necessidade de padrões éticos na coleta e tratamento de dados, orientando o desenvolvimento de soluções inovadoras. A confiança da sociedade nas instituições que coletam e utilizam dados é um elemento vital para o sucesso dessas estratégias, destacando a importância de uma comunicação transparente e educativa sobre as práticas adotadas. A promoção da literacia digital tornou-se uma prioridade para empoderar os indivíduos a compreenderem o impacto da coleta de dados em seu cotidiano.

Além disso, a pandemia acelerou mudanças nas dinâmicas de trabalho, saúde e educação, impulsionando a digitalização de setores inteiros. Esse cenário reforça a necessidade de uma discussão mais ampla sobre a coleta e tratamento de dados em diferentes esferas da vida cotidiana, estendendo-se para além do contexto de emergência. A partir disso, esse capítulo pretende fazer uma reflexão sobre os impactos e repercussões da coleta e tratamento de dados pessoais durante a pandemia de COVID-19, bem como promover um diálogo sobre o futuro da sociedade digital pós-pandêmica.

5.1 Os mecanismos de vigilância e monitoramento via dados celulares, geolocalização e rede de contatos como ferramentas de prevenção e combate ao coronavírus

Desde os primeiros registros na China, entre novembro e dezembro de 2019, até a declaração de Pandemia pela Organização Mundial de Saúde (OMS)[356] em março do ano seguinte, a COVID-19, causada pelo Coronavírus (SARS-CoV-2), desencadeou uma crise sanitária global. Essa crise mobilizou esforços

[356] OMS afirma que COVID-19 é agora caracterizada como pandemia, OPAS Brasil. 11 de mar. 2020. Disponível em: https://www.paho.org/bra/index.php?option=com_content&view=article&id=6120:oms-afirma-que-covid-19-e-agora-caracterizada-como-pandemia&Itemid=812. Acesso em: 20/11/2023

internacionais para desenvolver respostas rápidas diante da rápida disseminação da doença. Governos em todo o mundo adotaram diversas medidas para conter a propagação do vírus.

Diante da necessidade de estratégias além das medidas iniciais de controle epidêmico e isolamento, surgiram ações mais alinhadas com os avanços tecnológicos atuais. Isso incluiu a coleta e o tratamento de dados pessoais para monitoramento por meio de geolocalização (dados agregados de dispositivos móveis), identificação e rastreamento de pacientes e indivíduos. O objetivo era gerenciar os riscos de contágio, verificar a adesão ao isolamento social e garantir o cumprimento das medidas restritivas. A Comunidade Internacional e empresas privadas responderam com grande mobilização para desenvolver tecnologias que possibilitassem a obtenção de dados pessoais por meio desses métodos.

Na Europa, a Comissão Europeia emitiu, em abril de 2020, diretrizes para o desenvolvimento de tecnologias de rastreamento de contatos para os Estados-membros da União Europeia. O documento ressaltou a importância dessas tecnologias estar em conformidade com o Regulamento Geral de Proteção de Dados (RGPD) e proteger os direitos e princípios ali estabelecidos[357].

No setor privado, as gigantes tecnológicas Apple e Google rapidamente formaram uma parceria para garantir a interoperabilidade entre os sistemas iOS e Android. Isso resultou na criação de uma ferramenta de rastreamento para a COVID-19, que utiliza rastreamento de localização, incentiva a autodeclaração de sintomas pelos usuários e envia alertas automáticos sobre possíveis contatos com pacientes infectados. Esse sistema apresenta semelhanças com as orientações do Contact Tracing, que envolve a troca de identificadores anônimos entre telefones próximos via Bluetooth[358].

No Brasil, a Prefeitura de Recife implementou uma política de geolocalização em parceria com a startup In Loco. Isso permitiu o monitoramento anônimo de mais de 700 mil aparelhos celulares para medir a adesão ao isolamento, subsidiando

[357] SCHREIBER, Mariana. Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco sua privacidade? BBC News Brasil. 21 abr. 2020. Disponível em: https://www.bbc.com/portuguese/brasil-52357879. Acesso em: 20/11/2023

[358] ALMEIDA, Bethania Araujo et. al. *Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global.* Ciência & Saúde Coletiva. v. 25(Supl.1): 2487-2492, 2020. Disponível em: https://doi.org/10.1590/1413-81232020256.1.11792020. Acesso em: 20/11/2023

políticas de conscientização mais eficazes[359]. O Estado de São Paulo seguiu a capital nordestina ao adotar a infraestrutura das principais operadoras de telefonia para obter dados de geolocalização, criando o Sistema de Monitoramento Inteligente (SIMI)[360]. Em todos esses casos, os Estados enfatizaram que as tecnologias eram baseadas em dados anonimizados, minimizando riscos à identificação do usuário.

A anonimização de dados, definida como a aplicação de medidas técnicas para impossibilitar a associação direta ou indireta dos dados ao indivíduo, é uma prática adotada. No entanto, a preocupação surge quando dados, mesmo anonimizados, podem ser identificados ou tornar-se identificáveis por meio da integração e cruzamento entre diversas bases de dados[361].

A LGPD estabelece que dados anonimizados não são considerados pessoais, a menos que o processo de anonimização seja revertido com meios próprios ou esforços razoáveis[362]. No entanto, a possibilidade de identificação persiste, como observam Ehrhardt Júnior e Peixoto:

> Em um estudo que é um marco na privacidade informacional, Latanya Sweeney conduziu experimentos utilizando dados do censo dos Estados

[359] ARIMETHEA, Bruna; CAPELAS, Bruno. InLoco e Prefeitura de Recife vão monitorar 700 mil celulares em prol de isolamento social. O Estado de S. Paulo. 25 mar. 2020. Disponível em: https://link.estadao.com.br/noticias/inovacao,inloco-e-prefeiturade-recife-vao-monitorar-700-mil-celulares-emprol-de-isolamento-social,70003248010. Acesso em: 20/11/2023

[360] Nesse particular, insta registrar que o citado sistema foi alvo de questionamentos através de mandados de segurança impetrados por cidadãos que alegavam violação aos seus direitos pessoais pela plataforma. No entanto, a alegação foi afastada pelo TJSP que, ao reconhecer a legalidade do SIMI, justificou: “essa decisão reconhece que o monitoramento realizado pelo Estado de São Paulo vem sendo feito dentro dos limites constitucionais e infraconstitucionais, evitando a interrupção da utilização de ferramenta de grande importância para o combate à propagação do COVID-19”. TJSP reconhece legalidade do Sistema de Monitoramento Inteligente (SIMI). Procuradoria Geral do Estado de São Paulo. 08 jun. 2020. Disponível em: http://www.portal.pge.sp.gov.br/tjspreconhece-legalidade-do-sistema-de-monitoramento-inteligente-simi/. Acesso em: 20/11/2023

[361] Pontuam Almeida et. al.: “Em geral, dados anonimizados não são considerados dados pessoais ou o são com algumas ressalvas, enquanto dados pseudoanomizados são tidos como dados pessoais pelo potencial de
reidentificação dos indivíduos através da utilização do código chave, ainda que disponham potencialmente de um nível maior de segurança. Em virtude da possibilidade de identificação dos dados, mesmo anonimizados17, são necessárias combinações de vários procedimentos para preservar a privacidade dos indivíduos, particularmente quando ocorre integração entre bases de dados. ” ALMEIDA, Bethania Araújo et. al. *Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global*. Ciência & Saúde Coletiva. v. 25, supl. 1, 2487-2492, 2020. Disponível em: https://doi.org/10.1590/141381232020256.1.11792020. Acesso em: 20/11/2023

[362] EHRHARDT JÚNIOR, Marcos; PEIXOTO, Erick Lucena Campos. *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. 51

> Unidos de 1990, apontando que 87% da população norte-americana à época (216 milhões de 248 milhões de pessoas) era identificável de forma única apenas pela combinação de três informações: do ZIP *code*, da data de nascimento completa e do sexo. Metade da população dos Estados Unidos (132 milhões, 53%) era identificável apenas utilizando- se a informação do lugar ("*city, town, or municipality"*), do sexo e data de nascimento. Indicando o *county*, o sexo e a data de nascimento, 18% da população poderia ser identificada[363].

No contexto da persistência do risco residual de identificação de dados inicialmente considerados como anonimizados, uma matéria veiculada no site do jornal The Intercept destacou um incidente em que foi possível identificar dois usuários da operadora de telefonia Vivo. Isso ocorreu a partir de bases de dados comercializadas como anônimas para a Secretaria de Turismo do Estado do Espírito Santo. A planilha disponibilizada no site da Secretaria continha informações de milhares de pessoas não identificadas. Contudo, ao combinar e cruzar essas informações com outras bases, tornou-se possível chegar a perfis específicos e, consequentemente, identificar pessoas específicas[364].

A discussão sobre a anonimização dos dados utilizados por tais sistemas foi levantada no âmbito da Administração Direta Federal, visando investigar possíveis discrepâncias entre as tecnologias desenvolvidas e a Lei Geral de Proteção de Dados (LGPD). Mesmo que a LGPD estivesse em vacatio legis na época, seu conteúdo não poderia ser ignorado, pois seus princípios ecoam em outras normas vigentes, justificando assim sua observância. Em resposta a essa questão, a Secretaria de Telecomunicações do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) emitiu a Nota Informativa nº 1192/2020/SEI-MCTIC, indicando que, em uma análise preliminar, não havia impedimentos jurídicos para o compartilhamento de dados de geolocalização de usuários de serviços de telecomunicações, desde que organizados de forma anônima e agregada[365].

---

[363] EHRHARDT JÚNIOR, Marcos; PEIXOTO, Erick Lucena Campos. *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. 51

[364] DIAS, Tatiana. Vigiar e lucrar: nós identificamos dois clientes dos dados de localização 'anônimos' vendidos pela vivo. The Intercept Brasil. Disponível em: https://theintercept.com/2020/04/13/vivo-venda-localizacaoanonima/. Acesso em: 20/11/2023

[365] URUPÁ, Marcos. Para AGU, compartilhamento de dados de geolocalização não fere LGPD e Constituição. Teletime. Disponível em: https://teletime.com.br/13/04/2020/para-agu compartilhamento-de-dados-degeolocalizacao-nao-fere-lgpd-e-constituicao-federal/. Acesso em: 20/11/2023

Após a manifestação do MCTIC, a Advocacia-Geral da União (AGU) emitiu um parecer favorável ao compartilhamento de dados de usuários de serviços de telecomunicações para fins de combate ao coronavírus, desde que as informações fossem fornecidas ao Governo conforme as condições recomendadas pelo MCTIC. A AGU, respaldada pelos preceitos da LGPD, sustentou que os dados anonimizados não são considerados pela referida lei. O órgão reconheceu que tais dados não possibilitam a identificação do titular quando são utilizados meios técnicos razoáveis e disponíveis durante seu tratamento[366].

Não obstante o reconhecimento da importância dessas iniciativas, surgem, concomitantemente ao debate, preocupações sobre o volume de dados pessoais coletados e processados sob a justificativa da saúde pública e interesse coletivo. Especial atenção é dada às possíveis destinações futuras dessas informações quando a finalidade que orientou sua coleta e tratamento não está mais presente. Assim, as instituições responsáveis pelo processamento desses dados, sejam públicas ou privadas, enfrentam uma desconfiança justificada em relação ao respeito à privacidade e à proteção de dados dos cidadãos cujas informações pessoais foram coletadas[367].

Importante exemplo de ser mencionado seria a China, a qual evidencia uma completa ausência de consentimento por parte dos titulares de dados, caracterizando-se por um reconhecimento cultural da onipresença estatal[368]. Tal país, internacionalmente conhecida pela extensa utilização de tecnologias de monitoramento, implementou uma ampla rede que abrange desde a coleta de dados sobre as viagens dos cidadãos até a vigilância de redes sociais, internet e a

---

[366] URUPÁ, Marcos. Para AGU, compartilhamento de dados de geolocalização não fere LGPD e Constituição. Teletime. Disponível em: https://teletime.com.br/13/04/2020/para-agu-compartilhamento-de-dados-degeolocalizacao-nao-fere-lgpd-e-constituicao-federal/. Acesso em: 20/11/2023

[367] Almeida frisa que tais desconfianças e questionamentos não visam inibir o uso de dados pessoais como resposta à pandemia, mas buscam o equilíbrio entre os interesses individuais e coletivos conjugados, através de salvaguardas regulatórias. ALMEIDA, Bethania Araujo et. al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. Ciência & Saúde Coletiva. v. 25(Supl.1): 2487-2492, 2020. Disponível em: https://doi.org/10.1590/1413-81232020256.1.11792020. Acesso em: 20/11/2023

[368] Os chineses sabem há muito tempo que são rastreados pelo sistema de vigilância eletrônica mais sofisticado do mundo. A emergência do coronavírus tirou parte dessa tecnologia das sombras, fornecendo às autoridades uma justificativa para métodos abrangentes de controle social de alta tecnologia. Coronavirus brings China's surveillance state out of the shadows. The Japantimes. Disponível em: https://www.japantimes.co.jp/news/2020/02/10/asia-pacific/coronavirus-china-surveillance-state-privacyrights/#. Xk2CpypKiM9. Acesso em: 20/11/2023

aplicação de softwares de reconhecimento facial em locais públicos[369]. Embora esses mecanismos tenham contribuído significativamente para conter a propagação da doença, não são infrequentes os exemplos que suscitam debates ético-jurídicos sobre a violação da privacidade em detrimento do bem coletivo[370].

Por outro lado, a Coreia do Sul adotou uma abordagem distinta, empregando o monitoramento dos cidadãos por meio do rastreamento de contatos e realizando testes em massa. Essa estratégia envolveu parcerias público-privadas para o desenvolvimento de tecnologias de testagem, incluindo o RT-PCR, aprovando o uso desses testes para casos suspeitos e realizando o desenvolvimento rápido dos testes em colaboração com os governos locais. A modalidade de drive-thru foi inaugurada para ampliar os diagnósticos e reduzir a exposição dos profissionais de saúde. Essa abordagem foi possível devido à resposta coletiva da população diante da crise, demonstrando a disposição de tomar medidas não apenas para proteger a saúde individual, mas também para preservar o bem-estar coletivo[371].

No entanto, ao analisar esses exemplos, é imperativo exercer certa cautela, considerando a dinâmica da concepção de privacidade que se adapta a cada cultura de maneira específica. Como discutido anteriormente, a concepção de privacidade é dinâmica e culturalmente variável. Modesto[372] explica que, ao contrário da ênfase ocidental na privacidade pessoal, os asiáticos tendem a aceitar práticas invasivas em favor da coletividade. No entanto, isso não elimina a possibilidade de identificar abusos por parte do Estado, mesmo em contextos orientais, destacando a importância dos elementos fundamentais da ideia de privacidade, como a noção de solidão, segredo e controle sobre a esfera pessoal[373].

---

[369] CARBINATTO, Bruno. China está usando vigilância em massa para combater coronavírus. Abril. 25 mar.2020. Disponível em: https://super.abril.com.br/tecnologia/china-esta-usando-tecnologias-de-vigilancia-emmassa-para-combater-coronavirus/. Acesso em: 20/11/2023

[370] CURY, Maria Eduarda. Como a China usou o WeChat para conter a covid-19 - e vigiar as notícias. Exame. 4abr. 2020. Disponível em: https://exame.com/tecnologia/como-a-china-usou-o-wechat-para-conter-a-covid-19-evigiar-as-noticias/. Acesso em: 20/11/2023

[371] KANG, Margareth. Uso dos dados pessoais na Coreia do Sul no combate ao coronavírus: O que podemos aprender com a Coreia do Sul? Disponível em: https://www.jota.info/opiniao-e-analise/artigos/uso-dos-dadospessoais-na-coreia-do-sul-no-combate-ao-coronavirus-03052020. Acesso em: 20/11/2023

[372] MODESTO, Jéssica Andrade. O direito à privacidade na sociedade da informação à luz da lei geral de proteção de dados pessoais: uma análise da (in)efetividade da lei nº 13.709/2018 no brasil a partir do estudo comparativo com o regulamento geral de proteção de dados da união europeia. 2021. 364 f. Dissertação (Mestrado em Direito) - Universidade Federal de Alagoas, Alagoas, 2021.

[373] MODESTO, Jéssica Andrade. O direito à privacidade na sociedade da informação à luz da lei geral de proteção de dados pessoais: uma análise da (in)efetividade da lei nº 13.709/2018 no brasil

Ao abordar a possível colisão entre direitos fundamentais, especialmente entre privacidade e interesse público, é fundamental observar que a doutrina e jurisprudência destacam a ausência de um direito absoluto à privacidade. Nesse contexto, Silva, Modesto e Ehrhardt Júnior[374] explicam que a coexistência de direitos fundamentais em situações de conflito deve ser solucionada por meio da ponderação. Essa técnica interpretativa visa equilibrar os bens envolvidos, considerando as circunstâncias específicas de cada situação. No contexto da pandemia, argumentam esses autores[375], é possível permitir restrições parciais ao direito à privacidade em face da necessidade de preservar direitos coletivos, como o direito à vida e à saúde.

É relevante mencionar a contribuição legislativa por meio da Lei nº 13.979, de 6 de fevereiro de 2020, que regulamentou as medidas para enfrentar a emergência de saúde pública decorrente da COVID-19. Essa legislação tornou obrigatório o compartilhamento de dados pessoais com a Administração Pública e, se solicitado por autoridade sanitária, estendeu essa obrigação ao setor privado. Tal regulamentação buscou equilibrar a necessidade de informações para a gestão da pandemia com a proteção dos direitos individuais, estabelecendo um marco legal claro diante do cenário desafiador apresentado pela crise sanitária global[376].

Ao ser examinada sob a ótica da Lei Geral de Proteção de Dados (LGPD), observa-se que a Lei 13.979/20 buscou estabelecer de maneira explícita a finalidade da coleta de dados em seu artigo 6º. Este dispositivo, por sua vez, encontra respaldo no artigo 11 da LGPD, que autoriza o tratamento de dados sensíveis pelas autoridades públicas quando essencial para a preservação da vida ou da integridade física do titular ou de terceiros.

---

a partir do estudo comparativo com o regulamento geral de proteção de dados da união europeia. 2021. 364 f. Dissertação (Mestrado em Direito) - Universidade Federal de Alagoas, Alagoas, 2021.

[374] SILVA, Gabriela Buarque Pereira; MODESTO, Jéssica Andrade; EHRHARDT JÚNIOR, Marcos. *O tratamento de dados pessoais no combate à covid-19: entre soluções e danos colaterais*. In: EHRHARDT JÚNIOR, Marcos; CATALAN, Marcos; Malheiros Pablo (Coord.). Direito civil e tecnologia. Belo Horizonte: Fórum, 2020

[375] *Ibidem.*

[376] Art. 6º É obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação.
§ 1º A obrigação a que se refere o caput deste artigo estende-se às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária.
§ 2º O Ministério da Saúde manterá dados públicos e atualizados sobre os casos confirmados, suspeitos e em investigação, relativos à situação de emergência pública sanitária, resguardando o direito ao sigilo das informações pessoais. (BRASIL, Lei nº 13.979/2020)

Quanto aos dados sensíveis, a LGPD dedicou atenção especial a essa categoria restrita, e com razão. De maneira geral, os dados sensíveis constituem uma classe de informações pessoais que podem acarretar riscos e vulnerabilidades significativas aos direitos e liberdades fundamentais dos titulares. Isso se deve ao fato de que, ao abranger informações como origem racial, convicção religiosa, opinião política, dados relacionados à saúde ou à vida sexual, entre outros, os dados sensíveis têm o potencial de resultar em discriminação ou tratamento diferenciado[377].

A legislação concede tratamento ainda mais específico quando esses dados estão relacionados à saúde do titular. O artigo 11 estipula que o tratamento dessas informações só pode ocorrer mediante consentimento expresso e destacado do titular. Apesar da previsão em relação ao consentimento expresso do titular, a LGPD regulamenta situações em que o tratamento de dados sensíveis pode ocorrer sem esse consentimento, como quando necessário para cumprir uma obrigação legal ou regulatória, executar políticas públicas, conduzir estudos por órgãos de pesquisa, proteger a vida ou a integridade física do titular ou de terceiros, assegurar a prevenção à fraude e a segurança do titular, entre outras[378].

Dessa forma, ao retomar a análise do tema à luz da Lei 13.379/2020, destaca-se que a aplicação do artigo 6º dessa lei, mesmo quando compatível com a exceção de dispensa do consentimento do titular prevista na LGPD, deve estar alinhada aos princípios indicados nesta última legislação, como ocorreu em relação à finalidade específica e à segurança dos dados pessoais coletados.

5.2 A (in) constitucionalidade da medida provisória nº 954/20 e a abertura para o reconhecimento de um direito fundamental à proteção de dados

A discussão acerca dos instrumentos de monitoramento e rastreamento durante a pandemia ocorreu em um cenário desprovido de legislação específica, apesar da introdução tardia da Lei Geral de Proteção de Dados (LGPD). Isso levou

[377] SILVA, Gabriela Buarque Pereira; MODESTO, Jéssica Andrade; EHRHARDT JÚNIOR, Marcos. O tratamento de dados pessoais no combate àcovid-19: entre soluções e danos colaterais. In: EHRHARDT JÚNIOR, Marcos; CATALAN, Marcos; Malheiros Pablo (Coord.). Direito civil e tecnologia. Belo Horizonte: Fórum, 2020

[378] *Ibidem.*

as autoridades governamentais brasileiras a utilizar mecanismos regulatórios alternativos para gerenciar as medidas públicas necessárias no início da crise. Uma dessas tentativas de mitigar a inviolabilidade do direito à privacidade[379] em resposta à crise sanitária foi a emissão da Medida Provisória nº 954/20.

Seu propósito era estabelecer regulamentações sobre o compartilhamento de dados por empresas de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE), visando apoiar a produção estatística oficial durante a emergência de saúde pública causada pelo COVID-19, conforme previsto na Lei nº 13.979/2020[380].

No entanto, a constitucionalidade dessa medida legislativa foi questionada por meio de cinco Ações Diretas de Inconstitucionalidade (ADI), destacando-se a ADI nº 6.387/DF. Iniciada pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) em abril de 2020, essa ADI alegou, em síntese, a inconstitucionalidade formal da MP nº 954/20 por não observar os pressupostos constitucionais de urgência e relevância, conforme estabelecido no artigo 62 da Constituição Federal.

---

[379] Não obstante, na esteira dos ensinamentos de Silva, Modesto e Ehrhardt, adverte-se que a eficácia do direito à privacidade não está adstrita à vigência da LGPD, nem é a ela condicionada. A fundamentalidade deste direito é amplamente sedimentada na estrutura jurídica vigente, conforme tem-se abordado. SILVA, Gabriela Buarque Pereira; MODESTO, Jéssica Andrade; EHRHARDT JÚNIOR, Marcos. O tratamento de dados pessoais no combate àcovid-19: entre soluções e danos colaterais. In: EHRHARDT JÚNIOR, Marcos; CATALAN, Marcos; Malheiros Pablo (Coord.). Direito civil e tecnologia. Belo Horizonte: Fórum, 2020

[380] Acerca das disposições, o texto previu que as concessionárias de serviço de telecomunicações deveriam disponibilizar, ao IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas, que serão utilizados direta e exclusivamente pela fundação para produção de estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. (art. 2º). Ademais, verberou que os dados compartilhados com a Fundação teriam caráter sigiloso e, portanto, seriam utilizados exclusivamente para as finalidades elencadas nos arts. 1º e 2º e não serão utilizados como objeto de certidão ou meio de prova em processo administrativo, fiscal ou judicial (art. 3º). O §1º do art. 3º estabeleceu que é vedado ao IBGE disponibilizar os dados coletados a quaisquer empresas públicas ou privadas ou a órgãos ou entidades da administração pública direta ou indireta de quaisquer dos entes federativos. O §2º desse dispositivo trouxe importante instrumento de controle social, segundo o qual o IBGE informaria, em seu sítio eletrônico, as situações em que os dados compartilhados fossem utilizados e divulgaria relatório de impacto à proteção de dados pessoais. Em arremate, o artigo 4º da Medida Provisória em tela explicita seu caráter temporário ao aduzir que “superada a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), as informações compartilhadas serão eliminadas das bases de dados da Fundação IBGE” (BRASIL, 2020). Conquanto, elenca hipótese excepcional de utilização dos dados pelo IBGE em 30 (trinta) dias contados do fim da situação de emergência de saúde pública de importância internacional se houver necessidade de conclusão de produção estatística oficial.

Além disso, argumentou-se a inconstitucionalidade material por estar em desacordo com princípios como a dignidade da pessoa humana, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, o sigilo dos dados e o direito à autodeterminação informativa, bem como o princípio da proporcionalidade[381].

Esta discussão evidencia a possível incompreensão legislativa dos princípios e bases legais que orientam a proteção de dados, conforme buscado pela LGPD. A MP 954/20, ao tratar dos dados pessoais, foi vaga e não atendeu aos princípios regulamentados pela LGPD. A medida limitou-se a estabelecer genericamente sua finalidade, sem justificar adequadamente os requisitos excepcionais e indispensáveis à sua edição, especialmente em relação ao combate à COVID-19 em detrimento do direito à privacidade[382].

Além disso, a MP 954/20 não ofereceu clareza quanto à proteção dos dados coletados, ao manuseio adequado e à utilização, e não definiu procedimentos de fiscalização das posturas a serem adotadas. A concessão da medida liminar pela Suprema Corte[383] brasileira para suspender a eficácia da MP 954/20, com base nos fundamentos de proteção dos direitos fundamentais à privacidade, intimidade e proteção de dados, destaca a importância de equilibrar medidas excepcionais com a preservação desses direitos[384].

Tal decisão do Supremo Tribunal Federal não apenas estabeleceu um precedente significativo para a proteção de dados, mas também influenciou o entendimento da ADPF 695, que afirmou a ausência de autorização irrestrita para o livre fluxo de compartilhamento de informações de dados pessoais no âmbito do Poder Público. Esta decisão ressalta a necessidade de uma base legal sólida e

---

[381] GOIATÁ, Sarah Rêgo; RAMOS, Rafael Barreto. Pandemia da covid-19 e direito Fundamental à privacidade no estado Democrático de direito: (in)constitucionalidade das mitigações ao Direito à Privacidade em Tempos de Crise Sanitária à luz da Medida Provisória n.º 954/20 e ADI n.º 6.387/DF. Anais do Congresso Internacional: preservar e fortalecer a democracia em tempos de pandemia. Belo Horizonte: Conhecimento Editora, 2020

[382] *Ibidem*.

[383] BRASIL. Supremo Tribunal Federal. Referendo na medida cautelar na ação direta de inconstitucionalidade 6.387. Distrito Federal. Relatora: Ministra Rosa Weber. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 20/11/2023

[384] GOIATÁ, Sarah Rêgo; RAMOS, Rafael Barreto. Pandemia da covid-19 e direito Fundamental à privacidade no estado Democrático de direito: (in)constitucionalidade das mitigações ao Direito à Privacidade em Tempos de Crise Sanitária à luz da Medida Provisória n.º 954/20 e ADI n.º 6.387/DF. Anais do Congresso Internacional: preservar e fortalecer a democracia em tempos de pandemia. Belo Horizonte: Conhecimento Editora, 2020

critérios substantivos para salvaguardar as expectativas dos titulares e seus direitos quando há mudança de finalidade no tratamento de dados[385].

Adicionalmente, no ano de 2022, conforme já mencionado no capítulo anterior, fora aprovada a EC 115/2022, que a proteção de dados pessoais como um direito fundamental. Tal Emenda, além de estabelecer a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais, reforçou a importância atribuída à proteção de dados como um elemento essencial dos direitos fundamentais no contexto legislativo brasileiro.

5.3 Entre desafios e compatibilizações: o papel da LGPD na tutela de direitos e liberdades fundamentais no pós-pandemia

A pandemia global de COVID-19 desencadeou transformações profundas nas esferas social, econômica e política em todo o mundo. É evidente que as medidas restritivas, especialmente o isolamento social, provocaram uma reconfiguração significativa na vida cotidiana. Em consequência, testemunhou-se uma invasão marcante de ferramentas tecnológicas destinadas a enfrentar os desafios impostos pelo distanciamento. Contudo, é imperativo reconhecer que sempre que restrições são aplicadas às liberdades individuais, em particular ao direito à privacidade, surgem legítimas preocupações.

No rastro das interrogações suscitadas a época da pandemia, surgiu uma apreensão generalizada em diversos setores da sociedade sobre as consequências a serem experimentadas no pós-pandemia. Um exemplo notável foi a Lei nº 13.982, de 02 de abril de 2020, que instituiu o programa social Auxílio Emergencial no Brasil[386], o qual atualmente não se encontra mais em vigor.

Durante a vigência dessa iniciativa, os solicitantes do benefício, caso não possuíssem contas bancárias no momento do cadastro, tinham a opção de criar

[385] BRASIL. Supremo Tribunal Federal. Referendo na medida cautelar na ação direta de inconstitucionalidade 6.387. Distrito Federal. Relatora: Ministra Rosa Weber. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 20/11/2023

[386] Caixa encerra pagamento do auxílio emergencial após sete meses. Agência Brasil. 31 out. 2021. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2021-10/caixa-encerra-pagamento-do-auxilioemergencial-apos-sete-meses. Acesso em: 20/11/2023

contas digitais regulamentadas pela Caixa Econômica Federal exclusivamente para essa finalidade[387].

Tal procedimento resultou na inclusão de uma camada carente da população brasileira, até então desconhecida no cenário econômico, incorporando cerca de 30 milhões de novos consumidores nas bases de dados do país. Essa inclusão, a longo prazo, pode precipitar discriminações na concessão de crédito, baseadas na análise do perfil do consumidor e na categorização do beneficiário do programa[388].

Oliva[389] argumenta que os efeitos dessa inclusão no Auxílio Emergencial podem se refletir na concessão de crédito, transformando consumidores antes considerados incógnitos para os sistemas de análise de risco financeiro em figuras facilmente identificáveis. Esse cenário reforça a natureza excludente do mercado de crédito e viola a autodeterminação informativa do consumidor[390]. Importante destacar que a não discriminação é um princípio abrangido pela Lei Geral de Proteção de Dados (LGPD), proibindo a utilização de dados pessoais para fins discriminatórios, ilícitos ou abusivos.

Além disso, há uma justificada preocupação de que os efeitos dessa nova configuração social possam impactar as crianças e adolescentes, considerados titulares com notória vulnerabilidade. A substituição das salas de aula por ambientes online de videoconferência representa riscos substanciais à privacidade, dada a potencial utilização dos dados pessoais coletados para fins comerciais[391].

---

[387] OLIVA, Afonso Carvalho de. O auxílio emergencial e a vigilância dos consumidores pós-covid-19. In: BIONI, Bruno Ricardo et. al. Os dados e o vírus: Pandemia, proteção de dados e democracia. São Paulo: Reticências Creative Design Studio, 2020

[388] *Ibidem*.

[389] *Ibidem*.

[390] Anota Wimmer: “No caso do pagamento do auxílio emergencial, por exemplo, acórdão do Tribunal de Contas da União – TCU (2020) apontou para os riscos de inclusão e exclusão indevida de beneficiários, com identificação de seis fatores de risco: (i) baixa integração dos cadastros públicos; (ii) desatualização do Cadastro Único; (iii) dificuldade para identificação inequívoca em cadastros públicos; (iv) limitações para verificação de composição familiar; (v) limitações para verificação de vínculos de emprego e renda; e, (vi) limitações para cadastramento de pessoas com menor acesso a serviços públicos. Para endereçar tais fragilidades, o acórdão apresentou diversas recomendações quanto ao aprimoramento do cruzamento de dados contidos em bases do Poder Público.” WIMMER, Miriam. Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia. Revista Brasileira de Políticas Públicas. v. 11, n. 1 (2021). pp. 123-142. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/7136. Acesso em: 20/11/2023

[391] A Federal Trade Comission (FTC), nos Estados Unidos, conduziu uma pesquisa com 212 sites em 1998 e descobriu que 89% deles coletavam informações pessoais de crianças. Daqueles que coletaram dados de crianças, 46% não divulgaram esse fato ou explicaram como as informações foram usadas. No Brasil, por meio da pesquisa “TIC Kids Online Brasil 2017”, realizada pelo Nic.br com 20 (vinte) aplicativos de público infantil mais buscados no Brasil, mesmo após mais de 20 anos

A LGPD estabelece, em seu artigo 14, que o tratamento de dados de crianças e adolescentes deve ser guiado pelo princípio do melhor interesse e pela necessidade de proteção integral preconizada no Estatuto da Criança e do Adolescente (ECA).

Em um contexto de aumento exponencial de crimes cibernéticos, como o sequestro de dados, é igualmente relevante observar os perigos associados a outra realidade introduzida pela pandemia: o home office. Tanto no setor público quanto na iniciativa privada, a transição do trabalho para atividades telepresenciais, forçada pela pandemia, acelerou projetos de transformação digital em curso[392]. No entanto, essa mudança também expõe a vulnerabilidades, como evidenciado pelas falhas de segurança admitidas pela empresa Zoom em 2020[393]. A sistematização maciça de serviços, tanto públicos quanto privados, resulta na criação de vastas bases de dados essenciais para o funcionamento econômico, político e social, tornando-as alvos valiosos para criminosos virtuais.

No âmbito da proteção de dados pessoais e do direito à privacidade, destaca-se, em primeiro lugar, o princípio da segurança, cujo enfoque, conforme observado por Busatta[394], reside na implementação de medidas capazes de prevenir ataques cibernéticos perpetrados por hackers e crackers, que têm causado prejuízos significativos em escala global.

Em complemento a essa abordagem, outro princípio crucial é o da prevenção, que preconiza uma atuação proativa, técnica, científica e economicamente direcionada à evitabilidade de danos, exigindo dos responsáveis

---

e em outro contexto, foi verificado semelhante problema." MEDEIROS, Ana Beatriz; DA SILVA, Letícia de Lourdes Lunna Gesteira. Brasil pandêmico e proteção de dados de crianças e adolescentes no meio digital: diagnósticos gerais. Revista FIDES, v. 11, n. 2, p. 295-312, 21 jan. 2021.

[392] WIMMER, Miriam. *Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia*. Revista Brasileira de Políticas Públicas. v. 11, n. 1 (2021). pp. 123-142. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/7136. Acesso em: 20/11/2023

[393] ZOOM. A Message to Our Users. Disponível em: https://blog.zoom.us/a-message-to-our-users/. Acesso em: 20/11/2023

[394] BUSATTA, Eduardo Luiz. Do dever de prevenção em matéria de proteção de dados pessoais. In: EHRHARDT JÚNIOR, Marcos; LOBO, Fabíola Albuquerque (Coord). Privacidade e sua compreensão no direito brasileiro. Belo Horizonte: Fórum, 2019

pelo tratamento de dados a implementação de uma efetiva política de gestão de riscos[395].

A conjunção desses princípios resulta na exigência do "*privacy by design*"[396] ou proteção de dados desde a concepção, conforme estipulado no art. 46, §2º, que, de forma objetiva, demanda que a privacidade seja considerada em todas as fases do tratamento de dados. O dever de prevenção é, ademais, complementado pelos princípios da boa-fé e da responsabilização e prestação de contas[397].

Modesto[398] destaca a importância de adotar medidas de segurança técnica e administrativa ao longo de todo o ciclo de vida dos dados na organização, incorporando ações de segurança da informação desde a concepção do produto ou serviço. Ademais, estar em conformidade com a Lei 13.709/2018 requer um esforço contínuo dos agentes de tratamento, sendo insuficiente realizar mudanças apenas para uma adequação inicial à lei, sem testes periódicos[399].

O compliance desempenha um papel significativo nesse contexto, sendo definido como a regulação interna de entidades públicas ou privadas para prevenir os riscos associados à utilização de dados pessoais[400]. Conforme as lições de Frazão, Oliva e Abilio[401], a adoção de mecanismos de compliance é um instrumento valioso para promover condutas em conformidade com a regulamentação legal,

---

[395] BUSATTA, Eduardo Luiz. *Do dever de prevenção em matéria de proteção de dados pessoais.* In: EHRHARDT JÚNIOR, Marcos; LOBO, Fabíola Albuquerque (Coord). Privacidade e sua compreensão no direito brasileiro. Belo Horizonte: Fórum, 2019

[396] A expressão é atribuída a Ann Cavoukian, Comissária de Informação e Privacidade de Ontario, no Canadá, que, motivada pela convicção de que somente a existência de leis não seria suficiente para garantir a privacidade frente ao avanço das tecnologias que permitiam a coleta ilimitada de dados pessoais, sendo necessário encorajar as empresas as empresas a conceberem seus produtos e serviços, desde a concepção, incorporando a privacidade em todas as fases de seus projetos. Disponível em: Privacy by Design (exin.com). Acesso em: 14/01/2024

[397] BUSATTA, Eduardo Luiz. *Do dever de prevenção em matéria de proteção de dados pessoais.* In: EHRHARDT JÚNIOR, Marcos; LOBO, Fabíola Albuquerque (Coord). Privacidade e sua compreensão no direito brasileiro. Belo Horizonte: Fórum, 2019

[398] MODESTO, Jéssica Andrade. *O direito à privacidade na sociedade da informação à luz da lei geral de proteção de dados pessoais: uma análise da (in)efetividade da lei nº 13.709/2018 no brasil a partir do estudo comparativo com o regulamento geral de proteção de dados da união europeia.* 2021. 364 f. Dissertação (Mestrado em Direito) - Universidade Federal de Alagoas, Alagoas, 2021,

[399] *Ibidem*

[400] LEMOS, Alexandre; SAPHIER, Angélica, JÚNIOR EHRHARDT, Marcos. *Compliance e a proteção de dados em tempos de covid-19.* In: KRELL, Andreas Joachim; DANTAS, Juliana de Oliveira Jota; LINS JÚNIOR, George Sarmento (Org). A pandemia do coronavírus sob a ótica do direito: desafios e transformações em pauta. Maceió: Edufal, 2021,

[401] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance dos dados pessoais*. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato (Coord.). Lei geral de proteção de dados e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

tornando-se essencial diante das mudanças paradigmáticas no tratamento de dados.

Além disso, em meio às discussões sobre as implicações do tratamento de dados pessoais em situações de calamidade pública e interesse coletivo durante a pandemia, é imperativo reafirmar os compromissos estabelecidos pelas normativas de proteção de dados pessoais e pela tutela do direito à privacidade. A necessidade de garantir que as medidas adotadas sejam necessárias, proporcionais e temporárias é ressaltada diante dos diversos níveis de vigilância, exploração de dados e desinformação observados[402].

Diante desse contexto, a observância e aplicação dos princípios elencados na legislação nacional são de suma importância, especialmente porque a Lei Geral de Proteção de Dados (LGPD) é principiológica, apresentando prescrições genéricas e flexíveis, adaptáveis à volatilidade social decorrente dos avanços tecnológicos[403].

Busatta[404] destaca que a extensão desses princípios não se limita ao que está explicitamente previsto na LGPD ou ao que a autoridade administrativa estabelecer em complementação. Cabe à doutrina e jurisprudência densificar e concretizar tais princípios para aprimorar práticas e tecnologias de tratamento de dados pessoais seguras e éticas, em consonância com as legítimas expectativas, evitando lesões aos direitos dos titulares.

O respeito aos dados pessoais como extensão da personalidade requer uma proteção adequada, alinhada à sua hierarquia substancial superior em relação aos interesses meramente econômicos dos agentes de tratamento. Essa abordagem, segundo Busatta[405], é condizente com a Constituição da República e a LGPD, cuja técnica legislativa, baseada em princípios amplos e semântica vaga, permite a flexibilidade necessária para regular um campo em constante evolução tecnológica.

---

[402] MODESTO, Jéssica Andrade. O direito à privacidade na sociedade da informação à luz da lei geral de proteção de dados pessoais: uma análise da (in)efetividade da lei nº 13.709/2018 no brasil a partir do estudo comparativo com o regulamento geral de proteção de dados da união europeia. 2021. 364 f. Dissertação (Mestrado em Direito) - Universidade Federal de Alagoas, Alagoas, 2021

[403] *Ibidem.*

[404] BUSATTA, Eduardo Luiz. *Do dever de prevenção em matéria de proteção de dados pessoais.* In: EHRHARDT JÚNIOR, Marcos; LOBO, Fabíola Albuquerque (Coord). Privacidade e sua compreensão no direito brasileiro. Belo Horizonte: Fórum, 2019

[405] *Ibidem*.

No que diz respeito à responsabilidade civil dos agentes encarregados do tratamento de dados pessoais, que, durante esse processo, causem prejuízos ao titular, é possível a aplicação de indenizações por danos materiais e morais, sejam eles individuais ou coletivos, sem que isso exclua a aplicação das disposições do Código de Defesa do Consumidor (CDC). Modesto[406] destaca que esse sistema de responsabilização reconhece a disparidade existente entre o titular e os agentes de tratamento de dados, evidenciando a vulnerabilidade do primeiro.

Dessa maneira, esse sistema não apenas funciona como um estímulo adicional para que os agentes de tratamento estejam em conformidade com a Lei Geral de Proteção de Dados, mas também se presta à reparação ou, ao menos, compensação ao indivíduo pelas lesões sofridas em seu direito à privacidade.

Por outro lado, é imperativo observar que a atuação da Autoridade Nacional de Proteção de Dados (ANPD), no exercício de seus poderes regulamentares, sancionatórios e fiscalizadores, está condicionada à implementação de ações pedagógicas direcionadas ao público, especialmente ao titular de dados. Isso visa instruir o titular sobre seus direitos, proporcionando, a partir desse conhecimento, efetividade à Lei Geral de Proteção de Dados (LGPD)[407].

Nesse contexto, a LGPD, por meio da atuação da ANPD, assume um papel crucial, uma vez que desempenha um papel central na garantia da autodeterminação informativa. Esse aspecto é fundamental, indicando uma direção clara para o desenvolvimento desse campo. Como destaca Rodotà[408], a proteção das informações pessoais emerge como um elemento essencial da personalidade e da cidadania.

Portanto, a amplitude e efetividade das garantias asseguradas à privacidade dependem substancialmente da evolução da sociedade da informação para uma sociedade do conhecimento e do saber, e não para uma sociedade da vigilância, da classificação e do controle.

---

[406] MODESTO, Jéssica Andrade. O direito à privacidade na sociedade da informação à luz da lei geral de proteção de dados pessoais: uma análise da (in)efetividade da lei nº 13.709/2018 no brasil a partir do estudo comparativo com o regulamento geral de proteção de dados da união europeia. 2021. 364 f. Dissertação (Mestrado em Direito) - Universidade Federal de Alagoas, Alagoas, 2021

[407] *Ibidem.*

[408] RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje.* Org., sel. e apres. de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008. P.116.

5.4 O direito à proteção de dados e a pandemia de covid-19: A abordagem europeia

No espaço de poucos meses, a pandemia de COVID-19 mudou a vida e a rotina de todo o planeta. O impacto foi sentido em várias facetas da experiência humana, impulsionando a necessidade de mudança na maneira de se relacionar, de trabalhar, e até mesmo na saúde mental da população. A necessidade de atualização também contemplou as organizações do mundo inteiro, incluindo as instituições da União Europeia, que além de ter que se reorganizar para minimizar o contato social, adotar métodos alternativos de segurança, enfrentar diversos desafios em relação a trabalho e ambiente digital, também teve que se reorganizar no que toca a proteção de dados de sensibilidade tão ímpar quanto os da saúde.

Nesse cenário, desde os estágios iniciais de surgimento do COVID, o binômio segurança-privacidade foi avaliado no enfrentamento de uma crise nunca antes vista ou prevista. É sabido que dados pessoais são fonte de informação para o Estado para o dimensionamento de um cenário, como tal, os dados foram imprescindíveis para o gerenciamento da crise ocasionada pela pandemia de Covid-19. Isso pois, a coleta e instrumentalização dos dados permitem a realização de um diagnóstico situacional que possibilita também a construção de indicadores que conseguem demonstrar a complexidade das situações de forma a conferir exatidão e contemplar as mais diversas variáveis do problema. Nesse cenário, o adequado manejo dos dados, tem muito a somar na facilitação na elaboração de uma estratégia mais eficaz para conter a transmissão do vírus, e consequentemente contribuir para um cenário positivo de minimização das consequências negativas desse evento[409].

Apesar disso, tendo em vista que tecnologias ligadas a utilização de dados foram implementadas primeiramente em países que não protegiam o titular dos dados de maneira adequada, e por isso foram duramente criticados, em um primeiro momento houve certa resistência na utilização dessas ferramentas.

[409] SILVA, M. L. F. DA; TEIXEIRA, M. A. C.; FRANCISCO, E. DE R. *O uso de dados pessoais no combate à COVID-19: alcances e limites das experiências do Brasil e da União Europeia*. Revista de Gestão dos Países de Língua Portuguesa, v. 21, n. 2, p. 107–123, 23 ago. 2022, p.115.

A preocupação central foi relacionada à violação do direito à privacidade destas medidas, bem como ao seu poder de permitir a vigilância em massa, criando uma situação complexa onde o principal temor era criar uma situação excessivamente permissiva em que os governos pudessem continuar a recolher informações sensíveis perpetuamente, ou seja, muito para além da situação emergencial em questão. Assim, a questão central é descobrir se é possível uma conciliação, ao reconhecer a necessidade de proteção, e simultaneamente não permitir que as leis de proteção de dados se tornem fatores impeditivos na utilização dos dados como instrumento de auxílio ao combate à pandemia[410].

No continente asiático a geolocalização de doentes e casos suspeitos foi utilizada desde o início da epidemia do coronavírus, na contramão desse cenário, o continente europeu reconheceu a importância dos aplicativos na batalha afim de quebrar a cadeia de contaminação do vírus, mas empreendeu esforços para o incentivo ao desenvolvimento de aplicativos de monitoramento de contato. A maioria dos estados membros da união europeia lançaram esse tipo de aplicativo[411]. Adicionalmente, esforços também foram empreendidos para o desenvolvimento de aplicativos que rompem as barreiras nacionais é realizaram um serviço que permite aplicativos nacionais se comunicarem entre si, rompendo as Fronteiras dos países Europeus. Nessa perspectiva, evidenciou-se o caráter voluntário dos aplicativos, bem como o fato deles serem baseados na proximidade de *bluetooth*, e não em os dados relativos à localização.

O funcionamento não é complexo: não importa em qual local uma pessoa entra em contato com uma pessoa testada positiva para a covid-19 - o contato poderia ser feito no ônibus, trabalho, ou em um parque- o que de fato é analisado

---

[410] Nesse sentido o Comitê Europeu de Proteção de dados (CEPD) destacou como as regras de proteção de dados não devem e não têm a intenção de impedir as medidas que precisam ser implementadas no combate à pandemia de COVID-19.21 Pelo contrário, a proteção de dados deve ser considerada uma ferramenta essencial na construção da confiança social necessária que garante a eficácia dessas medidas. *Diretriz 04/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19*. , 21 abr. 2020. P.4. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb _guidelines_20200420_ contact_tracing_covid_with_annex_pt.pdf. Acesso em: 27 jan. 2024.

[411] KĘDZIOR, M. *The right to data protection and the COVID-19 pandemic: the European approach.* ERA Forum, 7 dez. 2020. Disponível em: https://link.springer.com/article/1 0.1007/s1 2027-020- 00644-4. Acesso em: 21/01/2014. P. 5.

é a proximidade com a pessoa contaminada, dessa forma a localização do usuário, nunca é utilizada. O único dado utilizado é a proximidade entre duas pessoas[412].

Tendo em vista essas necessidades, foram desenvolvidos protocolos como o *Pan-European Privacy-Preserving Proximity Tracing* (PEPP-PT/PEPP*), Decentralized Privacy-Preserving Proximity Tracing* (DP-3T)*, Temporary Contact Numbers Protocol* (TCN)*, e o Exposure Notification* (GAEN).

O protocolo *Temporary Contact Numbers Protocol (TCN)* foi lançado em março de 2020 pela equipe *covid watch*[413]*,* que foi uma colaboração entre as universidades de Stanford e de Waterloo. O protocolo TNC foi o primeiro a ser lançado e foi seguido pelos *Pan-European Privacy-Preserving Proximity Tracing* (PEPP-PT/PEPP*)*[414]*, Decentralized Privacy-Preserving Proximity Tracing* (DP-3T)[415], Exposure Notification (GAEN[416]), entre outros. Apesar da variedade de protocolos, e dos diferentes mecanismos por eles utilizados, todos eles possuem a mesma premissa: utilizar a tecnologia de Bluetooth para registrar encontros entre usuários.

Dessa forma, nesse sistema, a fim de se detectar se duas pessoas estão próximas o suficiente para correr o risco de uma infecção, utiliza-se *bluetooth* de baixa energia (BLE)[417]. A tecnologia do *bluetooth* só alcança alguns metros de distância, o que nesse caso, permite rastrear os contatos próximos o suficiente para

---

412 ABELER, J. et al. *Covid-19 contact tracing and data protection can go together (Preprint).* JMIR mHealth and uHealth, v. 8, n. 4, 14 abr. 2020.

413 A Covid Watch foi uma organização sem fins lucrativos fundada em fevereiro de 2020 com a missão de desenvolver tecnologia para o combate da pandemia da COVID-19 e, ao mesmo tempo, defender a privacidade digital. Os fundadores da equipe ficaram preocupados com a tecnologia emergente de rastreamento de contatos digitais que permite a vigilância em massa e iniciaram o projeto para ajudar a preservar as liberdades civis durante a pandemia. Maiores informações em About Us | Covid Watch (wehealth.org)

414 Em tradução livre, Rastreamento Pan-Europeu de Proximidade com Preservação da Privacidade (PEPP-PT/PEPP), foi introduzido em 1º de abril de 2020. Mais informações em Pan-European Privacy-Preserving Proximity Tracing - Wikipedia. Acesso em 19/01/2024.

415 Em tradução livre, Rastreamento de proximidade descentralizado com preservação de privacidade (DP-3T), foi introduzido em 4 de abril de 2020. Mais informações em Decentralized Privacy-Preserving Proximity Tracing - Wikipedia , Acesso em 19/01/2024.

416 Em tradução livre, Notificação de Exposição, é uma especificação de estrutura e protocolo desenvolvida pela Apple Inc. e Google, lançado em 10 de abril de 2020. Mais informações em Exposure Notification - Wikipedia Acesso em 19/01/2024..

417 Têm-se que : De maneira diversa do Bluetooth clássico, o BLE foi projetado para um consumo de energia significativamente menor. Isso permite que os apps se comuniquem com dispositivos BLE que têm requisitos de energia mais rigorosos, como sensores de proximidade, monitores de frequência cardíaca e dispositivos de condicionamento físico. *Em https://developer.android.com/develop/connectivity/bluetooth/ble/ble-overview?hl=pt-br . Acesso em 27/01/2024.*

a contaminação. Apesar disso, cabe ressaltar o funcionamento dessa estratégia só é eficaz se uma quantidade expressiva de pessoas instalar o aplicativo voluntariamente em seus telefones portáteis.

5.4.1 A diretriz 04/2020

Devido as preocupações suscitadas pelo novo cenário, a Comissão Europeia lançou a recomendação 2020/5189, em 8 de abril de 2020[418]. A recomendação foi categórica ao afirmar que a crise demonstrou que as autoridades de saúde pública e as instituições se beneficiariam amplamente de um maior acesso a informações essenciais para analisar a evolução do vírus e avaliar a eficácia das medidas de saúde pública, mas para isso era necessária a implementação de uma abordagem comum no sentido de garantir os direitos fundamentais presentes na ordem jurídica da União Europeia. Além disso, frisou-se que quaisquer restrições à direitos fundamentais protegidos devem ser temporários e justificados, e se limitarão estritamente ao necessário ao combate da crise, não sendo de forma alguma perpetuados sem justificativa.

O Comitê Europeu para a Proteção de Dados (CEPD) adotou uma abordagem semelhante na sua Diretriz 04/2020 de 21 de abril de 2020. As diretrizes se propuseram a esclarecer as condições e os princípios para a utilização dos dados de localização e ferramentas de rastreamento de contatos, com o objetivo de utilizar os apoiar a resposta à pandemia, e quebrar as cadeias de contaminação o mais cedo possível[419]. Em seu art. 4º, assevera acerca da necessidade de limitar o seu uso a alguns princípios, a saber:

> O CEPD considera, de um modo geral, que os dados e a tecnologia utilizados para ajudar a combater a COVID-19 devem ser utilizados para capacitar, e não para controlar, estigmatizar ou reprimir os cidadãos. Além disso, embora os dados e a tecnologia possam ser instrumentos importantes, têm limitações intrínsecas e podem apenas aumentar a eficácia de outras medidas de saúde pública. Os princípios gerais de

[418] COMISSÃO EUROPEIA. *Recomendação (ue) 2020/518 da comissão*. , 8 abr. 2020. Disponível em: https://eur-lex.europa.eu/ legal-content/PT/TXT/?uri =CELEX%3A32020H0518. Acesso em: 27 jan. 2024.

[419] UNIÃO EUROPEIA. *Diretriz 04/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19.* , 21 abr. 2020. P.4. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_pt.pdf. Acesso em: 27 jan. 2024.

> eficácia, necessidade e proporcionalidade devem orientar qualquer medida adotada pelos Estados-Membros ou pelas instituições da UE que envolva o tratamento de dados pessoais para combater a COVID-19.[420]

É importante frisar que a diretriz 04/2020, enfatiza e respeita as disposições e especificidades presentes na RGPD e a Diretiva 2002/58/CE, vejamos. Em primeiro plano, o CEPD ressalta que tanto o RGPD como a Diretiva 2002/58/CE[421] contêm regras específicas que abrem uma exceção para o tratamento de dados pessoais relativos à saúde, quando necessário por motivos de interesse público no domínio da saúde pública, quando previstas medidas adequadas para salvaguardar os direitos e liberdades do titular dos dados[422]. Nessa toada, o CEPD resguarda os direitos dos usuários quando orienta que os aplicativos de contato devem ser utilizados de maneira voluntária, e com base em proximidade dos utilizadores, e não o rastreio da localização.

No tocante à localização, o CEPD assevera que os dados só podem ser transmitidos a autoridades ou outras partes se forem anonimizados pelo prestador, ou com o consentimento prévio dos utilizadores. As informações de localização armazenadas no equipamento só podem ser acessadas se estritamente necessário e consentido pelo utilizador, nos termos do art. 4 do RGPD, ou seja, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento[423].

Ainda quanto a localização, o CEPD enfatiza a utilização de dados anonimizados, de maneira que os dados possam ser utilizados sem restrição, visto que os dados pessoais ou pseudonimizados[424] ainda tem a sua utilização regida pelo RGPD.

---

[420] *Idem*, p. 5.

[421] UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas. Jornal Oficial L. 201, 31 de julho de 2002. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32002L0058. Acesso em: 20/11/2023

[422] UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Art. 9º. Jornal Oficial L. 119/1008, 04 de maio de 2016. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023.

[423] *Idem*, Art. 4.

[424] Segundo o considerando 26 do RGPD: Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações

Verifica-se que os sinais de mobilidade são altamente correlacionados e únicos, por isso se torna, por isso esse tipo de dado se torna muito vulnerável em tentativas de identificação, a depender das circunstâncias, isso pois afirma-se até memo que existem pesquisas que os dados de localização, apesar de considerados anonimizados podem não o ser. Desse modo, para a anonimização ser totalmente bem-sucedida os dados devem ser cuidadosamente tratados a fim de que se passe no teste de razoabilidade[425]. Dessa forma, o tratamento abrange a aplicação de técnicas sólidas e eficazes, e a consideração de todos os dados de localização em conjunto, além disso a transparência quanto a metodologia utilizada, é altamente incentivada pelo CEPD.

Importante ressaltar que o CEPD reforça o fato de as diretrizes não serem prescritivas nem exaustivas, sendo que outras soluções para além das descritas podem ser utilizadas e lícitas, desde que respeitem o quadro jurídico pertinente (isto é, o RGPD e a diretiva).

5.4.2 A diretriz 03/2020

Nessa mesma linha o Comite Europeu de Proteção de Dados também se pronunciou acerca do tratamento de dados relativos à saúde para efeitos de investigação científica no contexto do surto de COVID-19, na diretriz 03/2020. Neste contexto, o CEPD reconhece o surgimento de questões jurídicas relacionadas à utilização de dados relativos à saúde no artigo 4.º, n.º 15, do RGPD para efeitos de investigação, e busca esclarecer as questões mais necessárias que possuem impacto no combate eficaz da pandemia.

Como já comentado neste trabalho, o RGPD entende dados relativos à saúde como “dados pessoais relacionados com a saúde física ou mental de uma

suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023

[425] Segundo a diretriz 04/2020: a anonimização refere-se à utilização de um conjunto de técnicas a fim de impedir que se possa estabelecer uma ligação entre os dados e uma pessoa singular identificada ou identificável mediante um esforço «razoável». Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32002L0058. Acesso em: 20/11/2023

pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde;"[426] . No RGPD tratamento de dados relativos à saúde, apesar de calcados de uma proteção especial conferida aos dados sensíveis, é permitido sempre que assim for necessário, tendo em vista o princípio da proporcionalidade, e assim dispor o direito da união ou dos estados-membro[427]. Nesse sentido, o art.9º assevera que o tratamento é permitido "*sempre que necessário para fins de investigação científica, histórica, ou para fins estatísticos, de modo que seja proporcional e respeite os direitos e interesses do titular"*[428]*.*

Tendo isso em vista, o CEPD dispõe que qualquer tratamento de dados pessoais de saúde, para ser realizado de maneira lícita, deve respeitar os princípios relativos ao tratamento estabelecidos no artigo 5.º do RGPD e estar abrangido por uma das bases jurídicas e derrogações específicas enumeradas, respetivamente, no artigo 6.º e no artigo 9.º do RGPD.

Assim, o deve haver consentimento livre, explícito, específico, informado, e sem desequilíbrio manifesto entre o titular e o responsável pelo tratamento, além do titular pode retirar o seu consentimento a qualquer momento. O tratamento deve obedecer ao princípio da transparência, ou seja, o titular dos dados deve ser informado individualmente da existência da operação de tratamento e de que os dados pessoais (de saúde) estão a ser tratados para fins científicos[429]. Os dados devem ser recolhidos para fins estritos e determinados, de maneira que não podem ser tratados posteriormente de maneira incompatível com as finalidades definidas previamente. Além disso, é mister que os dados sejam conduzidos com

---

[426] UNIÃO EUROPEIA. *Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas.* Jornal Oficial L. 201, 31 de julho de 2002. Art. 4°. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32002L0058. Acesso em: 20/11/2023.

[427] CORDEIRO, Menezes. D*ireito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019.* Coimbra: Almedina, 2020. ISBN 978-972-40-8952-2. P. 250.

[428] UNIÃO EUROPEIA. *Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Art. 9º. Jornal Oficial L. 119/1008, 04 de maio de 2016. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023.

[429] UNIÃO EUROPEIA. *Diretrizes 03/2020 sobre o tratamento de dados relativos à saúde para efeitos de investigação científica no contexto do surto de COVID-19.* 21 abr. 2020.P. 8. Disponível em: https://edpb.europa.eu/sites/default/files/ files/file1/edpb_guidelines_202003_health datascientificresearc hcovid19_pt.pdf. Acesso em: 27 jan. 2024

integridade e confidencialidade, de maneira que devem ser aplicadas medidas técnicas e organizativas adequadas e atualizadas para garantir um nível de segurança suficiente[430].

Em consonância com o princípio da limitação da conservação, o período que os dados são conservados devem ser limitados. O art. 5º *afirma "os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ",* apesar disso, os períodos de conservação devem ser definidos de acordo com critérios como a duração e o objetivo da investigação[431]. Da mesma forma, o regramento nacional deve legislar acerca do período de conservação dos dados.

Estabelecendo as bases de uma abordagem comum pan-europeia no que toca as transferências internacionais de dados, o CEPD orienta a realizar essas transferências com lastro no art. 49 do RGPD, que afirma que se pode realizar transferência em caráter excepcional por necessidade em relação a importantes razões de interesse público.

Nessa toada, pode-se notar que os princípios do RGPD oferecem diretrizes gerais sob o manto das quais acomodam todas as outras. Assim, o Comitê Europeu para a Proteção de Dados, que assume um papel central na aplicação coesa do RGPD[432], na emissão das diretrizes 03/2020 e 04/2020 mantém sempre em vista observação dos princípios de maneira integral.

A natureza global da pandemia demandou a utilização de esforços conjuntos para conter a disseminação do vírus pelo planeta. Nesse sentido, a ação empreendida pelas instituições da União Europeia em relação à proteção dos dados pessoais deve ser vista como instrumento complementar no contexto de

---

[430] UNIÃO EUROPEIA. *Diretrizes 03/2020 sobre o tratamento de dados relativos à saúde para efeitos de investigação científica no contexto do surto de COVID-19.* 21 abr. 2020.P. 11. Disponível em: https://edpb.europa.eu/sites/default/files/ files/file1/edpb_guidelines_202003_health datas cientificresearc hcovid19_pt.pdf. Acesso em: 27 jan. 2024

[431] UNIÃO EUROPEIA. *Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Art. 5º. Jornal Oficial L. 119/1008, 04 de maio de 2016. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023.

[432] CORDEIRO, Menezes. *Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019*, Coimbra: Almedina, 2020. ISBN 978-972-40-8952-2. p. 421.

gestão da pandemia de COVID-19. A boa gestão e utilização dos dados é um importante aparato no auxílio do aumento da eficácia de outras medidas de saúde pública.

Diante da grande capacidade do vírus de se espalhar além das fronteiras geográficas, a União Europeia concentrou-se em desenvolver uma abordagem comum em resposta à crise. Relativamente à proteção de dados pessoais, na resolução de 17 de abril de 2020, o parlamento se pronunciou no sentido de reconhecer a necessidade de proteção da privacidade e dados pessoais[433]. Em maio de 2020 foram acordadas diretrizes relativas a interoperabilidade transfronteiriça[434], o que possibilitou aos usuários dos aplicativos, a possibilidade de alerta de contato com outros usuários testados positivos para a covid em qualquer lugar da União Europeia, isso tudo mediante a utilização apenas dos dados estritamente necessários para tal.

O Comité europeu de proteção de dados emitiu diretrizes consistentes a respeito de questões relacionadas à proteção de dados e a utilização de ferramentas de rastreio e geolocalização, não permitindo de forma alguma que a proteção de dados sejam obstáculo na contenção da pandemia, mas também garantindo a proteção do titular dos dados no sentido de tornar indispensável a aplicação do regulamento geral de proteção de dados e sempre utilizando dos seus princípios para equilibrar as necessidades de dados para melhor realizar estratégias em termos de saúde pública, mas sem desamparar os direitos individuais do titular.

Os desafios foram inéditos, mas a união europeia não preteriu as normas aplicáveis: o desenho jurídico do RGPD se mostrou suficientemente flexível e, como tal, capaz de permitir uma resposta eficiente na limitação da pandemia e na proteção dos direitos humanos fundamentais e liberdades. Na adoção de diversos documentos políticos, diretrizes, as instituições da UE evidenciaram a capacidade de preservar a privacidade em situações adversas.

---

[433]COVID-19: garantir privacidade e uso além-fronteiras de aplicações móveis | Atualidade | Parlamento Europeu. Disponível em: https://www.europarl.europa.eu/news/pt/headlines/society/20200429STO78174/covid-19-garantir-privacidade-e-uso-alem-fronteiras-de-aplicacoes-moveis. Acesso em: 27 jan. 2024.

[434] COMISSÃO EUROPEIA. eHealth Network Interoperability guidelines for approved contact tracing mobile applications in the EU. [s.l: s.n.]. 13 DE maio de 2020. Disponível em: https://health.ec.europa.eu/system/files/2020-05/contacttracing_mobileapps_guidelines_en_2.pdf. Acesso em: 12 /01/2024

CONCLUSÃO

A proteção de dados pessoais e o direito à privacidade emergiram como tópicos de extrema relevância no contexto da pandemia de COVID-19. À medida que os países implementaram medidas extraordinárias para conter a propagação do vírus, a coleta, processamento e compartilhamento de informações pessoais intensificaram-se, levando a uma série de desafios éticos, legais e sociais. Neste trabalho, examinou-se os principais aspectos relacionados à proteção de dados e à privacidade durante a pandemia, considerando os avanços, desafios e a importância de encontrar um equilíbrio entre a necessidade de saúde pública e a salvaguarda dos direitos individuais.

A concepção moderna de privacidade teve sua gênese nas discussões filosóficas e jurídicas do século XIX. Contudo, foi no século XX que a privacidade começou a ser reconhecida como um direito fundamental, impulsionada por avanços tecnológicos e transformações sociais. O advento das tecnologias de informação e comunicação na segunda metade do século XX introduziu novos desafios à privacidade, com a coleta massiva de dados pessoais tornando-se uma preocupação central.

Na União Europeia, o reconhecimento da privacidade como um direito fundamental foi solidificado pela Carta dos Direitos Fundamentais da União Europeia, adotada em 2000. Em 2018, a implementação do Regulamento Geral de Proteção de Dados (RGPD) estabeleceu uma abordagem unificada para a proteção de dados em todos os estados-membros da UE, fortalecendo os direitos dos titulares de dados e impondo obrigações rigorosas às organizações que processam dados pessoais.

O RGPD representa um marco significativo na proteção de dados pessoais na União Europeia. Ele estabeleceu princípios claros, como o consentimento informado, a finalidade específica da coleta de dados e a obrigação de notificar violações de dados. Além disso, introduziu o conceito de "by design and by default", incentivando a integração de medidas de privacidade desde o início do desenvolvimento de produtos e serviços.

A UE, ao adotar o RGPD, demonstrou um compromisso inequívoco com a proteção da privacidade dos seus cidadãos, estabelecendo um padrão global para

a governança de dados. A eficácia desse regulamento é evidenciada pela sua influência nas práticas de negócios em todo o mundo e pela conscientização crescente sobre a importância da privacidade.

No contexto brasileiro, a noção de privacidade também passou por uma evolução notável. A Constituição de 1988 incluiu a inviolabilidade da intimidade, vida privada, honra e imagem como direitos fundamentais. Entretanto, a legislação específica sobre proteção de dados só ganhou destaque mais recentemente.

A aprovação da Lei Geral de Proteção de Dados em 2018, inspirada no RGPD, representou um avanço significativo. A LGPD estabelece princípios semelhantes, como a necessidade de consentimento, transparência no tratamento de dados e direitos robustos para os titulares. Sua entrada em vigor em 2020 representa um compromisso do Brasil com padrões internacionais de privacidade e um reconhecimento da importância de proteger os direitos individuais no ambiente digital.

No contexto da pandemia de Covid-19, as discussões relativas a proteção de dados pessoais ganharam contornos ainda mais intensos, exigindo respostas rápidas para conter a propagação do vírus. Isso levou muitos países a adotarem medidas que, em alguns casos, impactaram os direitos individuais à privacidade. A implementação de rastreamento de contatos, monitoramento de movimento e coleta massiva de dados de saúde tornou-se comum em várias jurisdições.

É crucial, no entanto, equilibrar a necessidade de proteger a saúde pública com a preservação dos direitos à privacidade. O respeito aos princípios de minimização de dados, finalidade específica e garantia de segurança dos dados são fundamentais, mesmo em tempos de crise.

No que diz respeito à responsabilização civil dos agentes envolvidos no tratamento de dados pessoais durante a pandemia, torna-se evidente a necessidade de um sistema robusto que reconheça a assimetria entre os titulares dos dados e os processadores dessas informações. A imposição de indenizações por danos materiais e morais, individuais ou coletivos, representa uma ferramenta fundamental para assegurar que a violação da privacidade seja devidamente compensada. A abordagem delineada por diversos autores, ao longo desta pesquisa, ressalta não apenas a importância de incentivar a conformidade com a legislação de proteção de dados, mas também a necessidade de proporcionar

reparação ou compensação adequada aos indivíduos prejudicados em seu direito à privacidade.

No entanto, a implementação eficaz dessas medidas não pode ocorrer apenas por meio de responsabilização; é necessária uma supervisão ativa e direcionada. A atuação da Autoridade Nacional de Proteção de Dados (ANPD) é crucial nesse sentido. Além de exercer seus poderes regulamentares, sancionatórios e fiscalizadores, a ANPD deve investir em ações pedagógicas voltadas ao público. O titular de dados precisa ser devidamente instruído sobre seus direitos, garantindo que a legislação, como a Lei Geral de Proteção de Dados (LGPD), seja efetivamente aplicada.

No contexto da pandemia, a LGPD, por meio da ANPD, desempenhou um papel central na manutenção do equilíbrio entre as necessidades de saúde pública e a proteção da privacidade. O desafio residiu em encontrar um desempenho gravitacional, um ponto de equilíbrio que assegure a autodeterminação informativa. Esse equilíbrio é essencial para garantir que a sociedade avance para uma era do conhecimento e do saber, ao invés de cair em uma sociedade caracterizada pela vigilância, classificação e controle excessivos. A visão apresentada por Rodotà destaca que a tutela das informações pessoais é um elemento essencial da personalidade e da cidadania, ressaltando a necessidade de evolução da sociedade da informação.

Na Europa o RGPD se mostrou capaz de permitir uma resposta eficiente na limitação da pandemia e na proteção dos direitos humanos fundamentais e liberdades. Além disso, foram emitidos diversas diretrizes e orientações em geral que buscaram conciliar a necessidade de utilização dos dados com os direitos fundamentais, evidenciando-se assim a habilidade de combate à pandemia sem abdicar da proteção dos dados pessoais.

Assim, não se pode ignorar os desafios inerentes à proteção de dados no ápice da pandemia. O rastreamento de contatos, o uso de aplicativos de monitoramento e a coleta massiva de dados de saúde, conforme mencionado anteriormente, tornaram-se práticas comuns. Embora essas medidas sejam fundamentais para conter a propagação do vírus, também levantam sérias preocupações com relação à privacidade. A necessidade de balancear a eficácia dessas práticas com o respeito aos direitos individuais é um dilema complexo.

Além disso, o aumento do trabalho remoto durante a pandemia trouxe consigo desafios adicionais para a segurança dos dados pessoais. Empresas e organizações precisam adotar políticas rigorosas de segurança da informação para proteger as informações confidenciais dos funcionários que agora operam fora dos ambientes tradicionais de escritório. Garantir que as conexões sejam seguras e que os dispositivos utilizados para o trabalho remoto sejam protegidos tornou-se uma prioridade inegável.

Em termos de legislação e conformidade, é crucial que os países revisem e atualizem suas leis de proteção de dados para lidar com os desafios específicos trazidos pela pandemia. A legislação deve ser flexível o suficiente para acomodar as necessidades emergenciais, mas também robusta o bastante para proteger os direitos fundamentais dos indivíduos. A harmonização internacional de normas pode ser benéfica para garantir uma abordagem coesa em escala global.

Portanto, com fulcro em tudo que fora abordado nesta pesquisa, pode-se concluir que a proteção de dados pessoais e o direito à privacidade no contexto da pandemia de Covid-19 são temas complexos e multifacetados. Encontrar o equilíbrio entre as necessidades de saúde pública e a proteção dos direitos individuais é um desafio constante que exige a colaboração entre governos, organizações, sociedade civil e especialistas em proteção de dados. A implementação eficaz das leis existentes, o fortalecimento das agências reguladoras e o investimento em conscientização pública são passos essenciais para enfrentar os desafios atuais e futuros nesse cenário em constante evolução. A sociedade deve continuar a buscar soluções que garantam a segurança e a saúde pública sem comprometer os direitos fundamentais à privacidade e à autodeterminação informativa.

REFERÊNCIAS

ABELER, J. et al. Covid-19 contact tracing and data protection can go together (Preprint). JMIR mHealth and uHealth, v. 8, n. 4, 14 abr. 2020. Disponível em: https://mhealth.jmir.org/2020/4/e19359/. Acesso em 22/01/2024

ALBUQUERQUE, Aline. Direitos humanos dos pacientes. Curitiba: Juruá, 2016.

ALVES, Carla Segala; GUIDI, Guilherme Berti de Campos. Cláusulas contratuais e dados pessoais: controladores, operadores, cocontroladores e transferências internacionais. In: BLUM, R.O.; VAINZOF, R.; MORAES, H.F. Data protection officer (encarregado): teoria e prática de acordo com a LGPD e o RGPD. São Paulo: Thomson Reuters Brasil, 2020.

ALEXY, Robert. Teoria dos Direitos Fundamentais. 1. ed. São Paulo: Malheiros Editores, 2016.

ALMEIDA, Bethania Araujo et. al. *Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global.* Ciência & Saúde Coletiva. v. 25(Supl.1): 2487-2492, 2020. Disponível em: https://doi.org/10.1590/1413-81232020256.1.11792020. Acesso em: 20/11/2023

ARAGÃO, A. L.; SCHIOCCHET, T. R. Lei Geral de Proteção de Dados: Comentários à Lei nº 13.709/2018. Editora Juspodivm, 2020.

ARIMETHEA, Bruna; CAPELAS, Bruno. InLoco e Prefeitura de Recife vão monitorar 700 mil celulares em prol de isolamento social. O Estado de S. Paulo. 25 mar. 2020. Disponível em: https://link.estadao.com.br/noticias/inovacao,inloco-e-prefeiturade-recife-vao-monitorar-700-mil-celulares-emprol-de-isolamento-social,70003248010. Acesso em: 20/11/2023

BAUMAN, Zygmunt. Vigilância líquida: diálogos com David Lyon. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BELLEIL, Arnaud. @-Privacidade: o mercado dos dados pessoais, proteção da vida privada na internet. Lisboa: Instituto Piaget, 2002.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Forense, 2019

BITTAR, Carlos Alberto. Os direitos da personalidade. 8. ed. São Paulo: Saraiva, 2015.

BOFF, Salete Oro; FORTES, Vinícius Borges. A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil. Sequência (Florianópolis) [online]. 2014, n.68.

BRAGANÇA, Luciano; TESTA, Marco. TIC Saúde e Privacidade: Uma Leitura Atualizada. In: Livro Verde Sociedade da Informação no Brasil: Dimensões e Propostas. CGI.br, 2011.

BRASIL. AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR (ANS). Resolução Normativa nº 305, de 9 de outubro de 2012. Institui o Padrão para Troca de Informação em Saúde Suplementar (TISS). Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/ans/2012/res0305_09_10_2012.html. Acesso em: 20/11/2023

BRASIL. AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR (ANS). Resolução Normativa nº 341, de 29 de novembro de 2013. Atualiza o Padrão para Troca de Informação em Saúde Suplementar (TISS). Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/ans/2013/res0341_27_11_2013.html. Acesso em: 20/11/2023

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 20/11/2023.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm Acesso em: 20/11/2023.

BRASIL. Lei n. 9.507, de 12 de novembro de 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm Acesso em: 20/11/2023.

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União, seção 1, Brasília, DF, a. 139, n. 8, p. 1-74, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/CCivil_03/leis/2002/L10406.htm. Acesso em: 20/11/2023.

BRASIL. Lei n. 12.414, de 09 de junho de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm Acesso em: 20/11/2023.

BRASIL. Lei n. 12.737, de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em: 20/11/2023.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 20/11/2023.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União, Poder Executivo, Brasília, DF, 31 dez. 1940. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-publicacaooriginal-1-pe.html. Acesso em: 20/11/2023.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm Acesso em: 20/11/2023.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 20/11/2023.

BRASIL. Ministério da Saúde. Portaria nº 2.073, de 31 de agosto de 2011. Define os parâmetros de interoperabilidade para Registro Eletrônico de Saúde (RES) no âmbito do Sistema Único de Saúde (SUS). Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2073_31_08_2011.html. Acesso em: 20/11/2023

BRASIL. Ministério da Saúde. Portaria nº 940, de 28 de abril de 2011. Institui o Sistema Cartão Nacional de Saúde (Sistema Cartão no âmbito do Sistema Único de Saúde (SUS), revoga a Portaria nº 1.206/GM/MS, de 9 de junho de 2000, e a Portaria nº 2.489/GM/MS, de 21 de outubro de 2005, e estabelece normas para o funcionamento do Sistema Cartão e a emissão do Cartão Nacional de Saúde. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt0940_28_04_2011.html. Acesso: 20/11/2023.

BRASIL. Supremo Tribunal Federal. Referendo na medida cautelar na ação direta de inconstitucionalidade 6.387. Distrito Federal. Relatora: Ministra Rosa Weber. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 20/11/2023

BUSATTA, Eduardo Luiz. Do dever de prevenção em matéria de proteção de dados pessoais. In: EHRHARDT JÚNIOR, Marcos; LOBO, Fabíola Albuquerque (Coord). Privacidade e sua compreensão no direito brasileiro. Belo Horizonte: Fórum, 2019

CAIXA encerra pagamento do auxílio emergencial após sete meses. Agência Brasil. 31 out. 2021. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2021-10/caixa-encerra-pagamento-do-auxilioemergencial-apos-sete-meses. Acesso em: 20/11/2023

CANOTILHO, J.J. Gomes. Direito constitucional e teoria da Constituição. 7. ed. Coimbra: Almedina, 2003.

CASELLA, Paulo Borba. União Europeia: instituições e ordenamento jurídico. São Paulo: LTr, 2002.

CASTELLS, Manuel. A galáxia internet. Reflexões sobre internet, negócios e sociedade. Tradução Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004.

CASTETS-RENARD, Céline. Droit de l'internet: droit français et européen. 2. éd. Paris: Montchrestien, 2012.

CAVALCANTI, José Carlos. "The new ABC of ICTs (analytics +big data + cloud computing: a complex trade-off between IT and CT costs". Hershey: IG Global, 2016.

CAVANILLAS, José María; CURRY, Edward; WAHLSTER, Wolfgang. The big data value opportunity. In: _____ (Org.). New horizons for a data-driven economy: a

roadmap for usage and exploitation of big data in Europe. Cham (Suiça): Springer Open, 2016.

CARBINATTO, Bruno. China está usando vigilância em massa para combater coronavírus. Abril. 25 mar.2020. Disponível em: https://super.abril.com.br/tecnologia/china-esta-usando-tecnologias-de-vigilancia-emmassa-para-combater-coronavirus/. Acesso em: 20/11/2023.

COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o acompanhamento do programa de trabalho para uma melhor aplicação da directiva relativa à proteção de dados. COM(2007) . Disponível em: https://eur-lex.europa.eu/PT/legal-content/summary/protection-of-personal-data.html. Acesso em:19/11/2023.

COMISSÃO EUROPEIA. Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. COM(2012) 11 final. Bruxelas, 25 jan. 2012. Disponível em: http://docplayer.com.br/3497609-Proposta-de-regulamento-do-parlamento-europeu-e-do-conselho.html. Acesso em: 24/12/2023

COMISSÃO EUROPEIA. Decisão 2000/520/CE. Decisão da Comissão de 26 de julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípios de “porto seguro” e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América. Jornal Oficial L 215, 25 de agosto de 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32000D0520. Acesso em: 20/11/2023

COMISSÃO EUROPEIA. Recomendação (ue) 2020/518 da comissão. , 8 abr. 2020. Disponível em: https://eur-lex.europa.eu/ legal-content/PT/TXT/?uri =CELEX%3A32020H0518. Acesso em: 27 jan. 2024

COMISSÃO EUROPEIA. eHealth Network Interoperability guidelines for approved contact tracing mobile applications in the EU. [s.l: s.n.]. 13 DE maio de 2020. Disponível em: https://health.ec.europa.eu/system/files/2020-05/contacttracing_mobileapps_guidelines_en_2.pdf. Acesso em: 12 /01/2024.

CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.227, de 13 de dezembro de 2018. Regulamenta a prática da telemedicina no país. Disponível em: https://abmes.org.br/legislacoes/detalhe/2694#:~:text=Resolu%C3%A7%C3%A3o%20CFM%20n%C2%BA%202.227%2C%20DE%2013%20DE%20DEZEMBRO%20DE%202018&text%202002. Acesso em: 20/11/2023

CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 1.638, de 29 de maio de 2002. Define e disciplina os procedimentos concernentes às Comissões de Revisão de Prontuários nos Conselhos Federal e Regionais de Medicina e dá outras providências. Disponível em: https://www.mpgo.mp.br/portal/arquivos/2019/09/11/15_40_13_481_Consulta_09_2019_comissão_revisora_em_unidades_de_saúde_1_pj_mineiros201900491013.pdf. Acesso em: 20/11/2023

CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 1.821, de 27 de setembro de 2007. Dispõe sobre a digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes/resolucao-cfm-no-1-821-de-11-de-julho-de-2007. Acesso em: 20/11/2023

CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.227, de 13 de dezembro de 2018. Regulamenta a prática da telemedicina no país. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2018/2227\. Acesso em:20/11/2023.

CORDEIRO, A. Barreto Menezes. Dados pessoais: conceito, extensão e limites. Disponível em: https://blook.pt/publications/publication/e38a9928dbce. Acesso em: 20/11/2023

CORDEIRO, A. Barreto Menezes. O Consentimento do Titular dos Dados no RGPD. Disponível em: https://blook.pt/publications/publication/e772e2d8f7b4/. Acesso em: 20/11/2023

CORDEIRO, A. Barreto Menezes. O tratamento de dados pessoais fundado em interesses legítimos. Disponível em: https://blook.pt/publications/publication/29c85b840a65/. Acesso em: 20/11/2023

CORDEIRO, A. Barreto Menezes. Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019. Coimbra: Almedina, 2020. ISBN 978-972-40-8952-2.

COURT OF JUSTICE OF THE EUROPEAN UNION (CJEU). Case C-311/18. Data Protection Commissioner v Facebook Ireland and Maximillian Schrems. Disponível em: https://www.europeansources.info/record/cjeu-case-c-311-18-data-protection-commissioner-v-facebookireland-and-maximillian-schrems/. Acesso em: 20/11/2023.

COSTA JR., Paulo José Da. O direito de estar só: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1970.

CUPIS, Adriano de. Os direitos da personalidade. Tradução Afonso Celso Furtado. Campinas: Romana, 2004.

CURY, Maria Eduarda. Como a China usou o WeChat para conter a covid-19 - e vigiar as notícias. Exame. 4abr. 2020. Disponível em: https://exame.com/tecnologia/como-a-china-usou-o-wechat-para-conter-a-covid-19-evigiar-as-noticias/. Acesso em: 20/11/2023.

CORONAVIRUS brings China's surveillance state out of the shadows. The Japantimes. Disponível em: https://www.japantimes.co.jp/news/2020/02/10/asia-pacific/coronavirus-china-surveillance-state-privacyrights/#. Xk2CpypKiM9. Acesso em: 20/11/2023

DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos e coordenação. LGPD na saúde. São Paulo: Thomson Reuters Brasil, 2021.

DELGADO, Mário Luiz. Big Brother Brasil: reality shows e os direitos da personalidade. Revista Jurídica Consulex, Brasília, a. VIII, n. 169, p. 24-26, jan. 2004. Disponível em: https://marioluizdelgado.files.wordpress.com/2014/04/mario-luiz-delgado-3.pdf. Acesso em: 20/11/2023.

DIAS, Tatiana. Vigiar e lucrar: nós identificamos dois clientes dos dados de localização 'anônimos' vendidos pela vivo. The Intercept Brasil. Disponível em: https://theintercept.com/2020/04/13/vivo-venda-localizacaoanonima/. Acesso em: 20/11/2023

DOVE, Edward S; TAYLOR. Mark J. Signalling Standards for Progress: Bridging the Divide Between a Valid Consent to Use Patient Data Under Data Protection Law and the Common Law Duty of Confidentiality. Medical Law Review, v. 29, Issue 3, Summer, p. 411–445, 2021.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2016.

DONEDA, Danilo. Os direitos da personalidade no Código Civil. Revista da Faculdade de Direito de Campos, Rio de Janeiro, a. VI, n. 6, p. 71-99, jun. 2015. Disponível em: http://www.uniflu.edu.br/arquivos/Revistas/Revista06/Docente/03.pdf . Acesso em: 20/11/2023.

DONEDA, Danilo. A proteção de dados pessoais como direito fundamental. Revista Espaço Jurídico 12/103. Joaçaba: Unoese, 2011.

EHRHARDT JÚNIOR, Marcos; PEIXOTO, Erick Lucena Campos. 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. 51

FERNANDES, Milton. Proteção civil da intimidade. São Paulo: Saraiva, 1977

FIGUEIREDO, Luciano. Curso de Direito Constitucional. 14. ed. São Paulo: Saraiva, 2017.

FOUCAULT, Michel. Vigiar e punir: nascimento da prisão. 31. ed. Tradução Raquel Ramalhete. Petrópolis: Vozes, 2006.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance dos dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato (Coord.). Lei geral de proteção de dados e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020

FREITAS, Juarez. A hermenêutica jurídica e a ciência do cérebro: como lidar com os automatismos mentais. Revista da AJURIS, Porto Alegre, v. 40, n. 130, p. 223-244, jun. 2013.

GARCIA, Lara Rocha. Lei Geral de Proteção de Dados Pessoais (LGPD: guia de implantação. São Paulo: Edgard Blücher Ltda, 2020.

GARFINKEL, Simson. Database nation: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010.

GOIATÁ, Sarah Rêgo; RAMOS, Rafael Barreto. Pandemia da covid-19 e direito Fundamental à privacidade no estado Democrático de direito: (in)constitucionalidade das mitigações ao Direito à Privacidade em Tempos de Crise Sanitária à luz da Medida Provisória n.º 954/20 e ADI n.º 6.387/DF. Anais do Congresso Internacional: preservar e fortalecer a democracia em tempos de pandemia. Belo Horizonte: Conhecimento Editora, 2020

GONÇALVES, Anabela Susana de Sousa. O tratamento de dados pessoais relativos à saúde no âmbito do RGPD. Cidades Inteligentes e Direito, Governação Digital e Direitos, Coimbra: Almedina, p. 251-269, nov. 2023. ISBN: 978-989-40-1598-7.

GREGORI, Maria Stella. Os impactos da lei geral de proteção de dados pessoais na saúde suplementar. Revista de Direito do Consumidor. v. 127, p. 171– 196, jan./fev. 2020.

GREENWALD, G; MACASKILL, E. NSA Prism program taps in to user data of Apple Google and others. The Guardian Online, June 7, 2013. Disponível em: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Acesso em: 20/11/2023.

GRIMALT SERVERA, Pedro. La necessária reconducción del régimen jurídico de la protección de los datos personales desde la perspectiva de los conflitos y solapamentos com otros derechos y libertades en internet. In: VALEROS TORRIJOS, Julián (Org.). La protección de los datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica. Cizur Menor, Navarra: Thomson Reuters/Aranzadi, 2013.

GUIDI, Guilherme Berti de Campos. A proteção dos dados pessoais na internet: contribuições da experiência europeia ao modelo brasileiro. 2016. Dissertação (Mestrado) – Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade de São Paulo, São Paulo, 2016.

GUIMARÃES, Marcia; PILAU SOBRINHO, Liton Lanes. O Direito à Saúde sob a Ótica do Mínimo Existencial e da Reserva do Possível. Revista Eletrônica de Iniciação Científica. Itajaí, Centro de Ciências Sociais e Jurídicas da UNIVALI. v. 4, n.4, p. 574-594, 4º Trimestre de 2013. Disponível em: www.univali.br/ricc - ISSN 2236-5044.

JIN, Julia. Luddism during the Industrial Revolution. In: WESTERN Civilization II guides. 24 abr. 2012. Disponível em: http://westerncivguides.umwblogs.org2012/04/24/luddism-during-the-industrial-revolution/. Acesso em: 20/11/2023

KAMEDA, Paulo Pazello. Segurança em e-Saúde: Desafios e Propostas. Tese de Doutorado, Universidade Estadual de Campinas, 2015.

KANG, Margareth. Uso dos dados pessoais na Coreia do Sul no combate ao coronavírus: O que podemos aprender com a Coreia do Sul? Disponível em:

https://www.jota.info/opiniao-e-analise/artigos/uso-dos-dadospessoais-na-coreia-do-sul-no-combate-ao-coronavirus-03052020. Acesso em: 20/11/2023

KĘDZIOR, M. The right to data protection and the COVID-19 pandemic: the European approach. ERA Forum, 7 dez. 2020. Disponível em: https://link.springer.com/article/1 0.1007/s1 2027-020- 00644-4. Acesso em: 21/01/2014. P. 5.

LEMOS, Alexandre; SAPHIER, Angélica, JÚNIOR EHRHARDT, Marcos. Compliance e a proteção de dados em tempos de covid-19. In: KRELL, Andreas Joachim; DANTAS, Juliana de Oliveira Jota; LINS JÚNIOR, George Sarmento (Org). A pandemia do coronavírus sob a ótica do direito: desafios e transformações em pauta. Maceió: Edufal, 2021,

LEMOS, André; LÉVY, Pierre. O futuro da internet: em direção a uma ciberdemocracia planetária. São Paulo: Paulus, 2010.

LEMOS, Ronaldo. Direito, tecnologia e cultura: desafios jurídicos da comunicação digital. Editora Atlas, 2014.

LIEBERMAN, Joel. (24 de abril de 2012). Luddism during the Industrial Revolution. Disponível em: http://westerncivguides.umwblogs.org2012/04/24/luddism-during-the-industrial-revolution/. Acesso em: 20/11/2023.

LIMBERGER, Têmis. Mutações da privacidade e a proteção dos dados pessoais. In: RUARO, Regina Linden; PIÑAR MAÑAS, José Luis; MOLINARO, Carlos Alberto (Org.). Privacidade e proteção de dados pessoais na sociedade digital. Porto Alegre: Fi, 2017.

LOTUFO, Renan; NANNI, Giovanni Ettore; MARTINS, Fernando Rodrigues (Coord.). Temas relevantes do direito civil contemporâneo: reflexões sobre os 10 anos do Código Civil. São Paulo: Atlas, 2012.

MALDONADO, V. N.; BLUM, R. O. LGPD: Lei Geral de Proteção de Dados comentada. 1. ed. São Paulo: Revista dos Tribunais, 2019.

MARTINS, Guilherme Magalhães. O direito ao esquecimento na Internet. In: Direito Privado e Internet. Coord: Guilherme Magalhães Martins. São Paulo: Editora Atlas, 2014.

MARTINS, Fernando Rodrigues. A galáxia internet. Reflexões sobre internet, negócios e sociedade. Tradução Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004.

MAQUIAVEL, Nicolau. O príncipe. 4. ed. São Paulo: Edipro, 2015.

MEDEIROS, Ana Beatriz; DA SILVA, Letícia de Lourdes Lunna Gesteira. Brasil pandêmico e proteção de dados de crianças e adolescentes no meio digital: diagnósticos gerais. Revista FIDES, v. 11, n. 2, p. 295-312, 21 jan. 2021.

MENÉNDEZ MATO, Juan Carlo; GAYO SANTA CECILIA, Maria Eugenia. Derecho e informática: ética y legislación. Barcelona: Bosch, 2014.

MENEZES, Wagner. Tribunais internacionais: jurisdição e competência. São Paulo: Saraiva, 2013.

MIGUEL ASENSIO, Pedro Alberto de. Derecho privado de internet. 4. ed. Madrid: Civitas, 2011.

MILLS, John L. Privacy: the lost right. New York: Oxford University, 2008.

MODESTO, Jéssica Andrade. O direito à privacidade na sociedade da informação à luz da lei geral de proteção de dados pessoais: uma análise da (in)efetividade da lei nº 13.709/2018 no brasil a partir do estudo comparativo com o regulamento geral de proteção de dados da união europeia. 2021. 364 f. Dissertação (Mestrado em Direito) - Universidade Federal de Alagoas, Alagoas, 2021.

NADER, Paulo. Curso de direito civil: parte geral. 10. ed. Rio de Janeiro: Forense, 2016.

NEWMAN, Abraham L. Building transnational civil liberties: transgovernmental entrepreneurs and the European data privacy directive. International Organization, v. 62, n. 1, p. 106, Jan. 2008. doi: https://doi.org/10.1017/S0020818308080041. Acesso em: 20/11/2023.

OLIVA, Afonso Carvalho de. O auxílio emergencial e a vigilância dos consumidores pós-covid-19. In: BIONI, Bruno Ricardo et. al. Os dados e o vírus: Pandemia, proteção de dados e democracia. São Paulo: Reticências Creative Design Studio, 2020

OLIVEIRA, Ana Paula de. A LGPD brasileira na prática empresarial. Revista Jurídica da Escola Superior de Advocacia da OAB-PR, ano 4, n.1, p. 172-200, 2019

OMS afirma que COVID-19 é agora caracterizada como pandemia - OPAS/OMS | Organização Pan-Americana da Saúde. 11/03/2020. Disponível em: https://www.paho.org/pt/news/11-3-2020-who-characterizes-covid-19-pandemic. Acesso em:15/12/2023.

ONU. Declaração Universal dos Direitos Humanos. Adotada e proclamada pela resolução 217 A (III) da Assembleia Geral das Nações Unidas em 10 de dezembro de 1948. Disponível em: http://unesdoc.unesco.org/images/0013/001394/139423por.pdf. Acesso em: 20/11/2023.

ORWELL, George. 1984. Tradução Alexandre Hubner, Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

ORDÓÑEZ SOLÍS, David. Privacidad y protección judicial de los datos personales. Barcelona: Bosch, 2011.

PARLAMENTO EUROPEU. CONSELHO DA EUROPA. Carta de Direitos Fundamentais da União Europeia (2000/C 364/01). Disponível em: https://www.europarl.europa.eu/ charter/pdf/text _pt.pdf. Acesso em: 20/11/2023.

PILAU SOBRINHO, Liton Lanes. Direito à Saúde: uma perspectiva constitucionalista. Passo Fundo, Universidade de Passo Fundo, 2003. ISBN: 8575151150.

PONTES DE MIRANDA. Tratado de direito privado. Atualizado por Rosa Maria Barreto Borriello de Andrade Nery. São Paulo: Revista dos Tribunais, 2012.

PRIMEIRO contágio pelo coronavírus teria acontecido em novembro, diz jornal, UOL. 13 de mar. 2020.Disponível em: https://noticias.uol.com.br/ultimas-noticias/efe/2020/03/13/jornal-afirma-que-primeiro-contagioda-covid-19-na-china-ocorreu-em-novembro.htm. Acesso em: 20/11/2023.

PUGLIESE, Giovanni. Il diritto alla riservatezza nel quadro dei diritti della personalità. In: Studi in onore di Alberto Asquini. Padova: CEDAM, 1965.

PORTUGAL. Lei n.º 58/2019, de 08 de Agosto. LEI DA PROTEÇÃO DE DADOS PESSOAIS, 2019. Disponível em https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3118A0001&nid=3118&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=#artigo

RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Tradução de Fábio Duarte Joly. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden; PIÑAR MAÑAS, José Luis; MOLINARO, Carlos Alberto (Org.). Privacidade e proteção de dados pessoais na sociedade digital. Porto Alegre: Fi, 2017.

SÁ JUNIOR, Sergio Ricardo C. A regulação jurídica da proteção de dados pessoais no Brasil. 2019. Monografia de especialização – Pontífica Universidade Católica do Rio de Janeiro, Rio de Janeiro.

SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. Porto Alegre: Livraria do Advogado, 2015.

SARMENTO, Daniel; GOMES, Fábio Rodrigues. *A eficácia dos direitos fundamentais nas relações entre particulares: o caso das relações de trabalho*. Rev. TST, Brasília, v. 77, n. 4, p. 60-101, out./dez. 2011.

SARTORI, Giovanni. Homo videns: a sociedade teledirigida. Tradução de Antônio Angonese. Bauru, SP: Edusc, 2001.

SCHREIBER, Anderson. Direitos da personalidade. 3. ed. São Paulo: Atlas, 2014.

SCHREIBER, Mariana. Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco sua privacidade? BBC News Brasil. 21 abr. 2020. Disponível em: https://www.bbc.com/portuguese/brasil-52357879. Acesso em: 20/11/2023.

SCHWARTZ, Germano. Curso de Direito Constitucional. 4. ed. rev. e atual. Rio de Janeiro: Forense, 2016.

SERRANO, Pablo. Vigilância e capitalismo de plataforma. São Paulo: Boitempo, 2019.

SERPA NETO, Ary. Desafios para a Implementação de Prontuário Eletrônico do Paciente em Unidades de Terapia Intensiva Brasileiras. Dissertação de Mestrado, Universidade de São Paulo, 2017.

SILVA, Gabriela Buarque Pereira; MODESTO, Jéssica Andrade; EHRHARDT JÚNIOR, Marcos. O tratamento de dados pessoais no combate à covid-19: entre soluções e danos colaterais. In: EHRHARDT JÚNIOR, Marcos; CATALAN, Marcos; Malheiros Pablo (Coord.). Direito civil e tecnologia. Belo Horizonte: Fórum, 2020

SILVA, João Bosco; BONATTI, Franco. Privacidade em risco: o mundo visto pelas lentes digitais. São Paulo: Revista dos Tribunais, 2011.

SILVA, M. L. F. DA; TEIXEIRA, M. A. C.; FRANCISCO, E. DE R. O uso de dados pessoais no combate à COVID-19: alcances e limites das experiências do Brasil e da União Europeia. Revista de Gestão dos Países de Língua Portuguesa, v. 21, n. 2, p. 107–123, 23 ago. 2022.

SOLOVE, Daniel J. Understanding Privacy. Harvard Law Review, v. 113, n. 3, p. 745-772, 2000.

SOUZA, Washington Bandeira de. Introdução ao direito digital. 3. ed. São Paulo: Atlas, 2014.

TEFFÉ, Chiara Spadaccini de. MAGRANI. Eduardo. VIOLA, Mario. Artigo “5 pontos sobre a importância de uma autoridade nacional de proteção de dados”. Disponível em:https://medium.com/@ITSriodejaneiro/5-pontos-sobreaimport%C3%A2ncia-de-uma-autoridade-nacionaldeprote%C3%A7%C3%A3ode-dados-4cf8137cf59e. Acesso em 20/11/2023.

TIBÚRCIO L. Emenda Constitucional 115/2022: direito à proteção de dados pessoais. 2022. Disponível em: https://www.estrategiaconcursos.com.br/blog/emenda-constitucional-115-2022/. Acesso em: 20/11/2023.

TINTO, Ana Rita Ramos Y Rio. Proteção de dados de saúde Percepção e conhecimento dos Administradores Hospitalares acerca do novo Regulamento Geral de Proteção de Dados da União Europeia. 2018. Dissertação (Mestrado). Escola Nacional de Saúde Pública. Universidade Nova de Lisboa, Lisboa, 2018.

TZU, Sun. A arte da guerra. Tradução Sueli Barros Cassal. Porto Alegre.

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 20/11/2023

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no

que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 20/11/2023

UNIÃO EUROPEIA. REGULATION (EC) No 1338/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 December 2008 on Community statistics on public health and health and safety at work (Text with EEA relevance). [s.l: s.n.]. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R1338&from=PT. Acesso em: 20 jan. 2024.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial L. 119/1008, 04 de maio de 2016. art. 9º, alínea gDisponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 20/11/2023.

UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas. Jornal Oficial L. 201, 31 de julho de 2002. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32002L0058. Acesso em: 20/11/2023

UNIÃO EUROPEIA. Diretrizes 04/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19. , 21 abr. 2020. P.4. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_pt.pdf. Acesso em: 27 jan. 2024.

UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas. Jornal Oficial L. 201, 31 de julho de 2002. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32002L0058. Acesso em: 20/11/2023

UNIÃO EUROPEIA. Decisão de Execução (UE) 2016/1250 da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho. Jornal Oficial L. 207/1, 01 de agosto de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016D1250. Acesso em: 20/11/2023

UNIÃO EUROPEIA. Corte de Justiça da União Europeia. Casos conjuntos C-293/12 e C 594/12. DigitalRights Ireland Ltd. v. Ireland, julgados em 8 de abril de 2014. Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang= PT&cid=513860. Acesso em: 20/11/2023.

URUPÁ, Marcos. Para AGU, compartilhamento de dados de geolocalização não fere LGPD e Constituição. Teletime. Disponível em: https://teletime.com.br/13/04/2020/para-agu compartilhamento-de-dados-degeolocalizacao-nao-fere-lgpd-e-constituicao-federal/. Acesso em: 20/11/2023

VIEIRA, Fabio Alonso; COSTA, Carolina Barbosa Cunha. Data Privacy and Protection Relating to Healthcare in Europe, the United States and Brazil.Latin Lawyer. August 2021. Disponível em: https://latinlawyer.com/guide/the-guide-corporate-compliance/secondedition/article/24-data-privacy-and-protection-relating-healthcare-in-europe-the-united-statesand-brazil. Acesso em: 20/11/2023

VIEIRA, Renata Malta. A privacidade na era digital. São Paulo: Revista dos Tribunais, 2018.

WARREN, Samuel. BRANDEIS, Louis. The Right to Privacy Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.Disponível em Http://links.jstor.org/sici?sici=0017811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C.Acesso em 20/11/2023.

WESTIN, A. F. Privacy and Freedom. Atheneum, 1967.

ZOOM. A Message to Our Users. Disponível em: https://blog.zoom.us/a-message-to-our-users/. Acesso em: 20/11/2023.