UNIVERSIDADE CESUMAR, CAMPUS MARINGÁ, PR.
PROGRAMA DE PÓS GRADUAÇÃO EM CIÊNCIAS JURÍDICAS

KEVIN HENRIQUE DE SOUSA PIAI

A EFETIVAÇÃO DO DIREITO DA PERSONALIDADE FRENTE AO ADEQUADO TRATAMENTO DOS DADOS PESSOAIS NO MEIO DIGITAL

MARINGÁ, PR.
2022

KEVIN HENRIQUE DE SOUSA PIAI

A EFETIVAÇÃO DO DIREITO DA PERSONALIDADE FRENTE AO ADEQUADO TRATAMENTO DOS DADOS PESSOAIS NO MEIO DIGITAL

Projeto de qualificação de dissertação de mestrado apresentado ao Programa de Pós-graduação em Ciências Jurídicas da Universidade Cesumar (PPGD/UNICESUMAR), como pré-requisito obrigatório à obtenção do título de Mestre em Ciências Jurídicas.

Orientador: Prof. Dr. Oscar Ivan Prux

MARINGÁ, PR.

2022

KEVIN HENRIQUE DE SOUSA PIAI

A EFETIVAÇÃO DO DIREITO DA PERSONALIDADE FRENTE AO ADEQUADO TRATAMENTO DOS DADOS PESSOAIS NO MEIO DIGITAL

Banca Examinadora:

_____ - Orientador
Prof. Dr. Oscar Ivan Prux
Doutor em Direito do Consumidor pela Universidade de Lisboa – Portugal (FDUL).
Professor de direito na pós-graduação *stricto sensu* da Universidade Cesumar.

_____ - Membro titular

Prof. Dr. Marcelo Negri Soares
Doutor em Direito do Consumidor pela Pontifícia Universidade Católica de São Paulo.
Professor do Programa de Mestrado e Doutorado em Direito UniCesumar.

_____ - Membro Titular Externo

Prof.ª Dra. Mariana Ribeiro Santiago
Pós-Doutora em Direito Civil pela Justus-Liebig-Universität Gieen (Alemanha)
Professora do Programa de Mestrado e Doutorado em Direito da Universidade de Marília – (UNIMAR)

Dados Internacionais de Catalogação na Publicação (CIP)

P579e Piai, Kevin Henrique de Sousa.
A efetivação do direito da personalidade frente ao adequado tratamento dos dados pessoais no meio digital / Kevin Henrique de Sousa Piai. Maringá-PR: UNICESUMAR, 2022.
172 f. ; 30 cm.

Orientador: Prof. Dr. Oscar Ivan Prux.
Dissertação (mestrado) – Universidade Cesumar - UNICESUMAR, Programa de Pós-Graduação em Ciências Jurídicas, Maringá, 2022.

1. Dados pessoais. 2. Direitos da personalidade. 3. Efetivação. I. Título.

CDD – 342.0858

Roseni Soares – Bibliotecária – CRB 9/1796
Biblioteca Central UniCesumar

Ficha catalográfica elaborada de acordo com os dados fornecidos pelo(a) autor(a).

Aos meus pais, minha família e minha esposa.

“Não há poderes soberanos, neste regime. Todos os poderes são subordinados à Constituição; e, se dela exorbitam, hão de voltar a ela pela força constitucional da autoridade judiciária.”

Ruy Barbosa

AGRADECIMENTOS

Não há como passar por anos tãos complexos e nebulosos e não ser grato primeiramente à Deus, pela oportunidade do sopro e permanência neste plano.

A partir disso, aos que compartilham dos anseios, angústias e fragilidades que constantemente nos encampam nestas fases de retiro do conforto. Esta experiência me mostrou ser possível superar limites e obstáculos, há tempos compreendidos por mim mesmo como intransponíveis. Isso se dá há um elemento, não tão vasto, composto por pessoas que alicerçam e sedimentam de maneira nobre, o intenso prazer de estar presente. Entre elas, minha família, o núcleo mais genuíno da composição humana e que lastreia este momento. Não foi fácil, chegar, estar e permanecer aqui, o nível sempre será mais alto, a cobrança de ontem passará a ser maior do que a estabelecida hoje, e assim, seguimos, em constante e necessária evolução.

Por estas e outras, é que muitas vezes nas adversidades, aprendemos a valorizar os que estão na fronte e não nos desamparam, mesmo quando tudo parece ter se limitado do plano material. São com estas singelas considerações, que enumero aqui em primeiro, minha mãe, pela incansável luta de me proporcionar dias melhores através do estudo, mesmo que isso tenha lhe custado à privação de sonhos pessoais, faltam-me palavras para agradecer!

A meu pai, que nunca mediu esforços ou criou obstáculos para minha felicidade e formação. Aos meus padrinhos que são consequência da minha chegada até aqui, mediante patrocínio incondicional e psicológico, que me proporcionaram à oportunidade do melhor estudo. Sem precedentes, à minha linda esposa que compreende, apoia, luta, perserva, tornando-se força e luz para trilha destes caminhos, até aqui em muitas oportunidades nebulosos.

Sobre medida, ressalto meu mais leal e fraterno agradecimento ao Professor Oscar Ivan Prux, pela grata felicidade em me aceitar como orientando neste Programa de Mestrado. Tenho muito orgulho de citá-lo como um dos responsáveis pela minha formação profissional. Agradeço sem medidas pela confiança, pela amizade, conselhos e paciência que lhe é intrínseca. O senhor é um exemplo de simplicidade, compreensão, profissionalismo, retidão e competência. Todos que trabalham com o senhor admiram sua dedicação e amor ao trabalho, à academia, aos alunos e orientados. Enfim, vai muito além do que o dever impõe, não tem hora e nem lhe falta apetite e simplicidade para aprender, sempre solícito, disposto e preocupado não só com a realização do trabalho, mas principalmente com o ser humano, deixo aqui minha manifestação da mais sublime honra e prazer em conhecer o profissional e ser humano.

Não podendo deixar obviamente de agradecer aos professores da Graduação e do Mestrado, alguns em ambos, que sem dúvidas fizeram parte da construção desta caminhada, que

teve início há longos anos, desde a iniciação científica, até a preparação da seletiva, muitos foram os desafios, aqui estamos e próximos do fim deste ciclo. Um fraterno agradecimento ao Prof. Thomaz Jefferson Carvalho, pela amizade, cumplicidade, apoio e orientação durante a graduação e na vida, você faz parte disso!

Por fim, a todos meus familiares, minha avó, meus tios e tias, minhas primas e primos queridos, que manejam luz sobre esta trilha, que é constituída de muita luta e sacrifício de todas as ordens pessoal, profissional, são horas de dedicação e tempo, com intuito não só do aperfeiçoamento pessoal, mas genuinamente com maior profundo desejo e responsabilidade de contribuir em alguma medida para o bem-estar social e melhoria de vidas, seja em qual medida.

RESUMO

A revolução tecnológica e o consequente estabelecimento da sociedade de informação exigiram a modificação do consumo para relações desmaterializadas, desterritorializadas e, a princípio, despersonalizadas. A utilização massiva de dados pessoais por organismos estatais e privados, a partir de avançadas tecnologias da informação, apresenta novos desafios ao direito à privacidade. As combinações de diversas técnicas automatizadas permitem a obtenção de informações sensíveis sobre os cidadãos, que passam a fundamentar a tomada de decisões econômicas, políticas e sociais. Nesse contexto, destaca-se a técnica de construção de perfis pessoais de forma voluntária e/ou involuntária, a partir dos quais podem ser tomadas decisões a respeito das pessoas, afetando diretamente as suas vidas e influenciando o seu acesso a oportunidades sociais. Crescem, portanto, os riscos ao direito de personalidade do cidadão, na medida em que esses perfis, verdadeiros clones virtuais, representam informações fragmentadas e descontextualizadas, que podem ser utilizadas de modo a prejudicar a liberdade e a chance de vida do indivíduo. Esses riscos, ampliados pela utilização da tecnologia da informação, tornam imperativa a regulamentação jurídica da matéria. Assim, se mostra necessário criar no país uma cultura jurídica apta a dar eficácia a este direito fundamental autônomo, que tem origem no direito à privacidade, mas que possui traços e distinções, em razão das transformações sociais e tecnológicas. Cumpre também verificar, que o presente estudo, tem por intuito realizar análise de decisões judiciais, que ao fim e ao cabo, buscam aferir e sistematizar os atuais critérios jurisprudenciais empregados pelo Poder Judiciário Brasileiro para fundamentação teórica e normativa, quando do enfrentamento de questões relativas à violação de dados pessoais. Por fim, o estudo tem por intuito problematizar a discussão dos resultados através do método dialético, com apresentação de proposições teóricas e empíricas acerca do objeto de pesquisa, em especial, à eficácia da proteção dos dados pessoais como um direito autônomo fundamental, agora devidamente consagrado na órbita constitucional.

Palavras-chave: dados pessoais; direitos da personalidade; efetivação.

ABSTRACT

The technological revolution and the consequent establishment of the information society demand a change in consumption towards dematerialized, deterritorialized and, in principle, depersonalized relationships. The massive use of data by state and private bodies, to new information technology resources, presents new challenges to the right to privacy. The fundamental solutions of strategic solutions allow the solution of decisions and social information, which In this sense, access to the construction of personal profiles in an artistic and influential technical and/or involuntary way, from which decisions can be made regarding the people, directly affecting their social opportunities and their opportunities. Therefore, the risks to the citizen's personality right grow, insofar as these profiles, true virtual clones, represent fragmented and decontextualized information, which can be used in order to harm the individual's freedom and chance of life. These risks, amplified by the use of information technology, make the legal regularization of the matter imperative. Thus, it is not necessary to have a culture able to give due diligence to this autonomous fundamental right, which originates in the right to privacy, but which has traits and distinctions, due to social and technological transformations. It should be noted that the present study also has questions regarding respect for the Brazilian cable, which at the end and purpose, seek to assess and analyze the current jurisprudential criteria by the judiciary when the theoretical and normative foundation, face the respect of the laws to the data of people. Finally, the has to problematize the discussion of the results through the dialectical purpose, with the presentation of theoretical proposals on the data object, in a special presentation, to the determination of the protection of personal data as a method of study of fundamental right, now properly in the constitutional sphere.

Keywords: personal data; personality rights; effectiveness.

LISTA DE ABREVIATURAS E SIGLAS

AC	Ação Cautelar
ADI	Ação Direta de Inconstitucionalidade
ADPF	Arguição de Descumprimento de Preceito Fundamental
AgR	Agravo Regimental
ANATEL	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados
CBS	Columbia Broadcasting System
CDC	Código de Defesa do Consumidor
CGI.br	Comitê Gestor da Internet no Brasil
CNIL	*Commission Nationale Informatique & Libertés*
CNJ	Conselho Nacional de Justiça
DJEs	Diário da Justiça Eletrônico
DPDC	Departamento de Proteção e Defesa do Consumidor
GitHub	Plataforma de hospedagem de código-fonte e arquivos baseado em Git.
HC	Habeas Corpus
IBDC	Instituto Brasileiro Direito Constitucional
IDEC	Instituto Brasileiro de Defesa do Consumidor
LGPD	Lei Geral de Proteção de Dados Pessoais
MP	Ministério Público
MPF	Ministério Público Federal
MS	Mandado de Segurança
NDC	Contribuição Nacionalmente Determinada
NSA	Agência de Segurança Nacional
NUP	Número Único de Protocolo
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
PEC	Proposta de Emenda à Constituição
PLBIR	*Privacy Laws & Business International Report*
PROCON	Programa de Proteção e Defesa do Consumidor
R	R é uma linguagem de programação
Rcl	Reclamação
RE	Recurso Extraordinário
Rstudio	RStudio é um software livre de ambiente de desenvolvimento integrado para R
SBDC	Sociedade Brasileira de Desenvolvimento Comportamental

SERPRO	Serviço Federal de Processamento de Dados
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TJ	Tribunal de Justiça
UE	União Europeia
USA	Estados Unidos da América

LISTA DE FIGURAS

FIGURA 1 - SERPRO – ADAPTADO CNIL, FRANÇA, DEZ. 2019. 28
FIGURA 2 - GRÁFICO DA LINHA DO TEMPO DAS LEIS DE PRIVACIDADE DE DADOS ENTRE 1973 – 2020 30
FIGURA 3 - NUVEM DE PALAVRAS DAS DECISÕES MONOCRÁTICAS SOBRE DADOS PESSOAIS NO STF. 119
FIGURA 4 - RELATORIA DE MINISTROS ACERCA DA PROTEÇÃO DE DADOS, STF. 120
FIGURA 5 - DEMONSTRATIVO DE PROCESSOS POR CAPÍTULO DA LGPD. 125
FIGURA 6 - LINHA DO TEMPO DE DECISÕES POR MÊS – SET.2020 A AGO.2021. 128
FIGURA 7 - GRÁFICO COM NÚMERO DE DECISÕES POR MINISTRO DO STF. 129
FIGURA 8 - GRÁFICO COM OCORRÊNCIA DE DEMANDAS NO STF SOBRE O TEMA 130
FIGURA 9 - LINHA DO TEMPO COM OCORRÊNCIA POR DATA DAS DECISÕES NO ÂMBITO DO STF. 130
FIGURA 10 - CLASSIFICAÇÃO DAS DECISÕES PROFERIDAS PELO STF. 131
FIGURA 11 - CLASSIFICAÇÃO DA RELEVÂNCIA DAS DECISÕES PROFERIDAS PELO STF 131
FIGURA 12 - CLASSIFICAÇÃO COMPLETA DAS DECISÕES MENCIONADAS 132
FIGURA 13 - GRÁFICO DE DISTRIBUIÇÃO DAS DEMANDAS ENTRE JUSTIÇA COMUM E ESPECIALIZADA 143
FIGURA 14 - GRÁFICO DE DISTRIBUIÇÃO DAS DEMANDAS NO ÂMBITO DA JUSTIÇA DO TRABALHO. 143
FIGURA 15 - GRÁFICO DE DISTRIBUIÇÃO DE ALOCAÇÃO DAS DEMANDAS POR TRIBUNAL 145
FIGURA 16 - LINHA DO TEMPO DE DECISÕES POR MÊS 145
FIGURA 17 - GRÁFICO DE ALOCAÇÕES DE DEMANDAS POR CAPÍTULO DA LGPD 146

SUMÁRIO

1. INTRODUÇÃO 14

2. O PANOPTISMO DIGITAL E A INAUGURAÇÃO DA DENOMINADA *DATA-DRIVEN SOCIETY AND ECONOMY*... 19

2.1. A TUTELA DA PRIVACIDADE E PROTEÇÃO DE DADOS NO CENÁRIO INTERNACIONAL 26

3. O QUE SÃO DADOS PESSOAIS E O QUE NÃO SÃO DADOS PESSOAIS 31

3.1. DADOS PESSOAIS E TUTELA JURÍDICA: CONCEITOS E DIMENSÕES 37
3.2. ENTRE O DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS 40
3.2. OS PRINCÍPIOS NORTEADORES DA PROTEÇÃO DE DADOS PESSOAIS 47
3.3. O CONCEITO DE AUTODETERMINAÇÃO INFORMATIVA E A ESTRUTURAÇÃO DE UM DIREITO À PROTEÇÃO DE DADOS PESSOAIS NA UNIÃO EUROPEIA 50

4. OS DADOS PESSOAIS E SUAS FORMAS DE TRATAMENTO NO AMBIENTE FÍSICO E DIGITAL E SUAS CONSEQUENCIAS PARA O DIREITO 52

4.1. O TRATAMENTO DE DADOS PESSOAIS NO ÂMBITO PÚBLICO E PRIVADO 52
4.1.1. O uso de dados pessoais pelo Poder Público 54
4.1.2. A utilização de dados pessoais em nome da segurança pública e suas implicações à tutela dos direitos difusos e individuais dos cidadãos 56

4.2. A UTILIZAÇÃO DE DADOS PESSOAIS NA PERSPECTIVA DAS RELAÇÕES PRIVADAS DE CONSUMO 67

4.4. SUAS CONSEQUÊNCIAS NO DIREITO PRIVADO 74
4.5. PRIMORDIALIDADE DA REGULAÇÃO DE NORMAS DE PRIVACIDADE DE DADOS PARA CRIANÇAS E ADOLESCENTES 75

5. A RESPONSABILIDADE CIVIL NO PLANO DA PROTEÇÃO DE DADOS PESSOAIS 85

5.1. A FUNÇÃO REPARATÓRIA DA RESPONSABILIDADE CIVIL NA TUTELA DOS DADOS PESSOAIS 93
5.2. A FUNÇÃO PUNITIVA DA RESPONSABILIDADE CIVIL NA TUTELA DOS DADOS PESSOAIS 94
5.3. A FUNÇÃO PREVENTIVA DA RESPONSABILIDADE CIVIL NA TUTELA DOS DADOS PESSOAIS 94
5.4. PERSPECTIVA DE UMA FUNÇÃO PROMOCIONAL E PREVENTIVA DA RESPONSABILIDADE CIVIL NO ÂMBITO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL 97
5.4.1. A função preventiva e o princípio da precaução 97
5.4.2. Distinções entre a função reparatória, preventiva e promocional 99
5.4.3. A função promocional nos danos individuais nas relações de consumo 101
5.5. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: ESTRUTURA VITAL PARA FISCALIZAÇÃO E PENALIZAÇÃO 107

6. CONTORNOS LEGISLATIVOS E JURISPRUDENCIAIS NO ÂMBITO DA PROTEÇÃO DE DADOS EM COMPASSO AO DIÁLOGO DAS FONTES 112

6.1. ANÁLISE DA JURISPRUDÊNCIA SOBRE PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DO SUPREMO TRIBUNAL FEDERAL 118
6.2. ANÁLISE DA JURISPRUDÊNCIA SOBRE PROTEÇÃO DE DADOS NO ÂMBITO DO SUPERIOR TRIBUNAL DE JUSTIÇA 132
6.2.1. Análise dos cadastros negativos e positivos de crédito 133
6.2.2. O (credit score) ou avaliação de risco de crédito no mercado de consumo 135
6.2.3. Remoção de conteúdos da internet e o direito ao apagamento de dados pessoais 137
6.3. COMO A JURISPRUDÊNCIA DECIDE SOBRE A PROTEÇÃO DE DADOS PESSOAIS EM DETERMINADOS TRIBUNAIS DE JUSTIÇA DO PAÍS 142
6.4. DO ENTENDIMENTO JURISPRUDENCIAL DOS DADOS PESSOAIS ENQUANTO DIREITO FUNDAMENTAL 148
6.5. UMA AGENDA REGULATÓRIA CONVERGENTE COM A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL 155
6.6. A PROTEÇÃO DE DADOS PESSOAIS EM SIMBIOSE COM A DIGNIDADE DA PESSOA HUMANA E O DIREITO AO LIVRE DESENVOLVIMENTO DA PERSONALIDADE NO ORDENAMENTO JURÍDICO BRASILEIRO EM COMPASSO COM O DIÁLOGO DAS FONTES . 158

7. CONCLUSÃO 162

REFERÊNCIAS 165

1. INTRODUÇÃO

Novas maneiras de pensar e de convivência estão sendo elaboradas e incrementadas na era digital. Em especial neste século, as relações humanas vêm mostrando significativa alteração nas dinâmicas da vida em sociedade, fazendo emergir uma nova dimensão fundamental no Direito envolvido com o entrelaçamento do real com o virtual. Há uma transformação do mundo humano por ele mesmo, contexto influenciado em muito pelo universo digital em que os dados pessoais são o pilar motriz.

Em tempos contemporâneos, aquilo que denominamos de Sociedade Informacional, impera a utilização mais ampla de dados pessoais para as mais variadas finalidades tais como a identificação, classificação, autorização, dentre outras variadas. A revolução da tecnologia da informação alterou radicalmente a realidade social, penetrando em todas as esferas das atividades humanas e, por conseguinte, criando novas situações a serem reguladas pelo sistema jurídico.

Nesse cenário, há muitos valores em jogo. Dentre estes, a privacidade, como a conhecemos, é um dos bens da vida mais caros ao ser humano, uma vez que, sem ele, o ser humano se expõe de modo a violar sua própria personalidade. Em 1949, na sua emblemática obra intitulada “1984” de George Orwell propôs uma sociedade completamente dominada por um governo totalitário, onde os dados pessoais dos cidadãos seriam elementos centrais. Independente da ficção literária, a realidade é que os fatos novos vêm se antecipando ao direito e demonstrando o papel exponencial dos dados pessoais na sociedade conectada, tudo numa velocidade que a criação de legislação específica não tem conseguido acompanhar.

Neste espectro, ordenamentos jurídicos de diversos países passaram a tutelar expressamente os dados pessoais de seus cidadãos, por entenderem que tais dados constituem uma projeção da personalidade do indivíduo, merecendo inclusive, em algumas oportunidades, uma tutela constitucional.

No plano internacional, mesmo praticamente iniciando-se a terceira década do Século XXI, diversos Estados não preveem em seus comandos constitucionais, o expresso reconhecimento da proteção de dados pessoais como direito fundamental; ao menos na condição de direito literalmente positivado pela Carta Constitucional. Ou seja, se limitam a manter um plano de fundo que permite expandir esse direito como implicitamente positivado, conforme o caso, seja utilizando adaptação legislativa, constitucional, ou seja pela fonte de direito representada pela jurisprudência.

Nesta senda, promulgada a Constituição Federal de 1988, que, em razão de seu caráter implicitamente social, amplia conceitos e o alcance da ideia de Constituição no Brasil. A Constituição é o ordenamento jurídico fundamental do Estado e da sociedade, que constitui e limita os processos de poder.[1] E, a partir das suas características sistemáticas, ela configura um sistema de direitos fundamentais que institucionaliza os pressupostos de comunicação necessários à autodeterminação democrática dos cidadãos.[2] Em análise dinâmica da Constituição, a realidade fática é mais flexível que o mundo do direito, que está sempre em busca desta equalização com o mundo dos fatos, por sua vez passível de trilhas até a rota de ajuste, sempre sujeito a alterações interpretativas, que refletem um processo de aprendizagem falível.

O texto constitucional prevê diversas disposições que se relacionam à proteção da privacidade e dos dados pessoais, como a inviolabilidade da vida privada e da intimidade (art. 5°, X), a proibição da interceptação de comunicações telefônicas, telegráficas ou de dados (art 5°, XII), a vedação da invasão de domicílio (art. 5°, XI) e de correspondência (art. 5°, XII) e a possibilidade de impetração do habeas data (art. 5°, LXXII).

Nesse contexto, uma mudança importante diz respeito à eficácia dos direitos fundamentais, em aporte às obras de Ingo Sarlet[3] e Barroso[4], que passam a compreender, além da eficácia sobre a relação entre os cidadãos e o Estado, uma eficácia também relativa a entes privados. Isso significa que os direitos fundamentais, antes aplicáveis apenas contra órgãos do governo ou de seus representantes, passam a ser compreendidos como direito também de eficácia privada, incidentes até mesmo sobre relações entre particulares. É o caso dos direitos à privacidade, à liberdade e à igualdade, que são de extrema relevância para o estudo da violação dos dados pessoais.

A Constituição Brasileira de 1988, não contemplava em seu texto, até 11.02.2022 um

---

[1] HÃBERLE, Peter. Incursus. Perspectiva de uma doctrina constitucional del marcado: siete tesis de trabajo. In: HÃBERLE, Peter. Nueve ensayos constitucionales y na lección jubilar. Trad.: Luciano Parejo Alfonso e outros. Lima: Palestra Editores, 2004, p. 103.

[2] HABERMAS, Jürgen. Direito e democracia: entre facticidade e validade. Vol. II. Trad. Flávio beno Siebeneichler. Rio de Janeiro: Tempo Brasileiro, 1997, p. 119.

[3] MONTEIRO, António Pinto; NEUNER, Jörg; SARLET, Ingo. Direitos fundamentais e direito privado: uma perspectiva de direito comparado. 1. ed. [S.l.]: Almedina Brasil, 2007, pg. 142.

[4] BARROSO, Luís Roberto. A nova interpretação constitucional: ponderação, direitos fundamentais e relações privadas. 2. ed. Rio de Janeiro, RJ: Renovar, 2006, pg. 33.

autônomo direito fundamental à proteção de dados pessoais.[5] Entretanto, pode-se observar que o art. 5º, X, da Carta Magna prescreve serem invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, direitos que se relacionam com a proteção de dados, mas tudo sem um detalhamento específico a respeito, inclusive para esclarecer as questões relacionadas ao significado jurídico, alcance e parâmetros de interpretação desses termos. Por conta disso, segundo expressiva literatura jurídica e mesmo algumas decisões jurisprudenciais, inclusive do Supremo Tribunal Federal (vide ADI 6387)[6], a proteção de dados acaba sendo tida como implicitamente positivada no texto constitucional, ficando para a legislação infraconstitucional o seu detalhamento mais específico. Nesse contexto, note-se inclusive, que o avanço da denominada *data driven society and economy*[7], tem impactado não apenas o direito positivo, ou seja, a digitalização dos direitos fundamentais[8] produção legislativa e normativa, mas contagiado a dogmática, estendendo "tentáculos" para os domínios da administração pública e atividade dos Tribunais, sendo que para estes últimos, em maior medida, cabe a missão de formular soluções (por vezes criativas) para os problemas concretos que lhes são submetidos.

Desta sorte, com avanço da "sociedade de dados", em paralelo, ocorre o que se denomina dimensão digital dos direitos fundamentais ou digitalização do direito. No direito brasileiro, tal fenômeno foi recepcionado na concepção de ser direito digital autônomo,[9] expressamente em compasso com avanços do direito internacional, a ponto de receber ampliação no âmbito de um direito humano específico para a proteção de dados (e garantias a ele conexos); em verdade, uma nova forma de dar ressignificação ou releitura para determinados direitos clássicos (como privacidade, intimidade, etc.).

Ou seja, essas concepções mostram que o direito a proteção de dados já é uma realidade no Brasil, contribuindo inclusive no sentido de instaurar uma linha limítrofe para atuação do Poder Público, como bem decidiu o STF no julgamento da Medida Cautelar da ADI 6387 (STF, 2020). Ressalte-se ainda, nessa conjuntura, o início da vigência da Lei Geral de Proteção de

---

[5] Emenda Constitucional Nº 115/2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. D.O.U. Publicado em: 11/02/2022 | Edição: 30 | Seção: 1 | Página: 2.

[6] (STF - ADI: 6387 DF 0090566-08.2020.1.00.0000, Relator: ROSA WEBER, Data de Julgamento: 07/05/2020, Tribunal Pleno, Data de Publicação: 12/11/2020)

[7] CURIAK, Dan and Maria Ptashinka. "Leveraging the Digital Transformation for Development: A Global South Strategy for the Data-driven Economy." CIGI Policy Brief 148 (April 3, 2019). https://www.cigionline.org/publications/leveraging-digital-transformation-development-global-south-strategy-data-driven.

[8] ROSSNAGEL, Alexander; WEDDE, Peter; HAMMER, Volker; PORDESCH, Ulrich. Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations-und Kommunikationstechnik. Opladen: Westdeutscher Verlag, 1990.

[9] HOFFMANN-RIEM. Innovation und Recht: Recht und Innovation. Heidelberg: Mohr Siebeck, 2016.

Dados, que no âmbito infraconstitucional, por meio de sua aplicação transversal, tem como um entre seus os objetivos (*mens legis*), garantir segurança jurídica e uniformidade a matéria. No combate à fragmentação, a LGPD conjuga em diversos diplomas, as prescrições pertinentes à proteção de dados, incidindo tanto na atuação do poder público, quanto na esfera privada, tudo com efeito de ampliar o debate para plano constitucional, em *prima facie*, em decorrência desse direito enquanto positivado.

Nesse aspecto, tange a liberdade não somente de ir e vir, mas de acesso (inclusão), oportunidades e escolhas; as nuances que envolvem discriminação algorítmica no acesso a crédito no mercado de consumo, nas questões relativas ao processo de seletivo de pessoas baseados em dados de saúde e comorbidade pré-existentes, dentre outras muitas questões da exclusão social, que podem ser ou não isenta de vieses discriminatórios.

Com esse pressuposto, o direito à privacidade e proteção de dados pessoais deriva da privacidade, previsto na constituição federal, infere-se que a tutela dos dados decorre da Constituição brasileira. Isso significa, sob o ponto de vista de seu caráter negativo, que nenhuma lei poderá ser promulgada de modo a eliminar esse direito fundamental, sob pena de vir a ser considerada inconstitucional e ser declarada nula.

Outrossim, à luz do seu caráter positivo, o direito fundamental à proteção de dados pessoais, agora, reconhecido diretamente pela carta constitucional, enseja a obrigatoriedade de ação do Estado para proteger a personalidade, tal como a edição do sistema jurídico que regulamenta o assunto. Nesse caso, compreende-se que o direito é garantido constitucionalmente, mas a sua densificação e conformação dependem da ação estatal.

Referida técnica normativa-legislativa acabou por fundamentar uma interpretação no mínimo temerosa no que diz respeito à matéria: se, por um lado, a privacidade é encarada como um direito fundamental, serem protegidas somente em relação à sua "comunicação", conforme o art. 5°, XII, que trata da inviolabilidade da comunicação de dados.

Ainda, tendo em conta tais fundamentos e parâmetros normativos, buscar-se-á delimitar o âmbito de proteção do direito fundamental, agora expresso, à proteção de dados pessoais na ordem jurídico-constitucional brasileira, na condição de um direito que, embora conectado fortemente com outros direitos fundamentais, assume claramente a condição de autônomo, conforme abordado recentemente pelo STF[10] acompanhado posteriormente pela Emenda

[10] Ocasião do julgamento do pedido de medida liminar na ADIn 6387, Relatora Ministra Rosa Weber.

Constitucional de n° 115 de 2022.[11]

Para além da sedimentação exclusivamente teórica, o referido estudo tem por frente de trabalho a realização de análise prática, mediante o uso da plataforma open-source R através da utilização do RStudio, por uso de bases já mineradas pela Associação Brasileira de Jurimetria e também pelo Prof. Dr. José de Jesus Filho no Supremo Tribunal Federal, via bases disponíveis no site Github, através da técnica de análise de jurisprudências que ao fim e ao cabo, buscam aferir e sistematizar os atuais critérios jurisprudenciais empregados pelos Ministros do Supremo Tribunal Federal para fundamentação teórica e normativa, quando do enfrentamento de questões relativas à violação de dados pessoais.

Para o desenvolvimento da presente pesquisa, a fonte de conhecimento está sedimentada inicialmente no estudo doutrinário dos referenciais teóricos selecionados como guias de análise do problema, com um estudo interdisciplinar entre a Filosofia, Direito do Consumidor, Constitucional, Cível, Processo Civil e Tecnologia de Informação.

Após estas leituras, construiu-se a linha teórica buscando concluir com base em produções científicas consultadas, auxiliados também por uma interpretação dos diplomas legais através dos processos lógico e sistemático. Utiliza-se ainda, como ferramenta apta a abordar as abstratas e complexas situações estudadas, metáforas e analogias para descrever tanto hipóteses aferidas como sugestões e influenciar um norte de soluções a serem alcançadas.

Assim, atendo-se à metodologia proposta, passa-se a analisar, nos capítulos que seguem, certos aspectos históricos e conceituais que envolvem o direito fundamental à privacidade, os valores a ele conexos, os diplomas legais normatizantes no Brasil e a discussão que levou até a necessidade de proteção dos dados pessoais como corolário da proteção à privacidade.

No campo da economia de dados, relações de poder, consumo e privacidade tomar-se-á como base a análise das obras Bauman (2008) Lipovetsky (2007), Castells (2000, 2015), Bauman e Lyon (2013) Zuboff (2018), Pierre Levy (1993), Sibilia (2010), todas listadas nas referências bibliográficas, sem prejuízo da análise de outros pensadores a serem indicados durante o desenvolvimento da pesquisa, no que diz respeito ao estabelecimento da economia de dados como uma relação de poder, cujo consumo se torna um condutor central do indivíduo.

Por outro lado, é necessário o estudo sobre aspectos da tecnologia da informação para analisar os mecanismos de coleta, tratamento e disposição de dados pessoais, além da formação de um novo ciclo mercadológico com novos agentes inseridos, a partir de uma reconstrução

[11] Emenda Constitucional Nº 115/2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. D.O.U. Publicado em: 11/02/2022 | Edição: 30 | Seção: 1 | Página: 2.

direcionada, possibilitando a incidência do assédio de consumo virtual, e seus impactos aos direitos da personalidade, utilizando como fontes as obras de Mendes (2015, 2019), Bioni (2018, 2020), Sarlet (2007, 2018), Doneda (2018), Schertel (2021), Menke (2021), Lemos (2021), Brito Cruz (2021), Wolfgang Hoffmann-Riem (2020), Zampier (2018) Taveira Junior (2021), Martins (2019), Rosenvald (2018) e demais referências.

A partir de então, realizada pesquisa doutrinária sobre a privacidade, destacando o seu caráter individual e coletivo, apresentado por Warren e Brandeis (1890), Solove (2004, 2008), Rodotà (2008), Leonardi (2011), Doneda (2019), a fim de analisar o panorama de proteção de dados, identificando os pressupostos de viabilidade teórica para sedimentação da tutela constitucional dos dados pessoais como um direito fundamental autônomo.

A análise bibliográfica, portanto, constitui a base da primeira fase da pesquisa a ser desenvolvida. Entretanto, também será apontada outra face: a análise legislativa em si, principalmente a partir da terceira seção. Assim, a terceira face tem por objetivo a análise legislativa sobre o horizonte normativo de proteção de dados pessoais e consequente estabelecimento de efetivação deste instituto enquanto direito fundamental autônomo, especialmente através do diálogo das fontes entre LGPD e Código de Defesa do Consumidor, Marco Civil da Internet e demais legislações que compõe o microssistema de proteção de dados no Brasil, composto também por resoluções, decretos, instruções e portarias.

Por fim, na parte final da seção, tem por finalidade apontar o estágio de aplicação da tutela de dados pessoais no âmbito do Supremo Tribunal Federal, apresentando os resultados empíricos e ampliação da efetivação dos dados pessoais como direito fundamental.

Por tudo, percebe-se que o objetivo é realizar um estudo de caráter científico, que supere a mera dogmática jurídica, buscando sedimentação teórica e empírica para a problemática apresentada.

Por fim, o aludido estudo tem por intuito sistematizar e apresentar os resultados empíricos e sugestões analíticas de aprimoramento da tutela dos dados pessoais enquanto direito fundamental, através da discussão dos resultados, com apresentação proposições teóricas e analíticas acerca do objeto de pesquisa, em especial, à efetivação dos dados pessoais agora na condição expressa de direito autônomo fundamental na órbita constitucional, sob o vértice de retaguarda e proteção aos direitos personalíssimos.

2. O PANOPTISMO DIGITAL E A INAUGURAÇÃO DA DENOMINADA *DATA-DRIVEN SOCIETY AND ECONOMY*

É incontestável que o mundo mudou. Desde a primeira revolução industrial, a agricultura foi mecanizada, as metrópoles surgiram e os deslocamentos ficaram mais rápidos. Porém, conclui-se que na terceira revolução com maior intensidade, efeitos precursores trouxeram maior dinamismo à vida em sociedade por meio da criação de multimeios como fax, computador, engenharia genética, dentre outros avanços técnico-científicos, e neste ponto se destaca a criação e disseminação da internet e suas confluências para prática de dados.

No primeiro momento, a difusão da internet fez-se sob a ótica da ideologia liberal, herdada da época industrial. Posteriormente, pós década de 70, as transformações na organização da produção foram acompanhadas por representações sociais. Correspondia, dessa forma, uma economia do conhecimento e do saber, inclusive, marcada pela passagem da produção de bens para a prestação de serviços.[12]

No mesmo período, o mercado passava por uma transformação estrutural. Neste momento, emerge a chamada terceira fase do capitalismo, onde consumo se torna-se a própria forma de consolo e funciona como agente de experiências emocionais que valem por si mesmas. Não se trata apenas de vender serviços, mas experiências, ligadas ao inesperado, capazes de causar emoções, afetos, sensações (economia de experiência) e de forma íntima. Instaurando-se, aqui, o consumo hedonista, de lazer e da economia da experiência.[13] Tal fase está em constante intensificação, atrelada à personificação exacerbada dos bens de consumo, influenciada pelo avanço tecnológico diante do acesso à informação ocorrido nas décadas seguintes.

A partir das décadas de 80 e 90, a rede (internet) foi apropriada por diversos grupos e indivíduos com diferentes objetivos. Com a passagem dessa tecnologia do controle militar para o domínio civil da internet, a sociedade da informação materializou-se em supervias (da informação). Paralelamente a esse processo, pode-se notar o surgimento de outra mídia, baseada na gratuidade e na troca: a arquitetura aberta e participação ativa dos usuários, de modo que cada um torna-se o ser produtor e consumidor das informações.[14]

Tal aprimoramento da rede foi essencial para restruturação do sistema capitalista. A partir desse período, o desenvolvimento e a manifestação da revolução tecnológica foram moldados pela lógica dos interesses do capitalismo informacional:

---

[12] LOVELUCK, Benjamin. Redes, Liberdade e Controle: Uma genealogia política da internet. Petrópolis: Ed. Vozes, 2015.

[13] LIPOVESTKY, Gilles. A felicidade paradoxal: Ensaio sobre a sociedade do hiperconsumo. Tradução Maria Lucia Machado. São Paulo: Companhia das Letras, 2007.

[14] LOVELUCK, Benjamin. Redes, Liberdade e Controle: Uma genealogia política da internet. Petrópolis: Ed. Vozes, 2015.

> Uma série de reformas, tanto no âmbito das instituições, como no gerenciamento empresarial, visavam quatro objetivos principais: aprofundar a lógica capitalista de busca do lucro nas relações capital/trabalho, aumentar a produtividade do trabalho e do capital; globalizar a produção, circulação de mercados, aproveitando as condições mais vantajosas para a realização de lucros em todos os lugares; e direcionar o apoio estatal para ganhos de produtividade e competitividade das economias nacionais frequentemente em detrimento da proteção social e das normas de interesse público. A inovação tecnológica e a transformação organizacional com enfoque na flexibilidade e na adaptabilidade foram absolutamente cruciais para garantir a velocidade e a eficiência de reestruturação. Pode-se afirmar que, sem a nova tecnologia da informação, o capitalismo global teria uma realidade limitada: gerenciamento flexível teria sido limitado à redução de pessoal, e a nova rodada de gastos, tanto de bens de capital quanto de novos produtos para consumo, não teria sido suficiente para compensar a redução de gastos públicos. Portanto, o informacionalismo está ligado à expansão e ao revejunescimento do capitalismo.[15]

Deste modo, as reduções de custos operacionais nas transações, em compasso a possibilidade de identificação dos seus agentes, atingiram o consumidor possibilitando rapidamente a concepção de que a internet é um mercado desmaterializado e, por isso, ideal pela existência de atritos. Evocou, então, o surgimento da "nova Economia": A economia de rede, "baseada em uma abolição da distância e feita de preços reduzidos, de ofertas mais diversificadas e personalizadas"[16], sendo a riqueza dependente da inovação perpétua.

Assim, a revolução tecnológia reestruturou a própria noção de mercado por ter como principal base a informação. A excessiva produção em massa foi substituída pela realização de serviços mais individualizados e direcionados através da rede. Se Deus não morreu e se tornou o próprio dinheiro,[17] sem dúvida nenhuma, pode-se afirmar que exercício do poder está também no capitalismo informacional, tendo como principal vetor da sociedade da informação, cujo motor é o *Big data.*

Para Zuboff, o capitalismo da informação está caracterizado pela centralidade das informações como matéria-prima mercadológica. Tais informações são obtidas do *Big data* para constante vigilância e monitoramento individual.[18] Para a autora, o capitalismo

---

[15] CASTELLS, Manuel. A era da informação: economia, sociedade e cultura. Vol 1. A sociedade em rede. Trad: Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999, p. 36-37.

[16] LOVELUCKY, Idem, Ibidem, pg. 8.

[17] AGAMBEN, Giorgio. Homo Sacer: O poder soberano e a vida nua. 1 2 ed. Belo Horizonte: UFMG, 2007.

[18] ZUBOFF, Shoshana. Big Other: Capitalismo de vigilância e perspectivas para uma civilização de informação. In. BRUNO, Fernanda. CARDOSO, Bruno. KANASHIRO, Marta. GUILHON, Luciana. MELGAÇO, Lucas (orgs.). Tecnopolíticas de vigilância: Perspectivas da margem. São Paulo, boitempo, 2018.

informativo tornou-se o capitalismo de vigilância pelos contínuos modelos de controle através de sistema de tecnologia da informação. Os dados têm essencial importância nesse contexto por serem fonte de abastecimento do *big data*, derivados de transações econômicas, fluxos mediados por computadores, banco de dados governamentais, corporativos e câmeras de vigilância públicas[19] e privadas[20] para construção de perfis detalhados, com finalidade ideológica ou mercadológica. A subjetividade é convertida em objeto e a liberdade em navegar na internet está em constante necessidade de reformulação face da invasão de privacidade e, consequente, modulação comportamental. A previsibilidade do exercício da vontade dá lugar ao vazio da servidão voluntária eterna.

Para Bauman e Lyon, esse processo de vigilância e controle realizados no ciberespaço trata-se da vigência do modelo pós-panóptico[21]. De forma que, em aumentando o acesso aos dados pessoais, maior será o poder daquele que os detém diante daqueles que os expõem. A inviabilidade do anonimato em razão própria condição de confissão e servidão voluntária da sociedade atual é uma consequência dos próprios serviços realizados na internet e nas mídias sociais. O indivíduo, consequentemente, tem papel ativo na sua própria vigilância uma vez que a negativa aos ditames da sociedade confessional é a própria morte social pela exclusão[22], bem como pela própria necessidade do *homo economicus* transformar a sua exposição em capital humano. Quando observa tal modelo em confronto com a disposição e acesso de dados pessoais na rede, é nítido que o próprio conceito de controle, disciplina e poder caminham para uma nova designação, face da constante vigilância, onde os algoritmos mostrarão aqueles que devem

[19] O atual cenário de combate à pandemia intensificou o uso dos dados pessoais em nível mundial. Estados asiáticos como o Japão, Coreia, China, Hong Kong, Taiwan e Singapura têm apostado no *Big data*. Na China, por exemplo, a busca por possíveis infectados baseando-se somente em dados técnicos averiguam os que são potenciais infectados e que precisam ser observados e isolados, inclusive através vigilância por câmeras públicas (HAN. 2020).

[20] O *google* já foi condenado pela invasão de privacidade pela utilização da tecnologia street view, como a publicação da imagem pessoal sem qualquer tipo de ferramenta de despersonalização. Ver em https://www.tecmundo.com.br/google/82898-google-condenada-indenizar-homem-apareceu-street view.htm. Nos Estados Unidos, o *google* foi processado em razão dos veículos usados pelo Google para seu serviço de mapeamento topográfico **Street View foi acusado de capturar** senhas e outras informações de redes **Wi-Fi** domésticas desprotegidas nos lugares por onde passavam a violação ficou conhecida como "Wi-Spy". Ver https://oglobo.globo.com/economia/google-propoe-pagar-us-13-milhoes-para-encerrar-processo-de-violacao-de-privacidade-do-street-view-23822964.

[21] Importante elucidar que Bauman (1999) entende que o sinóptico é uma variação do modelo pós-panóptico que opera através da vigilância em rede pela disposição e acesso de dados pessoais.

[22] Para Enriquez (2004, p. 49, tradução livre), “desde que não nos esqueçamos de que o que antes era invisível à cota de intimidade, a vida interior de cada um – agora deve ser obrigatoriamente exposto no público (sobretudo nas telas de TC, mas também no palco literário), devemos entender que aqueles que prezam sua invisibilidade tendem a ser rejeitados, postos de lado ou transformados em suspeitos de um crime; A nudez física, social e psicológica está na ordem do dia”.

ser confinados, reorientados e excluídos pela sua discriminação racional logarítmica.[23]

A influência é exercida pela vigilância e controle através do conhecimento de informações subjetivas filtradas pelos mecanismos de tratamento de dados pessoais que, por seu turno, moldam a realidade para cada um. É a modulação comportamental subjetiva pelo exercício coletivo de poder das redes virtuais:

> O cordão umbilical digital que liga as partes em uma relação imaterial é explorado para atualizar os serviços e produtos fornecidos com saída frequente e é customizado graças à aquisição e conhecimento de dados. Essa personalização vai além do indivíduo, colocando novas questões para a disponibilidade de dados como ativo competitivo (QUINTARELLI, 2016, p. 4).

A autoridade é estabelecida pela técnica, o que configura uma nova dimensão material do poder, "em que sistemas impessoais de disciplina e controle produzem certo conhecimento do comportamento humano independentemente do consentimento"[24]. Trata-se de uma nova arquitetura universal – chamada de Big *Other*, pela reconfiguração da estrutura de poder uma vez que ele não é mais resumido ao exercício totalitário e centralizado, conforme o modelo instruído por Betham e redesenhado na sociedade disciplinar por Foucault, mas descentralizado, continuo e sem rotas de fuga em conformidade com interesses financeiros e ideológicos que invadem a vida privada. Neste sentido, o capitalismo de vigilância exige uma nova forma de influência que solapta o contrato e o Estado de Direito, suplantada pelas punições e premiações de uma mão invisível:

> O capitalismo de vigilância, portanto, se qualifica como uma nova lógica de acumulação, com uma nova política e relações sociais que substituem os contratos, o estado de direito e a confiança social pela soberania do *big other*. Ele impõe um regime de conformidade baseada em recompensas e punições e administrado privadamente, sustentando por ums redistribuição unilateral de direitos. O *big other* existe na ausência de uma autoridade legítima e é em grande parte livre de detecção ou de sanções. Neste sentido, o big other pode ser descrito como um golpe automatizado de cima: não um *coup d'état*, mas sim um *coup des gens*.[25]

A publicidade desempenha um papel essencial no capitalismo ao promover o incentivo

[23] BAUMAN; LYON. Idem, Ibidem, pg. 42.
[24] Idem, Ibidem, pg. 32.
[25] ZUBOFF, Shoshana. Big Other: Capitalismo de vigilância e perspectivas para uma civilização de informação. In. BRUNO, Fernanda. CARDOSO, Bruno. KANASHIRO, Marta. GUILHON, Luciana. MELGAÇO, Lucas (orgs.). Tecnopolíticas de vigilância: Perspectivas da margem. São Paulo, boitempo, 2018, p. 49.

ao consumo através da prescrição de estilos de vida. O acesso, tratamento e disposição de dados pessoais exacerbaram a função da publicidade ao, através de testes estatísticos, identificar quais estratégias influênciam mais no comportamento de cada consumidor especificamente.

O mundo da propaganda e do *marketing* resume-se a contar a história e mensagem certa. O *big data*, como uma crescente produção de dados em um suporte digital, constituído pelo volume, velocidade, variedade, valor e veracidade[26], possibilitam a modulação de dados e o direcionamento publicitário ao público alvo específico, o que repercute favoravelmente ao sucesso daquela mensagem e gerará redução dos custos e aumento dos lucros pela provável venda do produto indicado.[27]

Como exemplo, pode-se citar a Target. Aproximadamente há 18 atrás, ela modificou o perfil da publicidade para torná-las mais subjetivas. Por isso, a empresa buscou analistas de números para criar programas para armazenar e cruzar os dados dos consumidores, a fim de atribuir um código de identificação, para possibilitar a publicidade personalizada, através de envios de cupons e anúncios direcionados, conforme as suas necessidades, gostos e preferências. A Target conseguia identificar as futuras mamães pela previsibilidade nas compras, como grandes quantidades de loção sem perfumes, estoque de vitaminas, desinfetantes para mãos, grande quantidade de toalhas de mãos, etc. Eram mais de 25 itens específicos para categorizar essa consumidora e, assim, enviar catálogos específicos com promoções e indicações desses produtos e serviços[28]. No mesmo sentido, *MCDonald´s*, CBS, *Mazda* e *Microsoft* monitoravam e traçavam perfis de hábitos para direcionar a publicidade, sendo que, em 2011, foram processadas pelo Estado de New York por invasão de privacidade.[29]

Assim, a revolução tecnológica, como sua maior característica, trouxe a redução das

---

[26] O *Big data* é um termo mais generalizado, abrangente, sistêmico e contínuo, caracterizado pelo volume de dados disponíveis, a velocidade em que esses dados são produzidos, as fontes de coleta, a correspondência com a informação atualizada e a definição da abordagem que será feita da massa coletadas. Ver MITSUICHI, Lucas. Big data: conheça os 5 V's e sua aplicação prática para PMEs. **SEMrush** 2017. Disponível em https://pt.semrush.com/blog/big-data-conheca-os-5-vs-e-sua-aplicacao-pratica-para-pmes/ Acesso 07 maio 2020. Para Zuboff (2018), o *big data* não pode ser compeeendido apenas como uma técnica de processamento de dados, mas um conceito generalista e aberto que precisa considerar, inclusive, implicâncias sociais.

[27] AKERLOF, George A. SHILLER, Robert J. Pescando Tolos: A Economia da Manipulação e fraude. Rio de Janeiro: Alta Books, 2016.

[28] Inclusive, na Target, o seu analista de dados criou um modelo de previsão de gravidez e, com base nesse sistema, era enviado um catálogo específico com cupons para parabenizar a futura mãe. Um senhor, após receber tais anúncios e cupons para roupas de bebês e berço em casa, foi diretamente na loja da Target em Minnesota para reclamar, destacando que aquele ato poderia ser interpretado como um incentivo a gravidez para sua filha menor de idade. Dias depois, o gerente ligou ao cliente para pedir desculpas e recebeu a seguinte informação: "Tive uma conversa com minha filha, ele disse. Pelo jeito, estão acontecendo coisas nesta casa das quais eu não estava totalmente ciente. Ele respirou fundo. Ela vai ter o filho em agosto. Eu lhe devo um pedido de desculpas" (DUHIGG, 2012, p. 209).

[29] DUHIGG, Charles. O poder do hábito: por que fazemos o que fazemos na vida e nos negócios. Tradução Rafael Mantovani. Rio de Janeiro: Objetiva, 2012.

incertezas mercadológicas ao criar bolhas de filtros através do *big data* as predileções dos consumidores através de seus dados, conforme abordado na obra "Nudge"[30] que delineia a lógica de uma arquitetura de escolhas, onde não existe design neutro e que pessoas não fazem escolhas num ambiente de informações completas, capacidade cognitiva ilimitada e autocontrole pleno. Tais informações essenciais para operar mercados individualizados são de difícil definição de valor, mas facilmente capturadas do cidadão-consumidor na utilização da web, sendo o rastreamento comportamental, o que permite a programação de sofisticadas técnicas de publicidade.

Destaca-se que dado e informação não são sinônimos, apesar de serem utilizados como se fossem. Os dados são conhecimentos brutos que podem ser refinados e revertidos em informações objetivas, através da data *business*[31], que podem se referir a uma pessoa identificada ou abstrata, o que caracteriza os ditos dados pessoais e (pseudo)anonimizados[32], respectivamente. Dão origem a um sistema informativo que possibilita conhecer e prever comportamentos ao "uso generalizado de técnicas psicométricas que permitem oferecer às pessoas produtos e serviços especificamente voltados a elas no momento em que os algoritmos detectam que elas estão mais propensas a adquirir o que lhes é oferecido".[33]

A influência, portanto, opera-se pelos valores de forma contínua, em diferentes níveis e perpassa em todo tempo, realizado pela obtenção de informações individuais em rede coletiva. Segue a lógica do conhecimento, através do controle e da vigilância, para intervenção através de sugestões e direcionamento comportamental, como, por exemplo, através da publicidade. Estar-se-ia, então, em um novo modelo de governabilidade neoliberal cujo mecanismo de produção de subjetividade está centrado na economia de dados? Reflexões que serão melhores abordadas nos capítulos posteriores.

---

[30] SUNSTEIN, Cass R.; THALER, Richard H. Nudge: Improving decisions about Health, Wealth and Happiness. USA: Penguim Books, 2008.

[32] Dados anonimizados não apresentam quaisquer identificações subjetivas. No entanto, a doutrina discute a necessidade dos controladores e operadores de dados informarem todo o processo de anonimização e seus riscos para análise da possibilidade de instauração da engenharia reversa através de critérios objetivos e subjetivos e, consequentemente, a reidentificar o sujeito (BIONI, 2020b). Tal discussão foi ampliada com a utilização de dados anonimizados por empresas de telefonia, solicitada pelos governos estaduais, para análise de fluxo durante a pandemia do covid19, principalmente no que diz respeito a reversão de informações anonimizadas e seu tratamento pós pandemia. Em 25.04.2020, a Ministra Rosa Weber, na concessão de liminar por meio da Ação Direta de Inconstitucionalidade (ADI) 6390, para suspender a **Medida Provisória (MP) 954/2020**, cujo teor permitia que empresas de telefonia repassem dados de clientes pessoa física e jurídica, como nome, endereço e telefone, ao IBGE. Tal liminar foi confirmada pela corte do STF em 06 e 07 de maio. No entanto, no que diz respeito à transparência do processo de anonimização para análise de movimentação através dos dados, não há ainda nenhuma decisão ao seu respeito.

[33] ABRAMOVAY, Ricardo. ZANATTA, Rafael Augusto Ferreira. Dados Pessoais Abertos: Pilares dos Novos Mercados Digitais? RDU, Porto Alegre, Volume 16, n. 90, nov-dez, 2019, p. 161.

2.1. A tutela da privacidade e proteção de dados no cenário internacional

Muito embora existam diversas formas de se regulamentar a privacidade, como por meio de previsões constitucionais, *privacy torts*, mecanismos contratuais determinados legalmente, nos últimos 30 anos, as leis gerais de proteção de dados pessoais se firmaram como umas das formas mais eficazes de se proteger a privacidade nos países desenvolvidos.[34]

A abrangência dessas normas e o seu âmbito de aplicação variam de país para país, conforme o seu próprio processo político. É possível, no entanto, observar semelhanças e tendências. Como visto, embora o início das legislações de proteção de dados pessoais tenha ocorrido em razão do temor do poder de processamento de dados pelo Estado, logo se viu que o perigo também residia no setor privado.

Desse modo, a Diretiva Europeia de 1995 orientou os países a promulgarem leis abrangentes que compreendessem tanto o setor público, quanto o setor privado. Esse movimento acabou por influenciar países como Canadá e Austrália, que buscaram, cada um dentro de sua estrutura federativa, abarcar de mesmo modo a regulamentação do setor privado.[35]

Fora dessa tendência estão apenas os Estados Unidos, que possuem uma regulação abrangente somente para o setor público, não regulamentando o tratamento de dados realizado pelo setor privado. É o que afirma Colin Bennett:

> Os Estados Unidos são agora o único país industrial avançado que ainda não aprovou, nem está em processo de aprovar, uma lei de proteção de dados que abranja também as atividades do setor privado. Embora o *Privacy Act* de 1974 seja um exemplo desse tipo de legislação, ele é aplicado apenas ao governo federal e sua implementação tem sido muito limitada. No âmbito do poder executivo federal, o Departamento de Administração e Orçamento é tido como o supervisor da aplicação da referida lei pelas agências e órgãos do governo. No entanto, não é uma autoridade "empenhada", em contraste com as agências de proteção à privacidade de outros países, e o seu impacto tem sido tanto esporádico, como brando. Nos Estados Unidos, a adoção de legislação geral para o setor privado tem sido fortemente resistida, e embora existam diversas normas setoriais, a privacidade é protegida de

[34] Idem, Ibidem, p. 126.
[35] Idem, Ibidem, p. 130.

> uma forma bastante incompleta.[36]

Como visto, percebe-se que o sistema americano de proteção de dados pessoais deixa a desejar, se comparado ao modelo abrangente europeu e que vem sendo, aos poucos, adotado por outros países. Com relação à coexistência de normas setoriais com uma norma geral de proteção à privacidade, essa possibilidade é reconhecida pela Diretiva Europeia de 1995, desde que a normas setoriais tenham como finalidade regular setores específicos de forma a complementar a regulação realizada pela lei geral.

A latência do modelo de lei geral reside no fato de que ela constrói uma arquitetura regulatória, capaz de fazer emergir a temática da proteção de dados pessoais enquanto verdadeiro setor de políticas públicas, composto por instrumentos estatutários, sancionatórios, bem como por um órgão administrativo, responsável pela implementação e aplicação da legislação. As leis gerais de proteção de dados pessoais constituíram o meio pelo qual a maioria dos países internalizou em seus ordenamentos jurídicos os princípios consagrados em instrumentos internacionais *(Fair Information Principies).* Assim, o regime legal de proteção de dados foi o instrumento adequado encontrado para atribuir direitos subjetivos aos titulares dos dados pessoais, em mesma medida para impor limitações e obrigações aos responsáveis pelo tratamento de dados.

Ademais, o regime legal de proteção de dados, na maioria dos países, estabeleceu uma autoridade administrativa competente para fazer cumprir a legislação. A experiência das últimas décadas dos órgãos administrativos de proteção de dados pessoais demonstrou que a existência desses órgãos é vital para a implantação da legislação e do ambiente de privacidade na sociedade:

> A coexistência de autoridades supervisora robusta tem sido considerada como condição *sine qua non* para a adequada proteção à privacidade, uma vez que as leis não são vistas como auto implementáveis e que a cultura da privacidade não pode se estabelecer sem uma autoridade que a patrocine.[37]

---

[36] Idem, Ibidem, p. 131 (tradução livre).
[37] Idem, Ibidem, p. 134 (tradução livre).

Variadas são as funções exercidas pelos órgãos administrativos criados para implementar a política de proteção de dados pessoais nos diversos países. É possível, no entanto, apontar as principais funções por eles exercidas, quais sejam, de ouvidores *(ombudsman)*, auditores, consultores, educadores, orientadores de política pública, negociadores, bem como de responsáveis pela implementação e cumprimento da legislação.

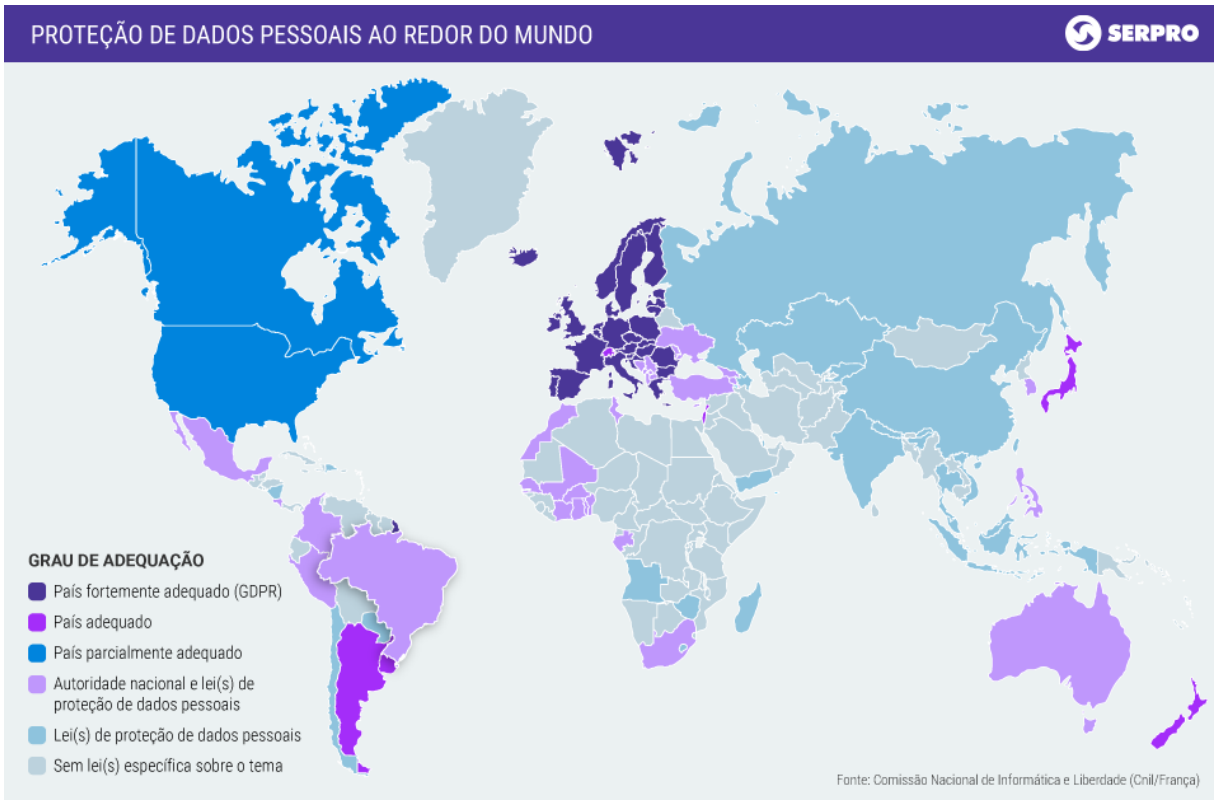


Figura 1 - SERPRO – Adaptado CNIL, França, Dez. 2019.

O mapa acima retrata o panorama global de implementação de legislações no que tange aos dados de titulares em todo globo, e que expõe a difícil tarefa de se implementar um *standard* global que delimite as finalidades para coleta, armazenamento e tratamento de dados. Nos últimos 47 anos, desde 1973, os países em todo o mundo promulgaram novas leis de privacidade de dados a uma taxa média de 3,3 novos países por ano, totalizando 156 apuradas até Dez/2020, conforme relatório elaborado abaixo:

Tabela de Leis por ano (1973-2020)[38]		
Ano	**n°**	**Jurisdição**
1973	1	Suécia
1974	1	Estados Unidos
1975	0	-
1976	0	-
1977	1	Alemanha
1978	4	França; Áustria; Dinamarca;
1979	2	Groenlândia; Luxemburgo
1980	0	-
1981	1	Israel
1982	0	-
1983	2	Canadá; San Marino
1984	1	Reino Unido
1985	0	-
1986	2	Guernsey; Ilha de Man
1987	2	Finlândia; Jersey
1988	3	Austrália; Irlanda; Países Baixos
1989	1	Islândia
1990	1	Eslovênia
1991	1	Portugal
1992	6	Bélgica; República Checa; Hungria; Eslováquia; Espanha; Suíça
1993	2	Mônaco; Nova Zelândia
1994	1	Coreia do Sul
1995	3	RAE de Hong Kong; Taiwan; Japão
1996	2	Itália; Lituânia
1997	3	Grécia; Polônia; Tailândia
1998	1	Azerbaijão
1999	2	Albânia; Chile
2000	2	Argentina; Letônia
2001	6	Cabo Verde; Chade; Chipre; Malta; Romênia, Bósnia e Herzegovina
2002	5	Armênia; Bulgária; Liechtenstein; Paraguai; Zimbábue
2003	6	Andorra; Bahamas; Croácia; Estônia; Seychelles; Vincent &
2004	4	Burkina Faso; Gibraltar; Ilhas Maurício; Tunísia
2005	2	Macedônia (FYROM); Qatar FC
2006	2	Macau; Rússia
2007	3	Dubai; Moldávia; Nepal
2008	6	Colômbia; República do Quirguistão; Montenegro; Senegal; Sérvia; Uruguai
2009	2	Benin; Marrocos
2010	8	Ilhas do BES; Curaçao; Ilhas Faroé; Kosovo; Malásia; México; Ilha de São Martinho; Vietnã

[38] GOOGLE DRIVE. Acervo Particular: Relatório de Normativos Globais sobre Proteção de Dados Pessoais até 05/2021. Disponível em: https://drive.google.com/file/d/1HsTzW2RhebMs-a6gKCSZdK-YtKXHh55B/view?usp=sharing. Acesso em: 6 mai. 2021.

2011	10	Angola; Aruba; Costa Rica; Gabão; Índia; Lesoto; Peru; Santa Lúcia; Trinidad e Tobago; Ucrânia
2012	6	Geórgia; Gana; Nicarágua; Filipinas; Cingapura; Iémen
2013	6	Antígua e Barbuda; Costa do Marfim; República Dominicana; Cazaquistão; Mali; África do Sul
2014	0	-
2015	2	Abu Dhabi; Madagáscar
2016	7	Peru; Bermudas; Equatorial Guiné; Catar; São Tomé e Príncipe; Indonésia, Malawi
2017	4	Níger, Guiné, Cayman Ilhas, Mauritânia
2018	8	Argélia, São Cristóvão e Névis, Brasil, Bahrein, Panamá, Líbano, Butão, R.P. China
2019	15	Uganda, Nigéria, Namíbia, Panamá, Ruanda, Tailândia, Togo, Uzbequistão, Barbados, Rep. Tcheca, Equador, Gambia, Grécia,
2020	9	Zâmbia, Botsuana, Gâmbia, Hungria, Letônia, Lituânia, Coreia do Sul, Malásia, Maldivas.
Total	**156**	***Média por ano = 3,3***

O relatório mostra as leis conhecidas até dezembro de 2020. É possível que outras leis existentes se tornem conhecidas posteriormente. A coluna Ano indica a data da lei de privacidade de dados original promulgada na jurisdição, para o setor público ou privado. E a coluna "n°" apresenta a quantidade de países com legislação de dados aprovados naquele ano.

O gráfico abaixo, apresenta a evolução da implementação da privacidade de dados no mundo entre os anos de 1973 e 2020, apresentando alguns picos nos inícios da primeira,

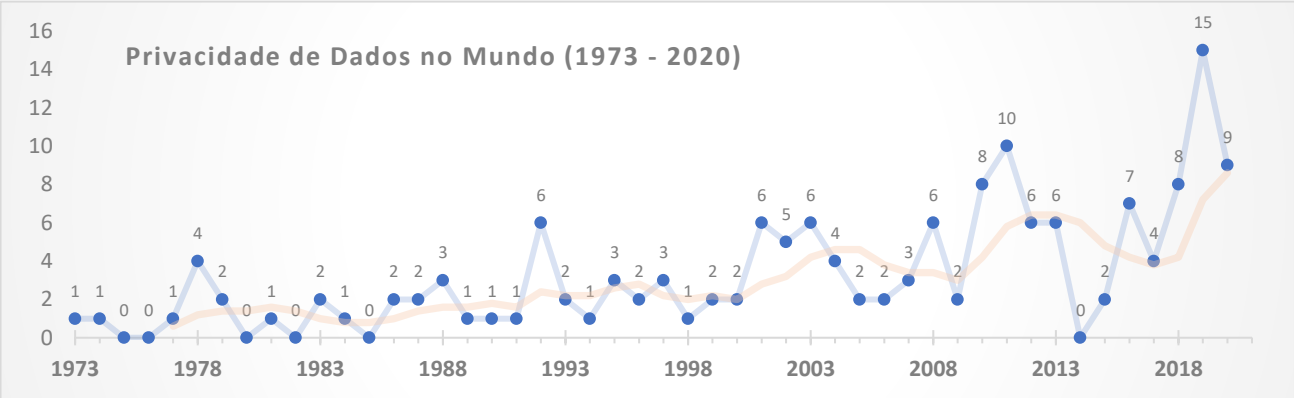


Figura 2 - Gráfico da Linha do Tempo das Leis de Privacidade de Dados entre 1973 – 2020

segunda e terceira década deste século, o que nos mostra uma tendência e regularidade de oxigenação do sistema de privacidade a cada década.

Esta lista é baseada em detalhes de 204 leis (4ª edição de abril de 2021) do Privacy Laws & Business International Report (PLBIR) e que contém o *hotsite* com indicação legislativa. Quando visto ao longo do tempo, algumas tendências históricas podem ser vistas. Até 1980, as leis de privacidade de dados eram limitadas a alguns membros da OCDE na Europa, além dos EUA. Seguindo as Diretrizes da OCDE (1980) e a Convenção 108 do Conselho da Europa (1981) até o final da década de 1980, eles foram reunidos por mais países da Europa Ocidental, além de alguns membros da OCDE fora da Europa (mas apenas para seus setores públicos) e Israel. Percebe-se, que após 1989, a dissolução do bloco de países da Europa Oriental levou a leis de privacidade de dados em toda a Europa Oriental ao longo da década de 1990, além de mais consolidação na Europa Ocidental e mais alguns países da OCDE na Ásia-Pacífico. Desde o início da década de 2000, a expansão continuou em todos esses regiões e países da América Latina e da África começaram a promulgar leis. No final da década, os países do Oriente Médio e da Ásia Central começaram a promulgar leis, e o número de leis caribenhas aumentou significativamente.

Nos últimos anos, a região com o maior crescimento em leis de privacidade de dados é a África, embora isso se deva em parte ao grande número de países na África. Ademais o gráfico mostra o número de novas leis por década e o número total de leis resultante no final de cada década. O número de novos países com leis de privacidade de dados dobrou a cada década, dos anos 1970 aos anos 2000 - 5, 10, 20, 40. Na década de 2010, o número de novas leis chegou a 66 até o final de 2019. O número de novas leis não dobrará nesta década, mas o aumento de 40 novas leis para 66 representa uma expansão contínua substancial de países com leis de privacidade de dados. Se a expansão da década de 2010 para 66 países continuar na década de 2020, haverá 200 países com leis de privacidade de dados e as leis de privacidade de dados serão onipresentes. Neste aspecto, necessário uma detida incursão na produção normativa sobre o tema e seus impactos na vida contemporânea, para avaliar as nuances de proteção de dados ao redor do mundo, e neste espectro verificar a latência de adesão à privacidade doméstica frente ao cenário global.

3. O QUE SÃO DADOS PESSOAIS E O QUE NÃO SÃO DADOS PESSOAIS

Em princípio, é necessário ponderar que alguns doutrinadores, tal como Bruno Bioni, argumentam que dados são amontoados brutos de fatos, portanto, incompreensíveis; e as

informações pessoais, por serem frutos de refinamento e processamento de dados primitivos, são inteligíveis e úteis economicamente.

Do artigo 5° da Lei Geral de Proteção de Dados Pessoais (LGPD), inciso "II", extrai-se que as informações pessoais sensíveis dos consumidores são sobre a origem étnica ou racial, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, saúde ou vida sexual, genético ou biométrico.

Ainda no âmbito dos dados pessoais, temos a incorrência dos dados melhores tutelados, que são denominados de "dados sensíveis" que segundo a doutrina de José Faleiros Júnior[39] destaca que as informações de naturezas sensíveis dos consumidores revelam características personalíssimas, bem como as opções e escolhas pessoais. Trata-se, portanto, de conteúdos frágeis que revelam aspectos íntimos e caro aos consumidores.

Referidos dados personalíssimos revelam conteúdos particulares e voláteis dos consumidores, e, portanto, devem ser resguardados de violações, discriminações e ações lesivas de terceiros. A LGPD, inclusive, destaca, conforme 6° artigo, inciso IX, que não deve haver abusividade, preconceito e finalidades ilícitas no tratamento de dados pessoais sensíveis dos destinatários finais de produtos ou serviços, sobre pena de violação ao princípio da não discriminação.

A lei de dados no Brasil, também previu a existência de dados pessoais não sensíveis, sendo relacionados aos consumidores identificados ou identificáveis. Nos termos do inciso "I", do artigo 5°, da (LGPD): "dado pessoal: informação relacionada a pessoa natural identificada ou identificável".

Referido conceito, detêm caráter mais abrangente, justamente para que não se engesse a dinâmica dos dados, que pauta-se na constante modificação das estruturas relacionais, culturais e econômicas, não podendo ter um rol exaustivo de dados dos consumidores; em contrário, pauta-se na ideia de que os dados pessoais não sensíveis são aqueles ligados aos consumidores, tendo aptidão para os identificarem.

Contudo, no âmbito da proteção de dados, temos também os dados que não se aplicam ao tratamento. São consideradores não pessoais e aqueles que não estão cobertos sobre o manto da proteção, sejam por razões de interesse público ou seja pela ausência de sua proteção.

Para inaugurar este tópico, devemos mencionar o artigo 4° da LGPD que prevê que não se aplica ao tratamento de dados pessoais, os dados que são para fins jornalísticos, acadêmicos

[39] FALEIROS JÚNIOR, José Luiz de Moura. A tutela jurídica dos dados pessoais sensíveis à luz da Lei Geral de Proteção de Dados. In: João Victor Rozatti Longhi. Estudos Essenciais de Direito Digital. Uberlândia: Laboratório Americano de Estudos Constitucionais Comparados, 2019, p. 214-215.

e artísticos: o direito constitucional à liberdade de imprensa, da arte e da ciência sobrevalece neste caso; com fins particulares: quando o tratamento de dados ocorre entre pessoas físicas com propósitos particulares; segurança pública e defesa nacional: tratamentos de dados que têm como intuito garantir a segurança e defesa nacional são isentos da LGPD. Todavia, apenas órgãos públicos, empresas públicas e empresas de economia mista se enquadram; tratamentos de dados fora do Brasil: a LGPD não se aplica a informações tratadas fora de território brasileiro. Nesses casos, as leis do outro país têm validade.

De outra perspectiva, em uma abordagem conceitual, a LGPD também retrata a qualificação clara no art. 5° de sua Lei Geral, abordando o conceito de **dados pessoais:** a informações que podem identificar uma pessoa física, como RG, nome completo e CPF; **dados pessoais sensíveis:** informações que podem ser usadas com fins discriminatórios e prejudiciais, como opção religiosa, raça, orientação sexual e posicionamento político; **dados anonimizados:** informações que deixam de identificar uma pessoa física.

A anonimização são dados relativos a uma pessoa identificada ou identificável, que não pode, razoavelmente, voltar a ser identificada ou identificável. Neste rumo, para efetividade deste conceito, necessário se faz a utilização de padrões robustos, na medida em que o processo de re-identificação seja “razoavelmente impossível”.

Diante disso, torna-se necessário destacar que os termos “dados” e “informações”, são frequentemente utilizados como sinônimos, inclusive como o foi até agora neste trabalho, pois ambas servem para determinar um fato da realidade. Entretanto, para melhor acerto metodológico, é preciso ressaltar que entre esses dois termos existem diferenças sutis que precisam ser apreciadas para melhor compreensão da temática de proteção de dados.

Em verdade, é possível dizer que o “dado” é o sistema bruto e primitivo da informação, isto é, um fato isolado, que por si só não desenvolve nenhum conhecimento, como uma espécie de “pré-informação”. Todavia, a partir do momento em que esses “dados” passam por tratamento, ou seja, são processados e devidamente organizados, tornando-se algo inteligível, se tornam verdadeiras “informações”. A informação, portanto, carrega consigo um sentido instrumental capaz de reduzir incertas e promover análises lógicas.

Em resumo, dado é qualquer informação em potencial, enquanto a informação é composta por atos ou sinais que, depois de devidamente interpretados, são dotados de sentido. Diante disso, ao se tratar de “banco de dados” é preciso compreender que há uma dinâmica de entrada (*input*) de dados, com o devido tratamento, para uma posterior saída (*output*) de informações relevantes.

Em outras palavras, o banco de dados se qualifica diante de uma lógica capaz de organizar um conjunto de informações esparsas, podendo ser administrado de maneira manual ou através da informática, em busca da produção de um conhecimento inteligível. Diante disso, a importância dos bancos de dados se torna ainda mais evidente ao destacar que as informações decorrentes de seu processamento podem ser usadas para tomadas de decisões táticas e estratégicas. Dito de outra forma, após os dados estarem devidamente estruturados e organizados, o conhecimento produzido é capaz de sustentar tomadas de decisões, como por exemplo, através da técnica denominada "mineração de dados" ou "*data mining*".

Neste ponto que o Direito apresenta a sua essencial participação, afinal, quanto mais a informação passa a ter utilidade na sociedade, em especial no mercado de consumo, maiores são as possibilidades de influir e induzir comportamentos, inclusive aqueles que expõe a pessoa ao risco ou mesmo ao dano efetivo. Atualmente, boa parte da liberdade das pessoas, principalmente quando se refere ao ambiente virtual, está submetida à estrutura de comunicação e informação.

É neste ponto que, diante das novas tecnologias da informação, esse processamento de dados, com uma determinada finalidade lógica, se tornou automatizado, havendo uma notável guinada qualitativa no que se refere à disposição de informações. É dizer que foi a tecnologia da informação que permitiu, de maneira mais precisa e efetiva, que a informação dispersa possa se transformar em informação organizada.

Em resumo, conforme expõe Bruno Bioni, o banco de dados precisa ser compreendido *"atrelado à ideia de um sistema de informação, cuja dinâmica explicita, sequencialmente, um processo que se inicia pela coleta e estruturação de dados, perpassa a extração de uma informação que, por fim, agrega conhecimento."*[40]

Antes mesmo da aprovação da lei geral sobre dados pessoais ser aprovada no Brasil, já se discutia *a priori*, se realmente há respaldo em afirmar que existam meios de garantia a anonimização de dados.

Desde do início deste século, um estudo clássico feito por Latanya Sweeney professora da Universidade de Harvard, concluiu que 87% da população americana tem características relatadas que provavelmente as tornam única com base somente em seu zip code, ou CEP.

Em estudo mais recente elaborado pelo por Yves-Alexandre de Montoye do *MIT Media Lab*, apresentou que dados sobre compras utilizando cartão de crédito, podem formar padrões únicos. De modo que, numa média de quatro transações ao dia, é suficiente para identificar de

[40] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 138.

forma exclusiva as pessoas em 90% dos casos.[41] Haja vista, que embora muitas pessoas possam comprar em um mesmo estabelecimento, somente algumas delas também comprarão em outra loja num determinado dia, e menos ainda são as chances de irem comer em uma mesma região. Num cruzamento de quatro lugares, os números alcançam 90% das vezes, há uma pessoa em toda base de dados que respondam a estas especificidades.

Os pesquisadores Ann Cavoukian e Daniel Castro ambos do *The Information Technology & Innovation Foudation* trouxerem em seu artigo *Big Data and Innovation, Setting the Record Straight: De-identification Does Work*[42] a expressão traduzida "quase identificar", que dizem respeito a variáveis que podem não identificar indivíduos diretamente, mas que têm uma correlação muito alta com identificadores únicos e ainda podem ser usados para re-identificação indireta.

Para esclarecer tais pontuações, o professor da universidade de Princeton, Arvind Narayanan, demonstra, por exemplo, os livros que determinado indivíduo leu, até mesmo as roupas disponíveis em armário,[43] embora estes elementos não sejam "quase-identificadores"[44], qualquer subconjunto de dados grande cruzados podem singularizar o indivíduo.

Outro ponto extremamente sensível acerca da privacidade na IoT "Internet das Coisas", se trata dos dados de localização, a exemplo emitido pelo GPS de smartphones e carros, por meio de um sistema conhecido como triangulação de antenas.

Sobre o tema em 2011, Jean Bolot e Hui Zang publicaram artigo traduzido denominado "A Anonimização de Dados de Localização não funcionam: Um Estudo de Medidas em Larga-escala"[45]. Neste estudo, os pesquisadores analisaram um banco de dados com mais de 30 bilhões de chamadas telefônicas realizadas por 25 milhões de celulares em todos os estados americanos, nesta hipótese, buscaram determinar até que ponto dados de geolocalização anonimizados podem revelar informações sobre pessoas que se utilizaram de determinados serviços.

---

[41] De Montjoye, Y.-A., L. Radaelli, V. K. Singh, and A. Pentland. "Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata." Science 347, no. 6221 (January 29, 2015): 536–539.

[42] Cavoukian, A. & Castro, D. Big data and innovation, setting the record straight: de-identification does work. http://www2.itif.org/2014-big-data-deidentification.pdf (2014).

[43] NARAYANAN, Arvind; BONNEU, Joseph; FELTEN, Edward; MILLER, Andrew; GOLDFEDER, Steven. Bitcoin and Criptocurrency Technologies: A Comprehensive Introduction. Artech Princeton: Princeton University Press, 2016. n.p.

[44] Idem, ibidem.

[45] Hui Zang & Jean Bolot, Anonymization of location data does not work: A large-scale measurement study, in Proc. 17th Intl. Conf. on Mobile Computing and Networking 145-156 (2011); Philippe Golle & Kurt Partridge, On the anonymity of home/work location pairs, Pervasive Computing 390-397 (2009).

O resultado desta pesquisa demonstrou que o compartilhamento de dados de geolocalização anonimizados provavelmente levará riscos a privacidade, razão pela qual os dados precisam ser minimamente menores especificados.

Ainda no mesmo cenário, em 2014 pesquisadores da SAP em conjunto com a Universidade Nacional de Singapura, Yi Son, Daniel Dahlmeier e Stephane Bressan elaboraram pesquisas acerca do "risco de re-identificação de trajetórias em dados e mobilidade humana"[46], baseados em um banco de dados com um número superior a meio milhão de indivíduos por um período de uma semana. Deste estudo, constatou-se que os indivíduos são altamente re-identificáveis com apenas alguns parâmetros de tempo-espaço. Examinando estes dados, concluíram que técnicas de anonimização podem melhorar a proteção à privacidade e redução aos riscos de re-identificação e riscos de quebra de privacidade, ainda que os dados sejam anonimizados não são capazes de fornecer o anonimato total.

Neste contexto, hoje já existem modelos que são estudados de modo a criar mecanismos para suprir estas lacunas, tanto do ponto de visto técnico, como jurídico. No cenário atual já existem modelos de re-identificação, anonimização e pseudonimização, utilizando técnicas como *K-Anonymity, L-Diversity, Differential Privacy e Data Masking.*

Por sua vez, surge a técnica capaz de elaborar o perfil de comportamento da pessoa a partir dos seus dados pessoais, técnica denominada como profiling. Com base nessa sistemática, os dados são tratados por diversos métodos, a fim de se obter uma "metainformação", ou seja, através de um conjunto de comportamentos, hábitos, preferências e desejos, traçando-se um quadro com possíveis decisões futuras. Essa técnica possibilita uma divisão de aplicações, desde casos que envolvem a segurança de um país até o envio seletivo e direcionado de publicidades somente aos potenciais consumidores.

De todas as técnicas o presente trabalho buscará brevemente pontuar de maneira mais afinada a técnica denominada *"Differential Privacy"* que apresenta os melhores resultados conforme diversos estudos de casos, pois diminui substancialmente a possibilidade de re-identificação, chegando a atingir valores raros à proteção dos dados.

A metodologia por trás da *"differential privacy*" está baseada numa lógica onde os dados são analisados a partir de um grande conjunto de dados de subamostragens, por um *hashing* que permite uma aprendizagem multidimensional, mantendo os dados individuais do usuário completamente privados, por meio de um recurso que adiciona um ruído matemático a estes dados que impossibilitam sua re-identificação. As grandes plataformas de comunicação

[46] Yi Song, Daniel Dahlmeier, and Stephane Bressan. Not so unique in the crowd:a simple and effective algorithm for anonymizing location data. ACM PIR, 2014.

como Netflix, Facebook e a Apple já adotam esta técnica com vistas a obter de maneira mais adequada os dados de seus usuários.

Fato é, que o tratamento de dados pessoais, em especial por processos de automação no manuseio dos dados, é por natureza uma atividade sensível, do ponto de vistas dos riscos iminentes. Tal possibilidade se materializa na hipótese da exposição e tratamento inadequado ou impróprio dos dados pessoais, recaindo na hipótese de tais dados não serem fidedignos ou indicarem negativamente a figura do seu titular, seja por terceiros ou sem seu prévio consentimento. A partir dessas considerações, urge a necessidade de mecanismos e órgãos capazes de decertarem, apurarem e fazerem frente à reparação dos danos, oportunizando à vítima e titular dos dados a expressão e fruição dos direitos de personalidade. Por esta razão, a tutela de dados pessoais deve ser compreendida, assim como já lhe é aplicável em diversos ordenamentos jurídicos como um expediente primordial para a tutela da pessoa humana, agora considerado um direito fundamental. [47]

3.1. Dados pessoais e tutela jurídica: conceitos e dimensões

A genese da tutela à privacidade ocorreu em momento histórico diverso de outros direitos de cunho neoconstitucional, sua origem dar-se inicialmente no contexto acadêmico, tendo sido reconhecido no âmbito legislativo apenas no Século XX.

O prefácio dos debates doutrinários sobre o direito à privacidade ocorreu pelo desenvolvimento de novas técnicas e instrumentos tecnológicos, que passaram a permitir o acesso e a divulgação de fatos relativos ao âmago particular do indivíduo de maneira anteriormente incompreensível. Tal conclusão pode ser observada no artigo sobre privacidade elaborado pelos professores Warren e Brandeis, publicado na Harvard Law Review e intitulado *"The Right to Privacy",* no qual os professores expunham as nuances técnicas de exposição de fotografias, os tablóides da época (jornais de capa amarela) e aparatos tecnológicos tinham invadido o estrito respeito à privacidade e vida íntima.

Na abordagem ede Danilo Doneda, o referido trabalho acadêmico não deve ser entendido como uma referência histórica apartada, mas sim, quando inserido num contexto histórico-cultural amplo da história norte-americana, em que a matriz de suas análises se pressupõe sob a ótica do capitalismo, naquele momento em franco desenvolvimento e a

[47] SOARES, Marcelo Negri; KAUFFMAN, M. E. ; CHAO, K. ; SAAD, M. O. . New Technologies and the Impact on Personality Rights in Brazil. PENSAR - REVISTA DE CIÊNCIAS JURÍDICAS, v. 25, p. 6, 2020.

expansão na conhecida marcha para oeste.[48]

A finalidade principal do referido artigo foi buscar identificar a perspectiva do direito à privacidade no sistema denominado *common law*, amparado por diversos precedentes jurisprudenciais de tribunais ingleses sobre o tema.

A análise inicia-se a partir da verificação de que os novos aparatos tecnológicos, como a imagem derivada da fotografia e a imprensa com *supressio* nos tablóides, estavam invadindo os círculos da vida privada, tornando públicos fatos antes privados. Com este marco de análise, o estudo daquele momento se propôs a encontrar uma proteção contra esse fato no direito da *common law*. Conforme publicado, a *common law* tem por característica e capacidade de se flexibilizar na dinâmica do tempo para ampliar os horizontes de direitos, sendo imperioso, em razão das novas invenções tecnológicas, que a *common law*, naquele recorte, respondesse como comando normativo a fim de mais uma vez no subsumir o "direito a ser deixado a só" ("*right to be let alone'*)".

Com tais considerações os pesquisadores então ao fundamentarem sua tese do direito à privacidade, inauguraram um marco temporal necessário no âmbito da proteção à inviolabilidade da personalidade, desassociando a proteção da vida privada à propriedade. Em outras palavras, "o princípio que protege documentos pessoais e outras produções personalíssimas, não contra o furto ou a apropriação física, mas contra toda forma de publicação, é na realidade não o princípio da propriedade privada, mas da inviolabilidade da personalidade."[49]

Nesse sentido, é importante ressaltar que o ineditismo do artigo consistiu, não apenas em identificar um direito à privacidade, mas em fundamentar esse direito na proteção da personalidade, em demonstrar a importância desse direito frente aos avanços da tecnologia e de tornar possível o reconhecimento futuro desse direito como um direito protegido constitucionalmente.[50]

Com estas ponderações estreiam o reconhecimento do direito à privacidade na própria vida moderna e dinâmica, que tornou o homem mais afeto à publicidade, de maneira que a intimadade ou preservação da imagem passaram a ser mais essenciais ao indivíduo.

---

[48] "Marcha para o oeste" é o nome que dado ao processo de expansão territorial que aconteceu nos Estados Unidos da América (EUA) ao longo do século XIX. Esse processo foi marcado tanto pela expansão territorial como pelo estabelecimento de colonos/habitantes nessas novas terras. Durante esse processo, os Estados Unidos deixaram de ser um território recluso ao das antigas treze colônias, alcançou as planícies centrais e estendeu-se até a costa oeste (costa do Oceano Pacífico).

[49] WARREN e BRANDEIS, *The Right to Privacy.*

[50] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* pg. 139.

Não menos relevante evidenciar que o referido estudo estabelece o direito à privacidade, buscando definir os seus liames e limítrofes, lastreados nos seguintes aspectos: a) a tutela da privacidade não exime a publicação daquilo que é público ou de interesse do público; b) amparado no direito à privacidade não é possível vedar a comunicação daquilo que, ainda que privado, é solenemente público, pois neste hipótese não há desrespeito desse direito; c) não cabe reparação se o ato de intromissão for objeto de uma revelação verbal que não cause danos; d) o consentimento afasta a ultraje do direito; e) a legalidade da informação não exclui o abuso do direito; f) a inexistência do dolo não é elemento para cacterização da transgressão.[51]

Isto posto, podemos denotar que as nuances de privacidade construídas naquele momento pelos professores Warren e Brandeis, possuem aspectos sensíveis para proteção de aspectos puramente individuais, alicerçado na perspectiva do direito de ser deixado só. Nesse sentido, que tal instituo foi preservado por longos anos, visando prevenir atos considerados negativos, afastando a figura do Estado da esfera privada do indivíduo e suas garantias.

Na obra de Danilo Doneda, encontramos o que tenha contribuído para a associação do sentido de privacidade à imagem de mundo tradicionalista, foi exatamente o contexto de seu surgimento, principalmente, no ambito judicial. Até porque, as primeiras decisões judiciais a despeito do tema de transgressão à privacidade diziam respeito a celebridades da época, como foi o caso da atriz Elisa Rachel Félix, ocorrido na França, no ano de 1858 e o caso de Mussolini, diante de sua fiel amante Clara Petacci, ocorrido na Itália no ano de 1953.[52]

A partir desta análise podemos notar que, no decorrer do século vinte, as transformações das funções do Estado, em compasso com à revolução tecnológica, contribuiram para modificação de sentido e alcance do que era concebido como direito à privacidade. Passando de um direito positivo com dimensão genuinamente particular, ao passo de ser considerado pressuposto para o reconhecimento de outros direitos fundamentais.

Neste contexto, que a violação da privacidade passou a deixar de ser um problema apenas de um círculo social privilegiado e passam abarcar e atingir a maioria dos cidadãos.

O desenvolvimento conceito de direito à privacidade prosseguiu para se flexibilizar às novas dinâmicas sociais, tracionadas pela revolução da tecnologia da informação, que possibilitou/possibilita a captura, processamento e armazenamentos dos dados pessoais de titulares de forma inaugural.

---

[51] WARREN e BRANDEIS, *The Right to Privacy*.
[52]DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* pg. 11.

Ademais adquirindo não só um caráter positivo e ao de ser reconhecido no âmbito internacional, o direito à privacidade se transformou em nuances dogmáticas e acadêmicas que espraiam e ampliam conceitos como o de proteção de dados pessoais, de modo que surgem os novos desafios ao ordenamento jurídico a partir do tratamento informatizado dos dados.[53]

Quando a tecnologia passou a possibilitar o armazenamento e o processamento acelerado de dados de natureza pessoal, deu-se a associação entre tutelas à privacidade e a manutenção das informações dos titulares. É nesse panorama, que percebemos uma alteração não apenas de conteúdo no que tange ao compromisso com a privacidade, mas também do seu léxico, inaugurando a denominação de "proteção de dados pessoais", "autodeterminação informativa", dentre entre outras variações.

É neste passo, que os ordenamentos jurídicos de diversos Estados passaram a tutelar e resguardar, não apenas a privacidade, mas expressamente os dados pessoais de seus cidadãos, diante da capacidade e compreensão de que os dados constituem uma projeção da personalidade do indivíduo, merecendo inclusive tutela constitucional, como foi o exemplo da Hungria, Rússia, Eslovênia, Portugal e Espanha.[54]

No Brasil, com advento da Emenda Constitucional de n° 115/2022, agora a proteção de dados pessoais está tutelada como cláusula pétrea, disposta no art. 5°, LXXIX, da Constituição Federal que aborda a proteção de dados pessoais, iniciando a observação do fenômeno da privacidade sob o prisma dos dados pessoais, e não da vida íntima ou privada.

3.2. Entre o direito à privacidade e à proteção de dados pessoais

Muito positivado por diversos países, o direito à privacidade ilustra variações quanto à léxica, teor e amplitude em diferentes normas. No que tange ao aspecto terminológico, este utilizado para sua designação, encontra o direito americano a expressão "*right to privacy*" e "*right to be let alone*", enquanto na literatura francesa encontramos "*droit a la vie privée*" e "*droit a la intimité*". Na doutrina italiana, utiliza-se termos como *"diritto alla riservatezza", "diritto alla segretezza"* e *"diritto alla rispetto della vita privatta",* enquanto na doutrina espanhola denomina de *"derecho a la intimidad"*, enquanto os alemães asseveram a expressão *"Recht auf informatiolelle Sebstbestimmung"* (direito à autodeterminação informacional)[55].

[53] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* pg. 27.
[54] MALTA, Tatiana. *O Direito à Privacidade na Sociedade da Informação.* pg. 44.
[55] CARVALHO, Ana Paula Gambogi. O Consumidor e o Direito à Autodeterminação informacional: considerações sobre os bancos de dados eletônicos. In: *Revista de Direito do Consumidor.* No. 46, Ano 12, abril-junho de 2003, p. 82.

Outrossim, a doutrina brasileira não estabelece terminologia consensual sobre a denominação de tal instituto, outrora a própria Constituição propiciou tamanho debate terminológico sobre o direito à privacidade, ao dispor em seu artigo 5°, X, sobre ser invioláveis a vida privada e a intimidade. Em assim sendo, a própria norma amplia sentido de cada uma das expressões: designariam "vida privada" e "intimidade", deixando como plano de fundo se tratam de institutos diferentes.

A fundamentação teórica trazida pelo Constituinte brasileiro pode ser encontrado na teoria das esferas de Heinrich Hubmann, que expõe o sentimento de privacidade do indivíduo pode ser assimilado na leitura dos círculos concêntricos, que passa a representar diferentes níveis de manifestação da privacidade: sendo o núcleo onde estaria contida a esfera da intimidade e/ou segredo, ao seu torno, encontramos a esfera privada, ao torno de ambas, um círculo de maior amplitude onde desagua a esfera pessoal que abrange a vida pública do indivíduo.

A referida teoria foi prestigiada no julgamento da "Lei do Microcenso" de 16 de julho de 1969, proferida pelo Tribunal Alemão que declarou que a mais restrita das esferas, a esfera do segredo não se poderia limitar, até mesmo por força de norma, uma vez que constituído do âmbito e aspecto inviolável da vida do indivíduo. Oportunamente o mesmo Tribunal, declarou a constitucionalidade da referida lei, por compreender que as suas previsões não acarretaram a violação da esfera do segredo. Muito embora, referida teoria posteriormente fora objeto de superação teórica pelos alemães, que posteriormente aquilatariam o conceito e diferenciação entre o direito de privacidade e intimidade.[56]

Em nossa Constituição Federal existem distinções entre "vida privada" e "intimidade", embora a carta constitucional aporte ambas terminologias.

Sob a perspectiva de que no direito toda divergência terminológica deverá se exprimir em distinção funcional, entendemos enquanto mais adequada a terminologia "privacidade"[57], que aduz a prevalência de um único direito para abranger todos os casos que se trata da proteção do indivíduo em sua esfera privada.

---

[56] BURKERT, Herbert. "Privacy-Data Protection – A German/European Perspective", in: Governance of Global Networks in the Light of Differing Local Values". Cristoph Engel; Kenneth Keller (ed.). Baden-Baden: Nomos, 2000, p. 46, apud DONEDA, Danilo, Da privacidade à proteção de dados pessoais. Op. Cit., p. 108.

[57] O vocábulo "privacidade", embora tenha raiz latina e tornou-se amplamente utilizado na língua inglesa, o que fez com que muitos autores considerassem a sua tradução para o idioma português como um anglicismo. (DONEDA. *Da privacidade à proteção de dados pessoais*, pg. 107)

Cabe-nos lembrar que no direito brasileiro, discute-se sobre os conceitos de vida privada, privacidade de dados, intimidade e sigilo, especialmente na perspectiva dos direitos da personalidade. Todos os termos, agora estão contidos no art. 5° da Constituição Federal:

> 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;
> XII - é inviolável o **sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas,** salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996)
> LXXIX - é assegurado, nos termos da lei, o **direito à proteção dos dados pessoais, inclusive nos meios digitais.** (Incluído pela Emenda Constitucional nº 115, de 2022)

Ademais, o direito à vida privada é reconhecido também no art. 21 do Código Civil: *"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".*

Dessa forma, alguns autores defendem a diferenciação entre os termos, não havendo, contudo, nenhuma uniformização doutrinária ou legislativa. Assim sendo, a intimidade poderia ser considerada no âmbito do exclusivo, referente ao que alguém reserva para si, sem qualquer tipo de repercussão social, nem sequer ao alcance de sua vida privada. Doutro turno, a vida privada, por mais isolada que possa ser, sempre se caracteriza pelo viver entre outros. Por sua vez, a proteção dos dados pessoais, relaciona-se as informações que podem indentificar determinada pessoa e sua tutela. Por sua vez, os termos segredo e sigilo são usados como sinônimos, mas de fato, embora imbricados, têm conotações um pouco diversas. Ambos traduzem aquilo que não pode ser exposto publicamente, aquilo que não pode ser comunicado. Mas o sigilo indica um dever legal, uma determinação para que o segredo seja mantido e que é conhecido como regra em várias profissões que preservam o sigilo.

Tal corrente entendimento, pode ser afinada na extrema parcialidade e distinção entre "vida privada" e "intimidade", que nos leva a prejudicialidade da conceituação do termo no Brasil. Neste estudo, ambos conceitos para melhor compreensão as expressões intimidade, vida privada, segredo ou privacidade serão consideradas sinônimos, pelas consequências jurídicas

que culminam as mesmas disposições no que tange à responsabilidade civil, embora possuam terminologias e carga conceitual diversas.

Isto posto, resta sopesar que a terminologia "privacidade" se mostra adequada também pelo fato de que possui uma amplitude léxica, quando comparada aos termos anteriormente empregados.

Grande parte da doutrina apresenta a privacidade sob a ótica das esferas concêntricas,[58] de Heinrich Hubmann, que diferencia os graus de manifestação da privacidade. Para o autor, a privacidade pode ser dividida em três círculos, a saber, i) da vida privada; ii) da intimidade; e iii) do segredo. A vida privada é composta de um grande número de relações interpessoal, contendo sigilos de âmbito patrimonial, como o bancário, por exemplo, e demais dados constitucionalmente protegidos, como os dados telefônicos.

Trata, portanto, daquelas informações restritas sobre a pessoa, com compartilhamento limitado a alguns poucos conviventes de confiança, como o próprio ambiente familiar e de amigos íntimos. Por fim, quanto ao círculo do segredo, é considerado o menor e mais oculto, necessitando, portanto, de maior tutela. Trata de informações cujo conteúdo a pessoa guarda para si, sem interesse em compartilhar, como por exemplo as opções sexuais, os traumas e as convicções religiosas.

Conforme manifestado, tal conceituação a divergência doutrinária, compreende que uma adequada definição do direito à privacidade é a prevista na obra do Professor Alan Westin, que constitui doutrina nesse tema: "*Privacidade é a reivindicação de indivíduos, grupos ou instituições para determinar, quando, como e em que extensão, informações sobre si próprios devem ser comunicadas a outros."*[59] Em mesma frente, temos outra terminologia interessante do pesquisador Rohan Samarajiva, que aborda que a "privacidade é a habilidade, explícita ou implicitamente, de negociar condições de delimitação nas relações sociais."[60] Na compreensão deste, "tal definição incluem o controle do curso de informações que podem ser estratégicas ou de valor estético para a pessoa e do contrafluxo de dados. A definição não interpreta a privacidade como um estado de solidão, conforme sugerido pelo conceito do direito a ser

[58] A teoria idealizada por Heinrich Hubmann "utiliza um esquema de esferas concêntricas para representar os diferentes graus de manifestação do sentimento de privacidade: a esfera da intimidade ou do segredo (*Intimsphäre*); a esfera privada (*Privatsphäre*) e, em torno delas, a esfera pessoal, que abrangeria a vida pública (*Öffentlichkeit*). Tal teoria, que hoje chega a ser referida pela própria doutrina alemã como a teoria da 'pessoa como uma cebola passiva', foi desenvolvida e posteriormente perdeu a sua centralidade nesta matéria […]" conforme abordado na obra de (DONEDA, 2008).

[59] WESTIN, Alan. *Privacy and Freedom.* Nova York: Atheneum, 1970, pg. 7

[60] SAMARAJIVA, Rohan. "Interactivity as though privacy mattered." In: *Technology and Privacy: the New Landscape,* pg. 283

deixado só".[61]

Podemos denotar, que mesmo diante de indeterminados conceitos prevalece a concepção e controle do indivíduo sobre os seus dados. Interpretado sobre esta ótica, a compreensão de privacidade espelha a coexistência de autonomia do titular na construção desse direito. É o mesmo que dizer que o titular do direito, possui a competência delimitar fronteiras e os limites de atuação do exercício de seu direito à privacidade.[62]

Na obra de Canotilho e Machado, respondem ao questionamento esclarecendo que tais personagens em reality renunciam ao seu direito de privacidade ao optarem por participar do entretenimento. Dado que, a conceituação de privacidade envolve necessariamente o estudo da autonomia: "o direito à privacidade consiste na possibilidade de a pessoa controlar, tanto quanto possível a massa de informações sobre si mesma a que outros podem ter acesso"[63]. Até porque, tal instituto da privacidade deve se estabelecer na proteção das decisões individuais, não o inverso atuando na tutela de determinada concepção do venha a ser este bem tutelado. Em posição diversa a este posicionamento temos, o direito à privacidade enquanto um dever de privacidade.

Tal conceituação não pode e nem deve servir para limitação de garantias e liberdades, afastando a concepção trazida por cláusulas dos bons costumes e da moral pública desejada. Inaugurando então a dignidade da pessoa humana, na qualidade de conceito amplo e não vazio, eivado da idealização dos indivíduos como sujeitos livres e responsáveis, capazes de autodeterminação.

Do caso em apreço, é possível abstrair, que no âmbito de uma sociedade pluralista que não tem por finalidade impor sua versão de mundo, o titular do conceituado direito à privacidade, possui lacunas de liberdade na interpretação e extensão do gozo de seus direitos. Ao fim e ao cabo, se tal direito à privacidade busca constituir-se no círculo do autônomo desenvolvimento de personalidade, não é adequado impedir que indivíduo de exercer livremente o direito à privacidade do qual é figura central, em uma democracia constitucional, baseada na dignidade humana e na autodeterminação do indivíduo. De forma diversa a este entendimento, corre-se a toda sorte e risco da exclusão de garantias, direitos, liberdades, hígidos na positivação constitucional. A permissibilidade do denominado direito fundamental à privacidade, tem fundamento na liberalidade do titular exercer tal direito, naquilo que melhor

---

[61] Idem, Ibidem.

[62] PINTO, Paulo Mota. "A Proteção da Vida Privada e a Constituição." In: *Boletim da Faculdade de Direito.* Vol LXXVI, Coimbra: Universidade de Coimbra, 2000, p. 190.

[63] Idem, Ibidem, pg. 55 e 56.

lhe aprouver, respeitando sua manifestação de vontade que é decorrente do próprio ideal de dignidade humana e do princípio da autodeterminação informativa, que esteiam e amoldam todos direitos fundamentais.[64] Outro aspecto não menos importante, se estabelece ao conceituarmos que a liberdade ao direito de privacidade, não o faz absoluto, à medida que se torna necessário para bom equilíbrio social a coexistência de limitações, que encontram-se amparadas em outros direitos coletivos e individuais, validamente necessários para harmonia social, ressaltados aqui somente para esclarecimento da abordagem.

De tal modo, que extrai-se que o direito à privacidade deve ser ponderado de modo a não ferir e interferir sob outros valores e fundamentos do ordenamento jurídico pátrio.

> O autônomo desenvolvimento da personalidade pressupõe, sob as modernas condições de processamento de dados, a proteção do indivíduo contra levantamento, armazenagem uso e transmissão irrestritos de seus dados pessoais. Essa proteção, portanto, é abrangida pelo direito fundamental do Art. 2, I, cumulado com Art 1, I. O direito fundamental garante o poder do cidadão de determinar em princípio ele mesmo sobre a exibição e o uso de seus dados pessoais.[65] (BVERGE 65, 1, Volkszahlung)

Na lida de tal decisão, o Tribunal Alemão naquela oportunidade declarou que a autodeterminação informativa não se consagra como direito absoluto, podendo ser restringido sobre a prevalência do manifesto interesse público.

> Esse "direito à autodeterminação sobre a informação" não é garantido ilimitadamente. O indivíduo não tem um direito no sentido de um domínio absoluto, ilimitado, sobre os seus dados; ele é muito, mas uma personalidade em desenvolvimento, dependente da comunicação, dentro da comunidade social. A informação, também quando ela é relativa à pessoa, representa um recorte da realidade social que não poder ser associado exclusivamente ao indivíduo atingido (...). Por isso, em princípio o indivíduo tem que aceitar limitações de seu direito à autodeterminação à informação em favor do interesse geral predominante. (BVERGE 65, 1, Volkszahlung)[66]

A Diretiva Europeia 95/46/CE, percebe a importância dada ao consentimento do titular

---

[64] MIRANDA, Jorge. *Perspectivas Constitucionais nos 20 anos da Constituição de 1976.* Coimbra Editora, 1996, pg. 287.

[65] MARTINS, Leonardo. Cinquenta anos de Jurisprudência do Tribunal Constitucional Federal Alemão. Montevidéu: Fundação Konrad Adenauer, 2005, pg. 238.

[66] MARTINS, Leonardo. Cinquenta anos de Jurisprudência do Tribunal Constitucional Federal Alemão. Montevidéu: Fundação Konrad Adenauer, 2005, pg. 238.

dos dados pessoais. no estabelecimento do art. 7°, que aborda que o consentimento inequívoco do titular constitui pressuposto para o processamento de dados pessoais, salvo na hipótese de previsão contratual ou legal. De outra frente, o art. 2°, c, definiu o consentimento como sendo "qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento".

Sabemos que o consentimento quando aplicado à proteção de dados pessoais, demonstra variadas dificuldades, acautelando-se aos seguintes aspectos: a) o problema da eficácia de consentimento no processamento de dados pessoais do titular, ante a hipótese do não consentimento do indivíduo resultar na sua própria exclusão do mercado de crédito e dos serviços sociais; b) a problemática de transgressão da proteção de dados pessoais, após tratamento validamente consentido pelo titular; c) o consentimento quando aplicado à tratamentos de dados considerados sensíveis.

Outra via, temos de ter em mente que eventual conduta abusiva do indivíduo que implique na revogação de consentimento, não estará isenta da iminência de reparação, na oportunidade de serem causados danos aos legítimos interesses do responsável pelo tratamento de tais dados de ordem pessoal.[67]

Ao fim, é permissivo dizer que tais pressupostos do esperado e denominado consentimento válido, no leito da proteção de dados pessoais, se reverberam a partir dos seguintes pressupostos: a) o titular dos dados que tenha interesse na manifestação do consentimento que o faça por de livre vontade; b) que tal consentimento possua a finalidade específica; c) que o titular seja devidamente notificado acerca do objeto e objetivo da coleta, de seu regular processamento, e por fim ao uso de tais dados, não obstante, rigorosamente consciente de eventuais consequências, vinculadas ao ato de não consentir com seu eventual tratamento.[68]

Destaca-se que essa teoria não está imune a críticas, em especial diante da dificuldade de diferenciar, nos casos concretos, qual valor está em risco, seja a vida privada, a intimidade ou o segredo, em razão do alto grau de subjetividade dos conceitos. Entretanto, têm-se indícios da importância de promover certos graus diferenciados de proteção, como se faz, por exemplo, com os chamados "dados sensíveis", consoante diferencia o artigo 5°, II, da LGPD.

Dessa maneira, visando melhor acerto metodológico, é preciso delinear que ao se

---

[67] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais.* pg. 381.

[68] *"Consent shall be effective only when based on the data subject's free decision. He shall be informed of the purpose of collection, processing or use and, in so far as the circumstances of the individual case dictate or at his request, of the consequences of withholding consent. (...)"*

destacar o direito fundamental à privacidade, trata-se de um valor amplo, autônomo frente a outros direitos correlatos, como a imagem e a honra, mas abrangente no que se refere aos valores de vida privada, intimidade e segredo. Dito de outra forma, para melhor compreensão do presente trabalho, destaca-se desde já que as expressões intimidade, vida privada, segredo ou privacidade serão consideradas sinônimos, pelas consequências jurídicas que culminam as mesmas disposições no que tange à responsabilidade civil, embora possuam terminologias e carga conceitual diversas.

Assim, os cidadãos adquirem o direito de exercer o controle direto sobre outras pessoas que, diante dos dados coletados, terão a ocorrência do poder de escolha. Nota-se, assim, que a autodeterminação é uma forma de defesa daqueles que têm os seus dados coletados, em uma nítida situação de vulnerabilidade, afinal, dificilmente a pessoa é capaz de compreender o sentido que a coleta de informações pode assumir para fornecedoras com organizações complexas e com tecnologias avançadas de tratamento de dados, podendo escapar até mesmo destas empresas o grau de periculosidade do uso destes dados.

Vislumbra-se assim, a emanação intimista da privacidade, como consequência do princípio da autodeterminação informativa, fato este evidenciado ao notar na Lei Geral de Proteção de Dados, em seu artigo 2°, inciso II, a garantia, ao titular dos dados, do livre desenvolvimento de sua personalidade, sendo dever do Estado propiciar, através de direitos positivos, a tutela favorável ao usuário comum, que é presumivelmente leigo.

Isso significa permitir ao usuário/internauta não apenas o direito de aquietar-se ou de não se manifestar e reservar-se à sua própria privacidade, mas também o direito de controlar o grau de sua exposição aos incessantes fluxos informacionais - que têm potencial de assolá-lo e perturbá-lo. Neste ponto, o consentimento da pessoa ganha novas concepções e, acima disso, renovada interpretação prática e jurídica.

3.2. Os princípios norteadores da proteção de dados pessoais

Implícito que tais regras de natureza procedimentalista, apresentem tal agrupamento de decisões que passaram a ser encontradas em variadas normativas sobre proteção de dados pessoais, às quais se passou a referir como *Fair Information Principles*. Esse "núcleo geral" encontra a denominação enquanto conjunto de valores e princípio que se aplicam aos dados pessoais, em especial à Convenção de Strasbourg[69] e nas linhas estabelecidas na OCDE, no

[69] Convenção n. 108 do Conselho Europeu. Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais.

início da década de 1980. É possível elaborar uma síntese destes princípios:[70]

I. *Princípio da transparência*, que aduz que a coexistência de um banco de dados de caráter pessoal deverá ser de conhecimento público e notório, pautado na necessidade de exigência prévia para seu funcionamento, ou comunicação de relatórios permanentes.
II. *Princípio da exatidão*: as informações abrigadas deverão ser fiéis, que impliquem necessariamente em sua coleta, armazenamento e tratamento para cumprimento dos parâmetros necessários de segurança da informação.
III. *Princípio da finalidade*, explicita que utilização de qualquer dado do titular deva obedecer à sua finalidade, consentida no momento da disponibilização. Neste conceito se funde a compreensão da restrição da transferência de dados pessoais à terceiros, estruturando a valoração de razoabilidade na utilização dos dados pessoais.
IV. *Princípio do livre acesso*, prevendo a ampla liberdade do titular ter acesso aos bancos de dados, pelos quais estejam vinculados, possibilitando inclusive a plena alteração, correção e remoção dos dados disponíveis.
V. *Princípio da segurança física e lógica*, implica necessariamente na segurança durante os processos de coleta, armazenamento e tratamento de dados, requerendo que sejam abrigados de incidente de perda, destruição, mutabilidade, cessão ou acesso de terceiros não consentidos.

Tais valores, ainda que diluídos, compactados ou reformularizados, formam a o eixo estruturante para diversas normas, tratados, convenções ou acordos entre privados em matéria de proteção de dados pessoais, formando a espinha dorsal de questões das quais são necessárias de serem pensadas para busca de resoluções do problema da proteção dos dados pessoais.

Para eficácia de tais princípios, no entanto, é a parte mais aparente de uma tendência rumo à constatação da autonomia da proteção de dados pessoais e à sua consideração como um direito fundamental em diversos ordenamentos. Alguns países que passaram por mudanças em seus regimes políticos, tiveram oportunidade na reelaboração de seus valores e princípios estruturantes, sendo nestes países a primeira sinalização e preocupação na proteção de dados

[70] Cf. Stefano Rodotà. *Repertorio di fine secolo*, cit. p. 62. José Adércio L. Sampaio. *Direito à intimidade e à vida privada*. cit., p. 509 ss.

pessoais. Nesse sentido, nas Constituições da Espanha[71] e de Portugal[72], se encontram dispositivos destinados a enfrentar os problemas da utilização da informática, e, no caso da Constituição portuguesa, uma referência explícita à proteção de dados pessoais.

A Convenção de Strasbourg, depois da Constituição Federal é o principal marco de uma abordagem da matéria pela chave dos direitos fundamentais. Em seu preâmbulo, a convenção deixa claro que a proteção de dados pessoais está diretamente ligada à proteção dos direitos humanos e das liberdades fundamentais, entendendo-a como pressuposto do estado democrático e trazendo para este campo a disciplina, evidenciando sua deferência ao artigo 8° da Convenção Europeia para os Direitos do Homem.[73] Posteriormente, também transparece, com clareza, presença dos direitos fundamentais na Diretiva 95/46/CE sobre proteção de dados pessoais na União Europeia. Seu artigo 1°, que trata do "objetivo da diretiva", afirma que *"Os*

[71] A Constituição Espanhola de 1978 transcreve:
Art. 18. - 4. *La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Art. 105. b) La Ley regulará el acceso de los ciudadanos a los archivios y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas*. Em tradução livre: A Lei limitará o uso da tecnologia da informação para garantir a honra e a privacidade pessoal e familiar dos cidadãos e o pleno exercício de seus direitos. Art. 105. b) A Lei regulará o acesso dos cidadãos aos arquivos e registros administrativos, salvo no que afete a segurança e defesa do Estado, a investigação de crimes e a privacidade das pessoas.

[72] I. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
II. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.
III. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosó¬ficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
IV. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.
V. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
VI. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.
VII. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosó¬ficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

[73] Tendo por teor a seguinte consideração:
1- Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
2- Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros."

Estados-membros assegurarão, em conformidade com a presente diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais."

O instrumento europeu que levou mais adiante essa sistemática foi, certamente, a Carta dos Direitos Fundamentais da União Europeia, proclamada em 7 de dezembro de 2000. Seu artigo 8°, que trata da "proteção de dados pessoais", inspira-se no artigo 8° da Convenção de Strasbourg, na Diretiva 95/46/CE e no artigo 286° do tratado instituidor da União Europeia.[74]

Não obstante, nota-se um duplo matiz: se a Diretiva, por um lado, procura proteger a pessoa física em relação ao tratamento de seus dados pessoais, por outro se destaca sua missão de induzir o comércio mediante o estabelecimento de regras comuns para proteção de dados na região, o que não surpreende se considerarmos as exigências de um mercado unificado como o europeu em diminuir de forma ampla os custos de transações, o que inclui harmonizar as regras relativas a dados pessoais.

3.3. O conceito de autodeterminação informativa e a estruturação de um direito à proteção de dados pessoais na União Europeia

Desde a Declaração Universal dos Direitos Humanos (DUDH de 1948) já se denotava uma significativa preocupação com a proteção da privacidade. Porém, foram os efeitos da denominada "economia digital" - principalmente a partir da última década do século passado - , o fator que fez salientar ainda mais, a relevância da proteção de dados pessoais. Nesse sentido, então, a União Europeia promulgou a Diretiva 45/95/CE que dispôs sobre o tratamento de dados pessoais e seus critérios para circulação, sendo que no mesmo período, diversos países criaram legislações internas sobre o tema, como foi o caso da Alemanha (ALBRECHT, 2016, pg. 89) (uma das principais inspiradoras para a privacidade de dados) e a Espanha (PINAR MANAS, 2016, pg. 16). Inclusive, no ano 2000, a Carta de Direitos Fundamentais da União Europeia prescreveu o direito à proteção da vida privada e dos dados pessoais, conforme expresso no seu

[74] De seguinte teor:
"Artigo 286°.
1. A partir de 1 de janeiro de 1999, os actos comunitários relativos à protecção das pessoas singulares em matéria de tratamento de dados de carácter pessoal e de livre circulação desses dados serão aplicáveis às instituições e órgãos instituídos pelo presente Tratado, ou com base nele.
2. Antes da data prevista no nº. 1, o Conselho, deliberando nos termos do artigo 251º., criará um órgão independente de supervisão, incumbido de fiscalizar a aplicação dos citados "actos comunitários às instituições e órgãos da Comunidade e adoptará as demais disposições que se afigurem adequadas".

artigo oitavo, contendo alguns preceitos para efetivação e, em complemento, aspectos relacionados a devida fiscalização, aqui devidamente abordada para contextualização histórica do conceito.

Nesse cenário que conjugava a proteção de direitos humanos, fundamentais e da personalidade com as decisivas influências da economia, surgiu o GDPR - Regulamento Geral de Proteção de Dados Pessoais Europeu (nº 679, aprovado em 27/04/2016, com previsão de aplicação das penalidades a partir de maio de 2018) versando sobre o tratamento e a proteção diante da livre circulação de dados das pessoas físicas. Esse fato sinalizou para os agentes econômicos que a sociedade imporia limites à liberdade de recolher, tratar e fazer circular dados pessoais e que a transparência, a lisura e a boa-fé objetiva deveriam ser atributos indispensáveis nesses processos. Aliás, refira-se que, por serem rastreáveis e auditáveis, esses processos passaram a ocasionar a possibilidade por parte principalmente da União Europeia, de impor de barreiras econômicas e mesmo de rejeição em fazer negócios com países que não viessem a implementar legislação de nível assemelhado ou com quem (basicamente, empresas) não demonstrasse licitude de condutas nessa área. E nas oportunidades em que a sensibilidade e consciência quanto a direitos relevantes não surgem ao natural, o viés econômico, por si só, pode influenciar decisivamente para gerar a motivação para o aprimoramento da legislação, principalmente em se tratando de países ainda não desenvolvidos. Nas contribuições Patrícia Peck Pinheiro (PINHEIRO, 2020, pg. 14), refere que:

Segundo o preâmbulo (2) e (13) do GDPR, o regulamento tem como objetivo: a) contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico e social, a consolidação e a convergência das economias no nível do mercado interno e para o bem-estar das pessoas físicas; b) assegurar um nível coerente de proteção das pessoas físicas no âmbito da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno; c) garantir a segurança jurídica e a transparência aos envolvidos no tratamento de dados pessoais, aos órgãos públicos e à sociedade como um todo; d) impor obrigações e responsabilidades iguais aos controladores e processadores, que assegurem um controle coerente do tratamento dos dados pessoais; e) possibilitar uma cooperação efetiva entre as autoridades de controle dos diferentes Estados-Membros.

Transparece evidente a relevância do tema e que deve ser tratado numa visão multidimensional, em razão da amplitude de suas inúmeras facetas, bem como, por ter alcance nacional e internacional. Inclusive, foi assim que essa matéria se espraiou na legislação brasileira, como se pode observar na Lei Geral de Proteção de Dados, que prevê a

autodeterminação informativa para o uso adequado no tratamento de dados no ambiente físico e virtual, conforme melhor abordado no capítulo posterior.

4. OS DADOS PESSOAIS E SUAS FORMAS DE TRATAMENTO NO AMBIENTE FÍSICO E DIGITAL E SUAS CONSEQUENCIAS PARA O DIREITO

A Lei Geral de Proteção de Dados Pessoais é aplicada, tanto para dados pessoais em material físico, quanto digitais (art. 1º, Lei 13.709/2018). A preocupação com a proteção dos dados pessoais é tamanha tramitou uma Proposta de Emenda à Constituição (PEC) – número 17/19 – que inseriu o inciso XII-A no rol do artigo 5º da Constituição Federal de 1988. Passando a prever como cláusula pétrea a proteção de dados pessoais (por meio físico e digital) passando a figurar como direito e garantia fundamental do cidadão.

Destaca-se, que até mesmo que a eliminação dos dados pessoais é considerada, pela LGPD, uma forma de tratamento de dados pessoais, de modo que a esta devem ser aplicados todos os cuidados, assim como os princípios esculpidos pelo legislador, para que não haja nenhuma afronta à norma quando da eliminação dos dados; as formas de eliminação estão previstas no artigo 16 da LGPD. Reitera-se, portanto, que a Lei Geral de Proteção de Dados Pessoais é aplicada tanto para dados pessoais em matfísicos quanto digitais (art. 1º, Lei 13.709/2018).

4.1. O tratamento de dados pessoais no âmbito público e privado

Com novos instrumentos tecnológicos, a todo momento dados pessoais são coletados, transmitidos e acessados por órgãos e entes públicos, empresas, organizações sociais, bancos e instituições financeiras, empresas de transporte público, aéreo e rodoviário, administradoras de cartão, vale alimentação, cooperativas, associações, provedores de internet, operadoras de telefonia, lojas, colégios e universidades, portarias e recepções de prédios, condomínios ou estabelecimentos de lazer.

A Lei de Proteção de Dados estabeleceu freios, limites e parâmetros de legalidade que devem ser respeitados pelas instituições quanto à captação, ao armazenamento e bom uso de dados que fazem parte da esfera dos direitos dos cidadãos, tanto por àquelas instituições, bem como também pela iniciativa privada, com o fim de evitar abusos e, havendo ilícitos, repreender, na forma da lei.

A saber pelo conteúdo jurídico conferido pela Lei n.º 13.709/2018 ao tratamento de dados pessoais, não há limites ou restrições para sua ocorrência, tampouco para a tutela

protetiva. Trata-se de conceito aberto, que abrange toda e qualquer operação realizada com dados pessoais, o que alcança, inclusive, aquelas que a tecnologia ainda não proporcionou.

Desta feita, para a tutela dos dados pessoais como garantidor dos princípios fundamentais da liberdade e da privacidade, bem como ao livre desenvolvimento da personalidade da pessoa natural, não há distinção quanto ao meio em que se desenvolve ou quanto à forma como que ocorre o tratamento. Tampouco a proteção aos dados está adstrita a determinado ramo do direito.

Assim como o tratamento de dados está presente em diversos os campos da vida, a sua proteção não se restringe a determinado ramo do direito, devendo ser observado e tutelado no sistema jurídico como um todo.

Dentre os conceitos de privacidade, liberdade e livre desenvolvimento da personalidade, se encontra a proteção de dados pessoais e o dever de informação, assumindo assim, caráter de direito fundamental autônomo, consolidado na Constituição Federal.

Portanto, qualquer atividade que utiliza dados dos cidadãos deve estar harmonizada com os princípios constitucionais, utilizando-se do princípio da proporcionalidade, razoabilidade para adequar o avanço legislativo à velocidade de modificação cibernética.

Seja qual for a especialidade em estudo, envolvendo o tratamento de dados pessoais, os operadores do direito devem sempre ter por objetivo ponderar os direitos e garantias fundamentais à liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural com os princípios norteadores da proteção de dados, qual seja, o da boa-fé, a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização e prestação de contas .

Sem a pretensão de esgotar as possíveis implicações nos diversos ramos do direito, inclusive pela celeridade dos avanços tecnológicos e a dinamicidade das relações, importante identificar que o tratamento de dados está presente nos mais diversos aspectos da vida, seja para o exercício das atribuições do Poder Público, nas relações de consumo, no vínculo empregatício, nos mais diversos negócios jurídicos da esfera privada.

Ora, a coleta e tratamento de dados pessoais tornou-se importante moeda na economia digital e meio indispensável para o desempenho de diversas atividades, inclusive estatais, gerando soluções e repercussões mais variadas, com implicações jurídicas, ainda incertas. As consequências da coleta e tratamento de dados pessoais irradia em número inimaginável de relações jurídicas, em todas as esferas do direito, cabendo-nos, a título de breve explanação, a eleição de alguns ramos e temas a mostrar a interdisciplinaridade da norma protetiva.

4.1.1. O uso de dados pessoais pelo Poder Público

A divisão administrativa do Poder Público nota a estrutura político administrativa da Constituição e facilita a gestão de inúmeros entes e órgãos que compõem a Administração Pública direta e indireta. Todos possuem bancos de dados próprios com dados pessoais dos cidadãos e informações específicas correlatas à atividade desenvolvida. A efetividade da atividade estatal tende a potencializar com o cruzamento desses dados com os de outros órgãos do mesmo ente jurídico ou de pessoa jurídica de direito público diversa, ou ainda de banco de dados privado.

A divisão político-administrativa da República Federativa do Brasil, nos termos do artigo 18 da Constituição Federal, compreende a União, os Estados, o Distrito Federal e os Municípios. Cada qual, constituído por estrutura administrativa própria, formada por órgãos, entidades e conjunto de pessoas jurídicas de direito público e relaciona-se com inúmeras outras de direito privado.

Todos, da administração pública direta ou indireta, valem-se de diversos bancos de dados pessoais de agentes públicos, contribuintes e responsáveis tributários, presos e menores submetidos à Medidas Socioeducativas, dos candidatos a cargos eletivos, dados de previdência pública ou privada, alunos e egressos do ensino público e privado e suas famílias, quando beneficiários de programas como Fundo de Financiamento Estudantil , Programa Universidade para Todos , de pessoas cadastradas no Sistema Único de Saúde ou em planos de governo e políticas públicas, como Minha Casa Minha Vida (Casa Verde e Amarela) e Lei Rouanet, dentre outros.

Torna-se evidente que a informação bruta ou manipulada por recursos tecnológicos pode valer grandes fortunas para a iniciativa privada. No entanto, também para o Estado tem grande valia. Órgãos e entidades podem atingir maior grau de eficiência ao se valer de outros bancos de dados, públicos ou privados, inclusive redes sociais.

Com certa frequência magistrados tem se valido do holerite, do Imposto de Renda da Pessoa Física ou mesmo de informações de cunho pessoal postadas pelo próprio requerente em rede social expondo padrão financeiro diverso do alegado nos autos para negar o benefício de Assistência Judiciária Gratuita, conforme a Lei 1.060, de 05 de fevereiro de 1950, e artigo 98 e seguintes do Código de Processo Civil, ou para identificar a existência de bens e restringir a disponibilidade de algum patrimônio, para dar efetividade à tutela jurisdicional.

Seguindo grande tendência da informatização do Poder Judiciário, o magistrado dispõe hoje de importantes Sistemas de Pesquisas Patrimoniais, a saber: Bacenjud, Cadastro de

Clientes do Sistema Financeiro Nacional (CCS-Bacen), Infojud, Infoseg, Renajud, Serasajud e Sistema de Registro Eletrônico de Imóveis (SREI).

Da mesma forma, a Receita Federal conta com inteligência artificial para cruzar dados de contribuintes como, por exemplo, com informações de operações financeiras controladas pelo Conselho de Atividades Financeiras ou mesmo o estilo de vida ostentada em redes sociais para analisar se o contribuinte apresenta irregularidade em suas informações.

Os Sistemas de Pesquisas Patrimoniais conferem rapidez e efetividade às tutelas que envolvam bens e valores. Da mesma forma, o banco de dados de atividades suspeitas sob controle do Conselho de Atividades Financeiras tem se mostrado muito eficaz no combate a crimes contra o sistema financeiro. No entanto, constituem efetivo tratamento de dados pessoais e por isso devem ser analisados e estarem conformes sob a égide da legislação de proteção de dados.

O Poder Público, de mesma forma a iniciativa privada, possui inúmeros bancos de dados, inclusive valendo-se do "cruzamento" das informações para analisar aspectos de saúde pública, segurança, fiscalização e tributação.

A legislação prevê as regras para o tratamento de dados pelo Poder Público, assim consideradas as pessoas jurídicas de direito público estabelecidas pela Lei de Acesso à Informação, com a restrição de que o sejam *"para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público"*.

Para os prazos e procedimentos perante o Poder Público, a legislação federal fixou que deve ser observado o disposto em legislação específica, como na Lei do Habeas Data, Lei Geral do Processo Administrativo e da Lei de Acesso à Informação.

Aplica-se a legislação de proteção, equiparando-se para fins de tratamento de dados pelas pessoas jurídicas de direito publico, os serviços notariais e de registros públicos, exercidos em caráter privado, por delegação do Poder Público, na forma do artigo 236 da Constituição Federal. Nesse sentido, estabelece a legislação que os notários e registradores deverão fornecer à administração pública, por meio eletrônico, acesso aos dados.

A manutenção de dados pelo Poder Público deverá observar formato interoperavel e estruturado para o uso compartilhado dos dados, para ultimação das políticas públicas, bem como à prestação de serviços públicos em espécie, como a descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Acerca do uso compartilhado de dados pessoais pelo Poder Público, convém destacar que devem observar as *"finalidades específicas de execução de políticas públicas e atribuição*

legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei".

O preceito legal do artigo 26 da LGPD, impõe ao Poder Público vedação de transferir à entidades privadas informações constantes das suas bases de dados, excepcionando determinadas hipóteses permissivas.[75]

Primeiramente, convém destacar que ao prever as regras de tratamento de dados pelo Poder Público, o artigo 23 da LGPD, em seu inciso II, originariamente estabelecia que *"sejam protegidos e preservados dados pessoais de requerentes de acesso à informação, nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), vedado seu compartilhamento no âmbito do Poder Público e com pessoas jurídicas de direito privado".*

No veto, constou a necessidade recorrente e essencial do compartilhamento de dados pelo poder público como medida para o exercício regular das suas atividades. Por seu turno, vetado o inciso II do § 1º do artigo 26, que trata das exceções à vedação de uso compartilhado de dados, cuja redação estabelecia hipótese permissiva *"quando houver previsão legal e a transferência for respaldada em contratos, convênios ou instrumentos congêneres".* No veto, constou, mais uma vez o presidente destacou a relevância do uso de dados pessoais, ainda que pelo uso compartilhado, para o funcionamento da máquina pública.

Neste caso, as fundamentações ao veto, trouxeran como razões, à proteção das organizações ou empresas que tem na coleta e armazenamento de dados pessoais como essenciais para sua existência e funcionamento. A exclusão da suspensão ou proibição de tratamento de dados não isenta os responsáveis pelas infrações cometidas, estando sujeitos às sanções previstas no artigo 52 da LGPD, como visto. A razão do veto tem como escopo conferir segurança jurídica, evitando que sanção de tamanha importância seja estabelecida por norma geral, sem critérios específicos, permita que haja intervenção na economia.

4.1.2. A utilização de dados pessoais em nome da segurança pública e suas implicações à tutela dos direitos difusos e individuais dos cidadãos

Vivemos atualmente um novo paradigma tecnológico e social, ante uma transformação radical marcada pela convergência de tecnologias físicas, digitais e biológicas. Na recente obra

[75] A hipótese é o tratamento para execução de políticas públicas (art. 7, III). A lei determina que a política pública apta a legitimar tratamento de dados deve ser fundamentada em lei ou instrumento bilateral (como convênios e contratos). Esse tratamento pode ser realizado por particulares, mas em regra compete ao Estado, motivo pelo qual importa analisar, neste artigo o regime específico que os artigos 23 a 30 da LGPD estabelecem para o Poder Público.

de Klaus Schwab intitulada "Quarta Revolução Industrial"[76] em que oferece subsídios para compreender e questionar a nova maré tecnológica que estamos vivenciando nos tempos atuais. A referida obra é um desdobramento do 46ª Fórum Econômico Mundial realizado em Davos no início de 2016, que discutiu a Quarta Revolução Industrial.

William Gibson, criador do termo "ciberespaço" oportunamente asseverou: "O ciberespaço, há não muito tempo atrás, era um espaço determinado, que nós visitávamos periodicamente, mergulhando nele a partir do nosso mundo físico. Hoje, o ciberespaço saltou para fora. Colonizou o físico".

Os atentados de 11 de setembro de 2001 nos EUA, mudaram a percepção de segurança, fazendo com que a sociedade enfrentasse, logo no início do século, o paradoxo entre direitos, à primeira vista conflitantes, a ampla liberdade versus a garantia de segurança.

após o referido ataque terrorista, houve diversas mudanças significativas em relação à segurança do tráfego aéreo, com mecanismos de controle intensos e não apenas nos Estados Unidos da América, mas em todo mundo.

Com o aparecimento de políticas que visavam reforçar a segurança dos aeroportos, o governo norte-americano, por meio da publicação do USA PATRIOT Act, publicado em 26 de outubro de 2001, previa diversas determinações que, em tese, violavam garantias constitucionais americanas, especialmente no que tange às questões de privacidade, com adoções de práticas que restringiam as liberdades individuais, consideradas um pilar da democracia naquele país.

As medidas de segurança desproporcionais tomada pelo governo norte-americano logo após os atentados trazem à tona, as mesmas reflexões em relação aos limites do direito à privacidade e liberdades individuais. Inquestionavelmente, as ações e estratégias traçadas como resposta imediata ao ataque terrorista eram, naquele momento, imprescindíveis para garantir a segurança e evitar a ocorrência de novos episódios. Entretanto, essas medidas não devem ultrapassar a finalidade a que se propõem, qual seja a segurança pública.

Uma pesquisa de opinião da *Princeton Survey Reaserch Associates*, feita apenas dez dias após os atentados entrevistou 1005 cidadãos estadunidenses, por telefone, com a seguinte pergunta: *"Para controlar o terrorismo no país, você acha que será necessário às pessoas comuns renunciarem a algumas de suas liberdades civis, ou não?".*

[76] SCHWAB, Klaus. A quarta revolução industrial. São Paulo: Edipro, 2016.

Em amparo aos resultados obtidos pela pesquisa, 63% dos entrevistados entendiam ser necessária uma redução de suas liberdades civis para o combate ao terrorismo.[77] Apesar do resultado da pesquisa realizada pela *Princeton Survey Reaserch Associates* ter demonstrado que a maior parte dos norte-americanos apoiava medidas no combate ao terrorismo, uma outra pesquisa de opinião, também feita por telefone, pelo *Los Angeles Times* apontou que uma parte relevante (37%) dos entrevistados estava preocupado com a eminência de limitação de suas liberdades civis.

Essas pesquisas corroboram o paradoxo entre liberdade e segurança já naquele primeiro momento de tensão entre a população daquele país. Além disso, os atentados às torres gêmeas também deram início a uma negociação muito intensa entre o governo norte-americano e a União Europeia, tendo o grupo europeu de autoridades de proteção de dados, em especial relevância para evitar que houvesse uma forte limitação das liberdades dos seus cidadãos. Isto porque, os métodos de vigilância de dados são frequentemente apresentados como uma forma eficiente de triagem de identidade, com capacidade de promover os objetivos do policiamento preventivo.

As denúncias de Edward Snowden quanto as atividades da *National Security Agency - NSA* por intermédio do programa *Prism* - programa de espionagem de coleta de informações, provocaram reações de grande relevância em nível político, com posicionamentos das presidentes da Alemanha, Ângela Merkel e do Brasil, Dilma Rousseff.[78]

O Programa *Prism*, também foi usado para interceptar e coletar metadados de todas as ligações telefônicas dos consumidores da empresa VERIZON, uma das maiores empresas americanas do ramo de telecomunicações. Por meio desse método de espionagem, era possível saber quem ligou, a hora, a duração e o local da chamada. Diversos registros de cidadãos americanos que não possuíam qualquer ligação criminal foram coletados.'[79]

Não apenas cidadãos americanos foram alvo desses registros, mas também pessoas de outras partes do mundo, que foram alvo do acesso de dados pelo Prism, que também coletava informações dos usuários de empresas como Google e Facebook.[80]

---

[77] ROPER CENTER. Princeton Survey Research Associates. Civil Liberties and Terrorism. 21 de setembro, 2001. Disponível em: <http://ropercenter.cornell.edu/CFIDE/cf/action/catalog/abstract.cfm?type=&start=&id=&archno=USPSRA2001 -NW1 1&abstract=>. Acesso em: 23 jun. 2021.

[78] CEIRI NEWS. As relações entre Alemanha e Estados Unidos, pós Snowden. Disponível em: https://ceiri.news/as-relacoes-entre-alemanha-e-estados-unidos-pos-snowden/. Acesso em: 16 fev. 2022.

[79] GREENWALD, Glenn. Sem lugar para se esconder. Rio de Janeiro: Sextante, 2014.

[80] GREENWALD, Glenn. Idem, Ibidem.

Todos esses eventos podem ser vistos como desdobramentos da vigilância constante instaurada pelo Governo dos Estados Unidos a partir dos atentados de 11 de setembro e, marcaram de forma relevante o contexto geopolítico internacional.

Claramente, diante de um cenário em que predominavam o medo e o caos constante na eminência de novos ataques, o contexto de segurança precisava ser reforçado e alterado, através da adoção de novos standards e medidas mais coercitivas. No entanto, não se deve perder de vista a preservação entre segurança e a liberdade.

A evolução do estado de vigilância não se limitou apenas ao território norte-americano, mas colocou todos as demais nações em estado de alerta. Para além da atenção a possíveis ataques terroristas, as atenções se voltavam para a segurança *lato sensu*.

Com o avanço da tecnologia, esforços foram despendidos em mecanismos de segurança e controle total de tudo e de todos. Dentre esses mecanismos, o reconhecimento facial pode ser considerado um dos avanços tecnológicos mais recentes e também um dos meios mais utilizados no controle dos indivíduos.

O Sistema *Skynet* na China é um exemplo clássico dos avanços do Estado sobre liberdade, ao conseguir mapear um determinado segmento da população por meio das suas mais de vinte milhões de câmeras espalhadas pelo país. Tal sistema chinês monitorava pedestres em tempo real e foi capaz de identificar características como idade, gênero e até mesmo as roupas, além de ser possível a identificação de veículos.

No decorrer da pandemia, o governo chinês utilizou-se da tecnologia do reconhecimento facial para checar a temperatura das pessoas e, inclusive, para controlar se as pessoas estavam,[81] de fato cumprindo a quarentena em casa, assim como averiguar a utilização de máscaras.

> Toda a infraestrutura para a vigilância digital se mostrou agora ser extremamente eficaz para conter a epidemia. Quando alguém sai da estação de Pequim é captado automaticamente por uma câmera que mede sua temperatura corporal. Se a temperatura é preocupante todas as pessoas que estavam sentadas no mesmo vagão recebem uma notificação em seus celulares. Não é por acaso que o sistema sabe quem estava sentado em qual local no trem. As redes sociais contam que estão usando até drones para controlar as quarentenas. Se alguém rompe clandestinamente a quarentena um drone se dirige voando em sua direção e ordena que regresse à sua casa. Talvez até lhe dê uma multa

[81] PRUX, Oscar Ivan. SOUSA, KEVIN. (DES)LIBERDADE VIRAL NA PANDEMIA: UMA RELEITURA DA ESCALADA POR DADOS PESSOAIS E SEUS IMPACTOS À LUZ DOS DIREITOS DA PERSONALIDADE E A PROTEÇÃO DE DADOS. Revista Newton Paiva. Disponível em: <https://revistas.newtonpaiva.br/redcunp/n-43-desliberdade-viral-na-pandemia-uma-releitura-da-escalada-por-dados-pessoais-e-seus-impactos-a-luz-dos-direitos-da-personalidade-e-a-protecao-de-dados/>. Acesso em: 18 nov. 2021, p. 49.

> e a deixe cair voando, quem sabe. Uma situação que para os europeus seria distópica, mas que, pelo visto, não tem resistência na China (HAN, 2020, s./p.)

O 'tecnonacionalismo chinês'[82] por ser considerado um país onde não há uma preocupação e sequer uma cultura em relação à preservação da privacidade, a tecnologia do reconhecimento facial já tem sido utilizada em outros países, inclusive no Brasil.

Em mesmo sentido, foram instaladas vinte e oito câmeras de reconhecimento facial em Copacabana, um sistema que era parte de um projeto piloto da Polícia Militar do Estado do Rio de Janeiro. O sistema em questão foi capaz de comparar as fotos de procurados que estavam no banco de dados da Polícia Militar com os rostos das pessoas filmadas em tempo real.

O uso do sistema gerou controvérsia na comunidade científica, que por intermédio do Idec - Instituto Brasileiro de Defesa do Consumidor, solicitou à Polícia Militar esclarecimentos acerca dos critérios de segurança dos dados coletados por meio do sistema de reconhecimento facial, justificado sob argumento da necessidade de garantia que tais dados coletados não sejam utilizados para nenhuma outra finalidade.

A carta enviada pelo Idec reconheceu a importância do uso dessa tecnologia para a segurança pública, entretanto, alertou para a necessidade do tratamento adequado das informações coletadas pela tecnologia:

> Consideramos que o desenvolvimento de novos instrumentos de Segurança Pública é prioritário e urgente, especialmente no estado do Rio de Janeiro, e deve contar com o apoio de toda a sociedade. Contudo, a eventual ausência de cuidados básicos no tratamento dessas informações, como acesso do fornecedor da tecnologia aos dados gerados, pode gerar riscos para os consumidores. Por isso, o Idec, no exercício de sua missão de defender os consumidores, deseja contribuir para que tais iniciativas sejam executadas sem sacrificar direitos de privacidade dos cidadãos, cujos dados pessoais podem ser indevidamente utilizados por terceiros para práticas de outras ilegalidades. (IDEC, 2019)

[82] A partir de uma intepretação que se convencionou denominar de tecno-nacionalista, tais políticas se organizam por meio de um eixo *top down* e se materializam em inúmeros esforços que se retroalimentam para reforçar o sistema nacional de inovação chinês em paralelo ao fortalecimento da estrutura produtiva. Grosso modo, tais diretrizes podem ser compreendidas a partir da coexistência de três grandes vetores de materialização, os quais combinam esforços de P&D, inovação, financiamento e formas de atuação do Estado de acordo com as estratégias e os atuais estágios de desenvolvimento produtivo e tecnológico da estrutura empresarial doméstica. (Zhou; Liu, 2016 e Chen; Naughton, 2016).

Na oportunidade da carta enviada pelo Idec, foram tecidos os seguintes questionamentos à Polícia Militar do Rio de Janeiro:

> Considerando que falhas e omissões de cuidado na condução desse projeto podem impactar de forma irreparável direitos difusos e individuais dos cidadãos, e diante da proximidade de sua implementação, o Instituto Brasileiro de Defesa do Consumidor se dirige respeitosamente à Secretaria da Polícia Militar do Rio de Janeiro para consultá-los sobre os cuidados e as garantias que estão sendo adotadas para evitar externalidades não previstas no funcionamento desse sistema de vigilância, e que podem evitar os graves danos mencionados:
>
> **1.** Quanto à parceria com a empresa Oi, que desenvolveu o software de reconhecimento facial utilizado. Quais os termos em que essa parceria foi firmada? O que levou à decisão final pela empresa? Houve processo de licitação em concorrência com outras empresas? Qual a contrapartida à empresa Oi, considerando que foi afirmado que a implementação da ferramenta terá "custo zero" ao governo do Estado?
>
> **2.** Quanto à segurança da ferramenta. Houve avaliação a respeito dos potenciais riscos e impacto à segurança dos cidadãos? Quais as garantias de segurança levadas à cabo pela Secretaria da Polícia Militar para evitar danos ao banco de dados, como possíveis vazamentos ou utilização inadequada das informações coletadas? O processo de escolha da tecnologia levou em consideração potenciais falhas que ela possa vir a apresentar?
>
> **3.** Quanto ao funcionamento da tecnologia. A realização do reconhecimento facial pelo software ocorre em tempo real? Há procedimentos posteriores de anonimização dos dados pessoais coletados? Há posterior descarte das informações e imagens não utilizadas pela PMERJ? Por quanto tempo as imagens seriam armazenadas? (IDEC, 2019)

A preocupação do Instituto com o tratamento adequado das informações coletadas e com a tutela da privacidade em relação ao uso de câmeras inteligentes veio antes mesmo do envio da carta à Secretaria da Polícia Militar do Rio de Janeiro. Uma notícia publicada no site do Instituto em 24 de janeiro de 2019 já alertava para possíveis problemas com o uso do sistema[83].

[83] Disponível em: https://idec.org.br/idec-na-imprensa/camera-inteligente-no-rj-tera-sistema-da-oi- multada-por-violar-privacidade

Inicialmente, a preocupação era com a terceirização do serviço à empresa de telefonia Oi, que já havia sido multada em 2014 pela criação de um software que sem o consentimento destes, vendia informações acerca de seus clientes de internet.

A TNL PCS, uma divisão da concessionária de serviços de telecomunicações Oi, foi multada em três milhões e quinhentos mil reais pelo Ministério da Justiça, através do Departamento de Proteção e Defesa do Consumidor (DPDC), por ter vendido informações de seus clientes para agências de publicidade. Segundo o DPDC, essa prática teria violado os princípios da boa-fé e da transparência. Essa foi a primeira violação comprovada da neutralidade da rede definida pelo Marco Civil da Internet[84].

O Idec também interveio na utilização de câmeras inteligentes em São Paulo, tendo entrado com uma Ação Civil Pública contra a Via Quatro, empresa concessionária do Metrô na capital paulistana. As câmeras estavam presentes3 nos monitores publicitários instalados no metrô da Linha 4-Amarela nas plataformas de embarque e desembarque e tinham por objetivo capturar as reações dos passageiros a cada anúncio publicitário que era exibido nos respectivos monitores.

A concessionária Via Quatro foi multada em 100 milhões de reais pela coleta indevida de dados. Na recente sentença da 37ª Vara Cível da Comarca do Estado de São Paulo, a juíza destacou que:

> A situação exposta no caso concreto é muito diferente da captação de imagens por sistemas de segurança com objetivo de melhoria na prestação do serviço, segurança dos usuários ou manutenção da ordem, o que seria não só aceitável, mas necessário diante da obrigação da fornecedora de serviço público zelar pela segurança de seus usuários dentro de suas dependências. É evidente que a captação da imagem ora discutida é utilizada para fins publicitários e consequente cunho comercial, já que, em linhas gerais, se busca detectar as principais características dos indivíduos que circulam em determinados locais e horários, bem como emoções e reações apresentadas à publicidade veiculada no equipamento. Ademais, restou incontroverso que os usuários não foram advertidos ou comunicados prévia ou posteriormente acerca da utilização ou captação de sua imagem pelos

[84] Disponível em: https://oglobo.globo.com/economia/defesa-do-consumidor/oi-multada-em-35-milhoes- por-invasao-de-privacidade-feita-por-velox-13348505

> totens instalado nas plataformas, ou seja, os usuários nem mesmo tem conhecimento da prática realizada pela requerida, o que viola patentemente o seu direito à informação clara e adequada sobre os produtos e serviços, bem como à proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, ambos elencados no artigo 6°, III e IV do Código de Defesa do Consumidor (TJ-SP - ACP 109066342.2018.8.26.0100, 37 Vara Cível do Foro Central Cível da Comarca de São Paulo).

A sentença considerou, portanto, que a conduta da concessionária violava o direito à imagem dos consumidores usuários do serviço público, bem como as disposições sobre a proteção especial que deveria ser dada aos dados pessoais sensíveis e, também, a violação de direitos básicos do consumidor, especificamente no tocante à informação e à proteção com relação às práticas comerciais abusivas. Cabe ressaltar que o referido processo, acima referendado, encontra-se em grau de Recurso, ainda sem decisão proferida pela 20ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo.

Todos esses casos apresentados até aqui chamam a atenção para o risco que envolve a terceirização dos serviços públicos, especialmente os de segurança pública. A terceirização desses serviços é uma preocupação que ganha ainda mais relevância quando se está diante de empresas que ofertam essa tecnologia e que já possuem algum histórico de violação à privacidade, como a utilização indevida de dados pessoais, por exemplo.

Para além do histórico dessas empresas, não é possível estabelecer ao certo um controle efetivo por parte do Estado acerca desses dados, já que o controle de toda a tecnologia - ou pelo menos boa parte desse controle - fica por conta das empresas e não do Estado.

Informações como hábitos simples do dia a dia das pessoas são muito valiosos para determinadas empresas, de modo a dar suporte a chamada publicidade direcionada, um método utilizado com muita frequência pelas empresas como *Google* e *Facebook,* que possuem um armazenamento muito significativo de dados pessoais, inclusive de caráter sensível. Segundo Eli Pariser, esses dados utilizados pela *Google* e *Facebook,* embora tenham estratégias diferentes, possuem os mesmos propósitos:

> A questão é que a base dos dois negócios é essencialmente a mesma: publicidade direcionada, altamente relevante. Os anúncios contextuais que o Google coloca ao lado dos resultados de pesquisas e em sites são sua única fonte significativa de lucro. E, embora as finanças do

> Facebook não sejam reveladas ao público, alguns *insiders* já deixaram claro que a publicidade está no âmago dos rendimentos da empresa. O Google e o Facebook tiveram pontos de partida e estratégias diferentes — um deles apoiou-se nas relações entre informações, o outro nas relações entre pessoas-, porém, em última análise, os dois competem pelos mesmos dólares advindos da publicidade. Do ponto de vista do anunciante on-line, a questão é simples: qual empresa irá gerar o maior retorno por cada dólar investido? É aí que a relevância entra na equação. As massas de dados acumuladas pelo Facebook e pelo Google têm dois propósitos: para os usuários, os dados são a chave para a oferta de notícias e resultados pessoalmente relevantes; para os anunciantes, os dados chave para encontrar possíveis compradores. A empresa que tiver a maior quantidade de informações e souber usá-las melhor ganhará os dólares da publicidade.[85]

Desse modo, observa-se o valor econômico e a relevância de mercado que esses dados pessoais possuem. Nas palavras de Marcelo Cardoso Pereira:

> O êxito dos negócios na denominada "economia digital" está pendente de que os Prestadores de Serviços da Sociedade da Informação possam apresentar produtos e serviços adequados a pessoas adequadas. Para isso, devem, esses prestadores (...), saber os gostos, preferências, hábitos, costumes, etc., de potenciais clientes que não são outros, como já dissemos, senão os usuários da Rede.[86]

Para além do campo publicitário, o vazamento dessas informações que aparentemente são simplórias pode acarretar risco à própria segurança pública. Isso porque pode ocorrer o vazamento de dados para organizações criminosas, que poderão utilizar essas informações para mapear determinados hábitos ou situações específicas para a prática de crimes.

A preocupação com a segurança sempre foi foco de atenção da maioria dos países, especialmente aqueles que são constantemente ameaçados por atentados terroristas. Com a pandemia de COVID-19, surgiu um novo inimigo. O centro das atenções passou a ser o controle e monitoramento da propagação do vírus. A tecnologia que vinha sendo constantemente utilizada para monitoramento da segurança pública passou a ser utilizada com escopo sanitário

---

[85] PARISER, Eli. O filtro invisível. O que a Internet está escondendo de você. Trad. Diego Alfaro. Rio de Janeiro: Zahar, 2012. p.41.

[86] PEREIRA, Marcelo Cardoso. Direito à intimidade na internet. 1. ed. 6. reimp. - Curitiba: Juruá, 2011.

de vigilância.

> A narrativa que justifica tais ações supõe que o bem-estar - traduzido, no momento, por controle e eliminação da covid-19 - viria com uma vigilância maior sobre as ações cotidianas dos cidadãos, garantindo-os um mínimo de bem-estar. Para tanto, seria necessário o uso de rastreadores e outros artefatos para a extração de dados de celulares, possível com parcerias estabelecidas com operadoras de telefonia. Identificar padrões de movimentos das pessoas e verificar se as pessoas estariam seguindo recomendações do governo de distanciamento social seriam algumas das atividades que justificariam tal uso. Entretanto, a maioria das ações governamentais vem sendo implementadas sem considerar questões como a estipulação de um prazo de duração da vigilância ou o tipo de proteção de privacidade que seria garantida ao cidadão durante o processo.[87]

Afim de esclarecer em exemplos dessa mudança, é o serviço de segurança *Shin Bet* em Israel, um serviço que antes era utilizado para dar suporte ao software de vigilância de combate ao extremismo, que no advento da covid-19, passou a ser utilizado para o acompanhamento de pacientes com coronavírus ou eventuais portadores do vírus[88]. O serviço israelense foi alvo de apreciação pela Corte de Israel, que entendeu não ser razoável a sua utilização sem uma legislação especial que autorizasse o programa e estabelecesse limites. A Corte afirmou ainda que o *Shin Bet* não teria autoridade para fazer o rastreamento de civis como forma de conter o avanço da crise sanitária, justamente em razão do risco de violação à privacidade e à democracia[89].

Outros países pelo mundo também se apropriaram do uso de tecnologias para o controle sanitário. Em Moscou, a polícia conseguiu localizar 200 pessoas que teriam inobservado as regras de isolamento impostas pelo governo, baseando-se em uma reportagem de um jornal russo que teria apontado supostos infratores que estavam fora de suas respectivas residências[90].

Na Rússia, dados telefônicos e informações relativas às transações de cartões de crédito foram utilizadas para mapear pessoas que teriam tido contato com pessoas contaminadas pelo

---

[87] FREITAS, Christiana Soares de; CAPIBERIBE, Camila Luciana Góes; MONTENEGRO, Luísa Martins Barroso. Governança Tecnopolítica: Biopoder e Democracia em Tempos de Pandemia. NAU Social, v. 11, n. 20, p. 191-201, 2020.

[88] Disponível em: https://www.jota.info/opiniao-e-analise/colunas/juiz-hermes/ferramentas - tecnologicas-e-controle-da-pandemia-14062020

[89] Disponível em https://edition.cnn.com/2020/03/29/europe/russia-coronavirus-authoritarian-tech-intl/index.html

[90] Disponível em: https://edition.cnn.com/2020/03/29/europe/russia-coronavirus-authoritarian-tech-intl/index.html

vírus. Além dessa checagem de dados críticos como esses, o sistema russo de monitoramento contou com 170 mil câmeras com mecanismo de reconhecimento facial[91].

Um sistema parecido foi utilizado na Coreia do Sul, que também se apropriou dos dados relativos às transações de cartão de crédito, geolocalização de aparelhos telefônicos e imagens de câmeras de vigilância para a identificação de pessoas que pudessem estar portando o vírus da COVID-19[92].

Conforme demonstrado, são vários os países que se valem da coleta de dados para o monitoramento da população em decorrência da pandemia, todavia, como observado por Rondon, já há "pesquisas e estudos relatando que este tipo de dado é pouco efetivo no combate de uma epidemia".[93]

Devido à natureza rotinizada e administrativa liderada pelo Estado, a vigilância em massa é normalizada.

> Em outras palavras, o conjunto de ações associadas às políticas de prevenção e tratamento da pandemia poderia se estender *ad infinitum* e, com isso, gerar um Estado de exceção permanente ao lado de novas formas de socialização, tendo como justificativa moral a proteção da vida, no sentido de "vida biológica".[94]

Assim, os mecanismos de controle demonstram a necessidade de estabelecer critérios objetivos para evitar que determinadas externalidades limitem de forma drástica o direito à privacidade, à intimidade e à proteção de dados.

No Brasil, no âmbito do Poder Judiciário, é necessário analisar as nuances sensíveis que possam acarretar em danos ao acesso e ao uso indevido dos dados ou o tratamento fora dos limites estabelecidos e requisitado pelo Poder Judiciário, em afronta a Lei Geral de Proteção de Dados, deve ser fiscalizado pelo Conselho Nacional de Justiça, Tribunal solicitante e operador e controlador dos dados disponíveis no sistema de proteção, assim como à Autoridade Nacional.

---

[91]Disponível em: https://www.themoscowtimes.com/2020/03/25/coronavirus-outbreak-is-major-test-for-russias-facial-recognition-network-a69736

[92] Conferir a reportagem em: https://www.newyorker.com/news/news-desk/seouls-radical-experiment- in-digital-contact-tracing

[93] RONDON, Thiago. Não precisamos da sua geolocalização para conter a propagação da covid-19: Tecnologia Bluetooth permite alertar pessoas sobre contato com alguém infectado sem violar a privacidade dos envolvidos. Época Negócios, em 14 de abril de 2021. Disponível em: <https://epocanegocios.globo.com/colunas/Multidoes/noticia/2020/04/nao-precisamos-da-suageolocalizacao-para-conter-propagacao-da-covid-19.html>.

[94] LACERDA, Marcos. Governança na pandemia: a ciência como regulação moral e os problemas da biopolítica. Simbiótica. Revista Eletrônica, 69-86, 2020. <https://doi.org/10.47456/simbitica.v7i1.30983>.

Em caso de infração às normas de proteção de dados, aplicam-se às entidades públicas e aos órgãos públicos a responsabilidade e sanções administrativas previstas na Lei de Proteção de Dados, sem prejuízo de aplicação de previsão legislativa específica do Estatuto do Servidor, Lei de Improbidade Administrativa e Lei de Acesso à Informação.

Neste caso, além das sanções cabíveis, a Autoridade Nacional poderá determinar as medidas cabíveis para interromper a violação, solicitar a elaboração de Relatório de Impacto à Proteção de Dados Pessoais e indicar padrões e boas práticas com vistas de proporcionar que o tratamento de dados pessoais pelo Poder Público seja seguro e sigiloso.

Em verdade, é possível notar que as práticas de vigilância constantemente estão calcadas em três justificações, quais sejam, i) a segurança, ii) a visibilidade e iii) a eficácia informacional.

No que se refere à segurança, a vigilância se fundamenta no combate à violência de uma forma geral, conforme supracitado, na luta contra o medo provocado pelo "terrorismo". No que tange à visibilidade, a vigilância se pauta nas novas formas e interpretações entre o "ver" e "ser visto" no âmbito social, em especial na cibercultura. Isto posto, no que se refere a eficácia informacional, a vigilância surge como justificativa para melhoria e maior efetividade no acesso e na prestação de bens e serviços, em especial no mercado de consumo.

Assim, nota-se que o monitoramento das pessoas não se reduz ao enquadramento e fiscalização de comportamento, mas ao revés, ao induzimento de determinadas condutas especialmente relacionadas ao consumo, onde impera a lógica da classificação e da padronização, conforme será detidamente debruçado no capítulo seguinte.

4.2. A UTILIZAÇÃO DE DADOS PESSOAIS NA PERSPECTIVA DAS RELAÇÕES PRIVADAS DE CONSUMO

A relação consumerista talvez seja a aplicação mais latente da legislação protetiva, sobretudo porque a coleta e tratamento de dados pessoais é exigida na maioria das relações. Ademais, o Código de Defesa do Consumidor constitui, em nosso ordenamento pátrio, o primeiro dispositivo legal onde se encontrou importante inovação na tutela de proteção de dados pessoais em nosso ordenamento jurídico. Fato este, diante, por exemplo, do artigo 43, que, ao prever o funcionamento dos bancos de cadastros e dados dos consumidores, possibilitou a regularização de informações equivocadas, assegurando o acesso à informação e o exercício do direito à informação. Desde então o consumidor tem o direito a ter acesso irrestrito e amplo a suas informações, devendo estes ser objetivos, verdadeiros, claros e de compreensão fácil. Tendo como finalidade precípua o acesso efetivo que possibilita o acompanhamento das

informações, de modo que, seja possível a correção de dados incorretos.

Pode se dizer que o Código de Defesa do Consumidor Brasileiro protege as mesmas bases informativas da legislação de proteção de dados. No entanto, esta tutela estava restrita às relações de consumo, proteção hodiernamente estendida às diversas relações sociais[95].

Na relação com o fornecedor, verifica-se nítido desequilíbrio entre as partes, por mais que seja assegurado pelo código, este consumidor, muitas vezes não pode tomar uma decisão clara, informada e livre sobre nuances contratuais, sobretudo o uso dos seus dados, que passa a ter maior tutela com a legislação específica.

A Lei de proteção de dados surge como medida de eficácia ao código consumerista, conferindo sanções e responsabilização em caso de violação, uma das maiores preocupações do direito do consumidor, que é atingir a eficácia do princípio da privacidade, intimidade, ou seja, que os dados do consumidor sejam de fácil acesso fornecido a ele, mas que seja limitado este acesso a terceiros.

O dever de prestar informações, esculpidos na lei protetiva de dados é mais específico e denso que a que se refere o Código de Consumo. A legislação protetiva de dados, impõe livre acesso e transparência, de modo que o titular dos dados tenha informação inequívoca, de forma gratuita e facilitada, acerca dos dados coletados, da forma de tratamento, duração e descarte destes.

Em verdade, o acesso à informação, rápido e dinâmico, não só amplia as possibilidades de ação das pessoas como também, na mesma proporção, maximizam os riscos de danos. Afinal, o monopólio de informações pessoais pode ter como consequência a geração de situações nefastas, como as previstas por George Orwell, ao criar a figura do “Big Brother”. ' Evidentemente, quando se trata de sociedade da informação, os desafios atingem tanto a esfera pública quanto a privada.

Sendo assim, a abordagem jurídica dos dados das pessoas, umbilicalmente relacionado à necessária garantia da privacidade, passou a ser tema de relevantes discussões jurídicas.

No Brasil, a Lei 13.709 foi promulgada em 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), visando a normatização do tratamento de dados, que até então não encontrava legislação atinente. Não obstante as diversas leis esparsas que existiam anteriormente tratando sobre o tema, com destaque para a Lei 12.965/14, isto é, o Marco Civil da Internet, não existia, ainda, no país, uma normatização suficientemente adequada à tutela de

[95] PRUX, Oscar Ivan. A Interação entre os Direitos da Personalidade e o Direito do Consumidor: Um Diálogo Construtivo. Revista do Instituto do Direito Brasileiro. Ano 3, n. 1, p. 461-481, 2014. Disponível em: <http://www.idb- fdul.com/uploaded/files/2014_01_00461_00481.pdf>. Acesso em: 26 Jun. 2020, p. 474.

dados pessoais em toda sua dimensão contextual. Assim, a LGPD estabelece, em seu artigo inaugural que a lei dispõe sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Neste sentido, é evidente que veio a norma jurídica tutelar direitos fundamentais já previstos em mandamentos constitucionais, a saber, a liberdade, a privacidade e o livre desenvolvimento da personalidade humana. Ressalta-se também que a proteção dos dados pessoais é um direito humano garantido como direito fundamental em diversas legislações, em vários países, como também assim considerado na Carta dos Direitos Fundamentais da União Europeia, expressamente em seu artigo 8°.

Entretanto, a característica mais importante da LGPD, para fins da presente análise, é a expressa disposição de que a lei, protegendo os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, inclusive nos meios digitais, será aplicada contra o tratamento ilegal de dados pessoais praticado, tanto por pessoa natural, quanto por pessoa jurídica, seja esta de direito público ou privado. Ou seja, assim como o CDC, lei decorrente do dever fundamental de proteção do consumidor como agente constitucionalmente designado, a LGPD trata de legislação que tutela direitos fundamentais de modo transversal, isto é, aplicável às relações jurídicas, tanto de direito público, quanto de direito privado, seguindo este mesmo sentido as propostas de reforma do CDC, que visam especialmente regular as relações virtuais de consumo.

Sendo assim, a LGPD corrobora para o entendimento de que cabem às legislações infraconstitucionais a retirada da abstração das normas fundamentais, previstas na constituição, por meio da setorização nas legislações específicas, aproximando a norma das particularidades e, além disso, da tecnicidade dos fatos concretos, ou seja, da vida real, inundada em variadas complexidades. Dessa maneira, vale lembrar que a LGPD é uma legislação extremamente técnica, composta por uma porção de conceitos jurídicos necessários ao fim a que se destina e de itens de controle para assegurar a efetividade das garantias defendidas pela norma. Sendo assim, a LGPD concretiza, de maneira mais bem definida, a proteção dos direitos fundamentais abstratamente tratados no artigo 5° da Constituição, garantindo, inclusive, a autonomia privada das pessoas, valor essencial à consagração do direito fundamental à liberdade.

Conforme se percebe, a LGPD corrobora para a compreensão de que a proteção dos direitos fundamentais não pode ser limitada à atuação da pessoa natural frente ao Estado, em especial quando há pessoa em situação de vulnerabilidade, como ocorre com os indivíduos sujeitos ao tratamento ilegal de dados pessoais e, posteriormente, expostos às publicidades

virtuais de consumo importunadoras.

Neste ponto, merece ênfase o pensamento de Guilherme Magalhães Martins, segundo o qual a desigualdade entre os fornecedores e os usuários da Internet, em especial nas redes sociais, é patente, afinal, além destes serem induzidos a contratar por técnicas agressivas de publicidades, a vulnerabilidade se agrava por desconhecer o consumidor as nuances das técnicas que fundamentam a relação que compõe.[96]

Logo, ao se considerar que a grande maioria das relações jurídicas no âmbito virtual são também relações de consumo, nítida está a situação de hipervulnerabilidade, que demanda maior atenção e, consequentemente, um âmbito de tutela mais intensificado.

Neste ponto, destaca-se que *"o potencial perigo para a privacidade dos cidadãos, representado inicialmente pelo Governo, deu lugar à outra ideia segunda a qual o setor privado poderia representar uma ameaça muito maior."*[97] Todos esses apontamentos indicam que a LGPD demonstra que a teorias da eficácia indireta e eficácia direta não são formas incompatíveis de tutela dos direitos fundamentais, afinal, havendo legislação específica tendente à proteção de direitos essenciais.

Sendo assim, é evidente a mitigação do debate quanto à polêmica consideração dos direitos fundamentais nessas relações privadas, afinal, partindo do pressuposto de que se tratam de relações desiguais, a tutela do vulnerável se torna um imperativo. Não obstante, o próprio CDC, em seu artigo I, estabelece ser a lei protetiva norma de ordem pública e interesse social, remetendo ao cumprimento da exigência prevista no artigo 5°, inciso XXXII da CF/88. Vale lembrar, inclusive, que a realidade é que o sistema jurídico é uno, de modo que a tutela da pessoa humana se apresenta como um problema unitário.

Neste ponto, há de se considerar a essencialidade do direito ao sossego, juntamente com a proteção de dados pessoais, como forma de garantir a liberdade integral das pessoas, inclusive sob a ideia de extensão da personalidade, também ao homem artificial.

Aliás, muito além de refletir acerca da eficácia horizontal desses direitos, têm-se pistas da necessidade de evidenciar o anverso fundamental, qual seja, o dever das grandes

---

[96] MARTINS, Guilherme Magalhães. Contratos eletrônicos de consumo. São Paulo: Atlas, 2016. p. 55.

[97] Não somente pelos regimes totalitários, como o demonstram a alardeada ação do sistema Echelon de 27vigilância. O Echelon é uma rede de rastreamento de telecomunicações cuja existência é formalmentenegada pelos países que seriam seus patrocinadores e usuários – os Estados Unidos, Inglaterra,Canadá, Austrália e Nova Zelândia - e que é objeto de debates pela comunidade internacional – vide odossier "Development of surveillance technology and risk of abuse of economic information",apresentado ao Parlamento Europeu por Duncan Campbell e disponível em <www.europarl.eu.int/stoa/publi/pdf/98-14-01-2_en.pdf?redirected=1> (02/01/2004). Também serve de exemplo o ímpetolegiferante que segue o 11 de setembro nos Estados Unidos, com a instituição de legislação restritivada privacidade e de outras liberdades civis.

fornecedoras em respeitar às pessoas expostas às práticas de mercado (consumidores por equiparação), em especial, no que se refere às publicidades virtuais de consumo.

Em verdade, analisando a lógica do mercado, que opera pelo código binário "lucrativo/não lucrativo", a proteção do consumidor se mostra como uma forma de superar as falhas do mercado, que expõe as pessoas ao risco de danos. Dito de outro modo, é a lei que cumpre a função de ordenar o mercado no afã de proteger as pessoas das práticas comerciais abusivas, como o tratamento inadequado de dados pessoais do consumidor, garantindo o cumprimento efetivo do fundamento de tutela da pessoa humana, expresso na carta constitucional, mesmo dentro da lógica do direito privado, o que reforça a supracitada eficácia horizontal das normas fundamentais.

Despiciendo dizer que o CDC, em seu artigo inaugural, estabelece que sua finalidade é a proteção e defesa do consumidor, matéria de ordem pública e interesse social, ressaltando o artigo 170, inciso V, da CF/88, o qual, expressamente, impõe ao legislador infraconstitucional a defesa do consumidor como princípio geral da atividade econômica, mas que cumpre função promocional dos direitos humanos.

Noutras palavras, no sistema jurídico brasileiro, só se admite a prática comercial que, além de outros princípios, respeite a dignidade da pessoa humana, que, em seu sentido mais amplo, congloba os direitos dos consumidores. Significa dizer que a norma constitucional procura compatibilizar a livre iniciativa com a tutela das pessoas vulneráveis expostas às práticas do mercado, utilizando o CDC como mecanismo para a instrumentalização dessa tutela.

Sendo assim, o lucro só se legitima a partir do respeito ao direito dos consumidores. Por causa disso, conforme exposto, o artigo I do CDC expõe que a lei protetiva do consumidor é uma norma de interesse social, ou seja, é legislação que vai além da relação entre as partes (consumidor/fornecedor), pois também deve ser interpretada no interesse de toda a sociedade. Noutros termos, o fornecedor que age contrariando o CDC não apenas viola o direito do consumidor diretamente envolvido, como também prejudica a livre concorrência e, em última análise, pode colocar em risco os direitos e interesses legítimos de outras pessoas.

Como "coluna vertebral" do CDC, o artigo 4° traça a Política Nacional de Relações de Consumo, prevendo os princípios mais importantes do código consumerista no intuito de cumprir essa função social supracitada. Destacadamente, o inciso I reconhece a vulnerabilidade do consumidor no mercado de consumo, razão pela qual se tem um microssistema norteado por um código, que é expressamente protetivo. Com efeito, é em razão dessa vulnerabilidade que se busca, por meio da lei, promover à tutela das pessoas em situação de consumo.

Além disso, é importante mencionar o artigo 6° do Código, que prevê os direitos básicos

dos consumidores. Em verdade, muitos direitos fundamentais expressos na Constituição surgem como direitos da personalidade no Código Civil e, na relação de consumo, são protegidos como direitos básicos. À guisa de exemplo, destaca-se a proteção à vida, à saúde e à segurança - mandamentos fundamentais - em todos os âmbitos do Direito (constitucional, civil e consumidor).

Diante do exposto, uma vez assentada a ideia de que a CF/88 previu a tutela do consumidor como direito fundamental, sendo setorizado através do CDC especialmente. É importante ressaltar que a coexistência de direitos fundamentais pressupõe também a existência de deveres fundamentais, os quais, segundo Fernando Martins *"são aqueles alocados na cúspide do sistema (a Constituição Federal)."*[98]

Aliás, neste ponto, extrai-se do próprio artigo 5°, inciso XXXII da CF/88 que o Estado possui o dever de defender o consumidor.

Daí porque é possível reconhecer a proteção de dados pessoais como um dos mais relevantes direitos básicos reconhecidos ao consumidor atualmente, e conforme supracitado, orienta-se no sentido dos direitos da personalidade, fundamentais e humanos.

Ademais, em uma sociedade da informação, onde dados pessoais dos consumidores são tratados de maneira cada vez mais intensa, por meio de tecnologias cada vez mais avançadas, é preciso repensar acerca da necessidade de se ampliar a tutela da personalidade do consumidor.

Afinal, *"a proteção dos dados pessoais é instrumental para que a pessoa possa livremente desenvolver sua personalidade"*. Em razão disso, nota-se que a concretização da proteção do consumidor no atual contexto somente pode ser atingida com o reconhecimento de um direito básico do consumidor à proteção de dados pessoais, envolvendo uma dupla dimensão, qual seja, a de tutela da personalidade do consumidor contra os riscos inerentes à coleta, processamento, utilização e circulação dos dados pessoais (legitimidade do tratamento de dados pessoais) e, também, através do empoderamento do consumidor no sentido de controlar o fluxo de seus dados na sociedade (autodeterminação informativa do consumidor).

Neste sentido, cabe mencionar a proposta do Projeto de Lei 3.514/15, que pretende atualizar as disposições do CDC para dispor sobre o comércio eletrônico, inclusive tratando de maneira específica a proteção de dados pessoais como direito básico do consumidor. Segundo a proposta legislativa:

> Art. 6º, XI - a privacidade e a segurança das informações e dados pessoais

[98] MARTINS, Fernando Rodrigues. Os deveres fundamentais como causa subjacentevalorativa da tutela da pessoa consumidora: contributo transverso e suplementar à hermenêutica consumerista da afirmação. Revista de Direito do Consumidor, São Paulo, v. 23, n. 94, p. 215-257, jul./ago. 2014.

> prestados ou coletados, por qualquer meio, inclusive o eletrônico, assim como o acesso gratuito do consumidor a estes e a suas fontes;
> XII - a liberdade de escolha, em especial frente a novas tecnologias e redes de dados, vedada qualquer forma de discriminação e assédio de consumo;

Mais do que nunca, é preciso ser reconhecida a necessária integridade humana nas diferentes posições jurídicas que a pessoa assume durante a vida, inclusive dentro do contexto da sociedade de consumo e do mundo virtual, posto que *"o processo descritivo deve ser passível de diferenciadas conclusões considerando a funcionalidade investigativa fragmentada, em outras palavras: policentexturalidade."*[99]

Portanto, destacando a importância da regulação das aplicações tecnológicas, com as devidas responsabilidades, é possível afirmar ser preciso assumir uma responsabilidade coletiva, por um futuro em que a inovação e a tecnologia estejam focadas na humanidade e na necessidade de servir às pessoas, visando um desenvolvimento sustentável, e não baseada na total liberdade, capaz de violar direitos fundamentais e, em última análise, perturbar o sossego das pessoas.

4.3. Leis setoriais e a elaboração de um microsistema de proteção de dados pessoais no brasil;

Vale ressaltar que a intenção do direito à proteção de dados pessoais, nos diversos países conforme suas respectivas legislações (inclusive no Brasil), não é proteger os dados em si, mas, sim, a pessoa titular dos dados - que, ao longo da evolução do Direito, passou a ter o inafastável poder de autonomia sobre seus dados. E, com isso, contribuir para a preservação das garantias fundamentais a igualdade, a liberdade, a democracia e a personalidade.

No caso da legislação brasileira, é acertado afirmar que as normas que regem a sociedade de maneira geral são plenamente aplicáveis ao universo tecnológico onipresente nos dias atuais.

Contudo, haja vista os inúmeros desafios postos, como em diversas outras nações, também no Brasil fez-se necessária a existência de normas específicas a regularem esse novo campo social e negocial, iniciando-se com o Marco Civil da Internet - Lei 12.965/2014 - e, mais

[99] MARTINS, Fernando Rodrigues. Sociedade da informação e promoção à pessoa: empoderamento humano na concretude de novos direitos fundamentais. In: MARTINS, Fernando Rodrigues. Direito privado e policontexturalidade: fontes, fundamentos e emancipação. Rio de Janeiro: Lumen Juris, 2018. p. 403.

recentemente, com a Lei Geral de Proteção de Dados Pessoais - Lei 13.709/2018 -, que dispõe sobre o tratamento de dados pessoais nos meios analógicos e digitais.

4.4. Suas consequências no Direito Privado

Podemos afirmar que o diálogo das fontes está presente na Lei Geral de Proteção de Dados Pessoais. Essa abertura a outras fontes legislativas favorece intrincada rede de proteção que garante respeito aos dados pessoais, haja vista que eventuais violações não podem, assim, passar despercebidas.

Nesse sentido, há diálogo, por exemplo, quando ocorre violação de dados (mas não só) pelo chamado "encarregado", que não se encontra inserido no conceito de agente de tratamento, tampouco foi alvo de disciplina específica de responsabilidade civil na Lei 13.709/2018. Todavia, trata-se de alguém que pode causar danos, violar direitos e, em vista disso, deve ser responsabilizado por seus atos. Logo, esse silêncio parece atrair a cláusula geral do Código Civil.

Considerando a hipótese de o encarregado violar direitos e causar danos a titulares de dados em relações de consumo, possível torna-se a aplicação do Código de Defesa do Consumidor, sendo possível avocar seu artigo 34, que estabelece a responsabilidade solidária do fornecedor do produto ou serviço por atos de seus prepostos ou representantes autônomos.

Isso se justifica porque a Lei Geral conceitua (artigo 5º, inciso VIII) o encarregado como a *"pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)".* Ao que parece, pois, ora pode ser preposto, ora representante autônomo do controlador e, com este, ser responsável solidário pelas lesões causadas.

Ademais, há potencial lesivo nas atividades do encarregado (ainda que não haja relação de consumo), dentre as quais a de adotar providências diante de comunicações recebidas pela Autoridade Nacional e de reclamações e comunicações dos titulares de dados, nos termos do artigo 41, § 2º, incisos I e II, da Lei Geral de Proteção de Dados Pessoais.

Quando, nesses casos, houver dano, o encarregado deverá ser responsabilizado, mormente por se tratar de dano a direito fundamental, a direitos da personalidade. Com efeito, o caso concreto indicará a norma a ser simultaneamente aplicada com a Lei Geral. Cabe destacar que, situações como essa, não raras vezes incluem a ocorrência de ato ilícito ou de abuso de direito, exigindo a incidência, por exemplo, dos artigos 186 ou 187, combinados com o 927,

todos do Código Civil.[100]

Noutro exemplo, identifica-se presente a busca de concretude na Lei Geral de Proteção de Dados Pessoais (consoante se denota da investigação de princípios antes considerados), tal qual visa o Código Civil com o princípio da operabilidade. Ambos os diplomas pretendem garantir efetividade de suas normas e oferecem, cada qual a seu modo, instrumentos para que combinados, ser alcançado o almejado foco.

Desse modo, vislumbra-se contínuo diálogo, seja com o intuito de conferir efetividade ao ordenamento jurídico, seja para identificar responsáveis em ações indenizatórias. Em relação ao segundo propósito, o diálogo garante respeito aos diplomas legais, de forma concreta, e reconduz à harmonização abalada por prejuízos decorrentes de tratamento irregular de dados e transgressões a normas, tudo respeitada a segura orientação de preceitos constitucionais.

Vale acrescentar que a previsão do artigo 6º da Lei Geral de Proteção de Dados Pessoais determina a obrigatória observância da boa-fé nas atividades de tratamento de dados. Esse norte está presente, também, no Código Civil, do qual se extraem positivações derivadas da boa-fé objetiva, como a fonte de interpretação de negócios jurídicos (artigo 113) e o limite do exercício de direitos subjetivos (artigo 187 – abuso de direito). Tais experiências e dispositivos legais devem ser (co)utilizados na interpretação de situações que envolvam dados pessoais, sendo, portanto, aplicáveis a esses casos, também abrangidos pelo princípio da boa-fé (art. 422, Código Civil) e a função social dos contratos.

Uma vez apresentados importantes aspectos da proteção de dados, reporta-se necessário o exame das pretensões restitutórias pelos lucros ilícitos para, mais adiante, identificar a viabilidade dessas pretensões serem exploradas em casos que envolvem a proteção de dados pessoais, com a presença de diálogo das fontes, norteada pela escala de valores estabelecida pela Constituição Federal.

Adiante, investigaremos a responsabilidade civil na LGPD, mas desde logo importa registrar o texto do artigo 45 da LGPD que prevê as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente, conforme será abordado nos tópicos a seguir.

4.5. Primordialidade da regulação de normas de privacidade de dados para crianças e adolescentes

[100] MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados: Comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. Revista de Direito do Consumidor. v. 130. Ano 29. São Paulo: Ed. RT, jul-ago. 2020.

Crianças e adolescentes compõem o grupo mais vulnerável de pessoas cujos dados pessoais circulam na ubiquidade dos meios digitais. Por estarem vivenciando um período peculiar de desenvolvimento, tanto físico, quanto cognitivo, psicológico e social, de acordo com as respectivas idades, esses menores muitas vezes não têm condições de compreender a complexidade da sociedade da informação ou do conhecimento, quanto menos defenderem-se dos abusos que nela são perpetrados. São, com efeito, menos conscientes, tanto dos modelos, quanto das consequências e ameaças do processamento de seus dados.

Antes de adentrar o tema, forçoso conceituar e distinguir os vulneráveis e hipervulneráveis, enquanto subsídio para melhor compreensão do estudo. A categoria ético-política, e também jurídica, dos sujeitos vulneráveis inclui um subgrupo de sujeitos hipervulneráveis, entre os quais se destacam, por razões óbvias, as pessoas com deficiência física, sensorial ou mental.

No Recurso Especial de nº 586316/MG Superior Tribunal de Justiça, explicitado no voto do Min. Herman Benjamin na relatoria, trouxe didaticamente a conceituação:

> O Código de Defesa do Consumidor, é desnecessário explicar, protege todos os consumidores, mas não é insensível à realidade da vida e do mercado, vale dizer, não desconhece que há consumidores e consumidores, que existem aqueles que, no vocabulário da disciplina, são denominados hipervulneráveis, como as crianças, os idosos, os portadores de deficiência, os analfabetos e, como não poderia deixar de ser, aqueles que, por razão genética ou não, apresentam enfermidades que possam ser manifestadas ou agravadas pelo consumo de produtos ou serviços livremente comercializados e inofensivos à maioria das pessoas.[101]

Isto posto, no que tange as crianças e adolescentes, ainda que não tenham acesso ou mesmo, conforme o caso e a idade, uma certa capacitação tecnológica de manuseio das ferramentas, o que, inclusive, gera a percepção de que crianças seriam supostas nativas digitais. Entretanto, apesar de apresentarem habilidades de uso das novas tecnologias de informação e comunicação, não conseguem, muitas vezes, compreender as complexas dinâmicas de causa e

[101] (STJ - REsp: 586316 MG 2003/0161208-5, Relator: Ministro HERMAN BENJAMIN, Data de Julgamento: 17/04/2007, T2 - SEGUNDA TURMA, Data de Publicação DJe 19/03/2009)

consequência atreladas a essas ferramentas. A questão que se coloca diz respeito à capacidade de usufruírem plenamente dos recursos disponíveis nas novas tecnologias da informação e da comunicação, de maneira que possam se incluir na nova ordem social da tecnologia digital tendo o conhecimento e o repertório necessários.

São também mais vulneráveis pelo volume de utilização que fazem das tecnologias da informação e da comunicação. A esse respeito, vale observar que, no ambiente brasileiro, crianças e adolescentes são usuários frequentes e bastante entusiasmados das novas tecnologias da informação e da comunicação, ainda que sejam expostos a riscos diversos. Vale dizer que, de acordo com a pesquisa TIC Kids Online Brasil 2019[102], divulgada pelo Comitê Gestor da Internet no Brasil (CGI.br)15, 89% das crianças e adolescentes entre 9 e 17 anos têm acesso à Internet (acessaram a rede nos três meses que antecederam a pesquisa), sendo que, destes, 95% fizeram esse acesso por meio do telefone celular enquanto 38% usaram computadores, 43% a televisão e 18% o videogame.

Esse crescente acesso de crianças e adolescentes a novas tecnologias da informação e da comunicação não significa que sejam eles hábeis e competentes usuários. Assim, a ideia de que crianças e adolescentes seriam "nativos digitais", já nascidos com certa qualificação para dominarem a complexidade do universo digital, é um exagero. Há quem faça um paralelo do processo de aprendizado das habilidades de domínio das novas tecnologias da informação e da comunicação com a alfabetização, no sentido de que o uso acrítico da tecnologia poderia se assemelhar ao mero conhecimento das letras do alfabeto, mas não indicar uma capacidade de leitura crítica.

Ainda, os impactos e problemas sociais advindos do processamento de dados de crianças e adolescentes para seu bem-estar individual e social são múltiplos, como: **(i)** a ameaça à integridade física, psíquica e moral por contatos maliciosos de terceiros; **(ii)** a hiperexposição de dados pessoais e discriminação; **(iii)** a modulação e manipulação de comportamento; e **(iv)** a microssegmentação da prática abusiva e ilegal da publicidade infantil, que implicam em vícios comportamentais (adicção) como vício do "auto-play", comumente conhecido barra de rolagem, técnica esta derivada das técnicas de design que exploram as vicitudes de humanos,

[102] De acordo com a pesquisa TIC Kids Online Brasil 2019, divulgada pelo Comitê Gestor da Internet no Brasil (CGI.br), das pessoas entre 9 e 17 anos que acessaram a Internet nos três meses anteriores à pesquisa, nos 12 meses que antecederam a data da pesquisa: (i) 43% já viram alguém ser discriminado na Internet; (i) 15% tiveram contato com conteúdo sensível de autodano sobre formas para ficar muito magro; (ii) 12% tiveram contato com conteúdo sensível de autodano sobre formas de machucar a si mesmo; (iii) 15% tiveram contato com conteúdo sensível de autodano sobre formas de cometer suicídio; e (iv) 10% tiveram contato com conteúdo sensível de autodano sobre experiência ou uso de drogas. https://cetic.br/media/analises/tic kids online brasil 2019 coletiva imprensa.pdf. Acesso em: 10 jan. 2022.

em especial crianças e adolescentes de forma a explorar tais vulnerabilidades para o fim de propiciar maior dependência de plataformas e operações digitais, o que vulnerabiliza o contexto de crianças e adolescentes expostos no ambiente digital.

Pela coleta massiva de dados pessoais e seu armazenamento muitas vezes não seguro, crianças e adolescentes podem ser mais facilmente contatados por pessoas mal-intencionadas por meio de seus dados pessoais expostos ou em tecnologias vulneráveis, apresentando perigo a sua integridade física, psíquica e moral. Ainda, a hiperexposição indevida desses dados pessoais coletados e processados relativos à educação, saúde, comportamento, gostos e desejos - inclusive dados sensíveis ligados a biometria, genética, religião, opinião política, filosófica ou dados referentes à saúde ou à vida sexual - pode, inclusive, servir de base para discriminação em processos de admissão em trabalho, educação e contratação de planos de saúde.

A hiperexposição indesejada de dados pessoais pode comprometer, assim, o desenvolvimento sadio desses indivíduos no presente, por gerar mais estresse e ansiedade no indivíduo e na família, mas também no futuro, em função do "rastro digital" dessas informações e do mau uso por empresas de saúde, contratação e seleção de profissionais, ou processos seletivos em educação, além do impacto em sua reputação.

Outro ponto objeto de necessária atenção é o uso de dados pessoais para modulação e manipulação dos comportamentos de crianças e adolescentes. O uso de dados para direcionamento de conteúdo, publicidade ou propaganda pode comprometer a diversidade das informações disponíveis às crianças e adolescentes e afetar o seu direito ao livre desenvolvimento da personalidade, criando a chamada bolha autorreferencial, limitando o acesso a diferentes oportunidades e contato com a diversidade de opiniões e ideias no seu desenvolvimento. Nesse sentido, crianças são mais vulneráveis a estratégias de uso de informações pessoais para segmentação das mensagens para persuasão para comportamentos ou decisões relativas a desejos de compra e, até mesmo, percepções sobre o mundo e as opiniões sobre ele.

Ainda, é preciso compreender que o excesso de vigilantismo e rastreamento de desejos e comportamentos de crianças e adolescentes pode restringir suas práticas de pesquisa e buscas on-line, modificar práticas e interações sociais, com implicações na fruição de direitos diversos, como o direito ao livre desenvolvimento da personalidade, privacidade e autonomia.

Por fim, dados pessoais sensíveis e íntimos são coletados, utilizados e monetizados para realização de microssegmentação da publicidade infantil, já considerada prática considerada abusiva e, portanto, ilegal pela legislação brasileira e decisões em tribunais superiores. Contudo, o uso de dados pessoais na publicidade infantil deixa ainda mais evidente sua

abusividade, uma vez que tal prática permite uma eficácia ainda maior de persuasão de crianças e manipulação dos seus desejos de consumo. Exemplo disso é a criação de "necejos" derivação de (necessidade + desejos), que propicia o uso de informações sobre a saúde ou estado de humor de um indivíduo para a criação de estratégia ainda mais eficaz de convencimento para aquisição de produtos ou serviços.

Diferentes autores de teorias das necessidades[103], e sobre a ténue linha que as vezes diferencia às necessidades dos desejos, mas o fato é que o consumo satisfez necessidades e desejos e está conectado tanto a bens essências quanto a bens supérfluos. Salienta também uma conclusão recorrente nas pesquisas de consumo: *"Os consumidores sabem muito bem o que não querem, porém não sabem o que desejar".* Despertar necessidades e criar desejos e expetativas não são ações suficientes para se conseguir sucesso com os consumidores potenciais, YANAZE (2011).

Mesmo que crianças e adolescentes sejam educados e preparados para se apropriarem de todo o potencial que as novas tecnologias da informação e da comunicação possuem - por estratégias necessárias de educação para o uso de mídias -, ainda assim serão mais vulneráveis diante do massivo tratamento de dados pessoais que tem dominado as práticas comerciais e, por vezes, são atentatórias à ética e à moral, dada a condição peculiar de desenvolvimento que vivenciam - especialmente quanto mais novos forem.

Vale lembrar que o desenvolvimento cognitivo e mental do ser humano inicia-se na infância e é um processo identificável que se dá por várias etapas e superação de fases subsequentes na sequência correta, sem que seja possível pular estágios. Não se trata de algo que se adquire e transforma-se em um patrimônio do indivíduo, mas é uma evolução, uma construção paulatina, que demanda tempo e vivências, atreladas a uma interação complexa e multirreferencial entre a natureza da constituição genética (*nature*) e os estímulos dos meios de convivência e socialização da criança (*nurture*), inclusive os provenientes das novas tecnologias de informação e comunicação.

De todas essas constatações, provenientes das teorias acerca do desenvolvimento humano, resulta a conclusão de que as fases de desenvolvimento humano devem ser guardadas e cuidadas também socialmente ou, em outras palavras, as crianças e os adolescentes devem ter seu direito a um sadio desenvolvimento preservado, também no que se trata das relações sociais no âmbito das tecnologias da informação e da comunicação.

No campo da privacidade, diversas são as pesquisas que comprovam a sua necessidade

[103] YANAZE, Mitsuru H. Gestão de marketing e comunicação: Avanços e aplicações. São Paulo. Saraiva. 2011

para o florescimento da subjetividade humana. A individualidade não existe sem que se possa estabelecer limites à pervasiva modulação social. O processo de autodiferenciação não é, portanto, inato, mas se dá a partir da infância, passando pela adolescência até a idade adulta, sendo consequência do desenvolvimento de diversas e variadas estratégias - físicas, espaciais e informacionais - para gerenciar as fronteiras do "eu", dinamicamente e ao longo do tempo.

A privacidade e, mais especialmente, a proteção dos dados pessoais - que supõe mais do que a interdição de acesso a informações pessoais, mas também o acesso condicionado e limitado à vontade do sujeito titular dos dados - são essenciais para a formação da personalidade e, portanto, é fundamental que sejam assegurados, especialmente no período da infância e da adolescência, ao longo do desenvolvimento social, cognitivo e biológico. A proteção de dados pessoais, na perspectiva da autodeterminação informativa, é indispensável na infância e na adolescência para a configuração de sujeitos plenos, capazes de estabelecer vínculos sociais e culturais com a sociedade e o entorno, e igualmente aptos a desenvolver perspectivas críticas acerca do contexto em que vivem.

A garantia da proteção de dados pessoais de crianças e adolescentes, além de possuir uma relevância maior em relação aos demais entes da sociedade, é mais complexa porque, enquanto pessoas em estágio peculiar de desenvolvimento biopsíquico e social, crianças e adolescentes estão começando a desenvolver a compreensão da amplitude do tratamento de dados pessoais e a capacidade de tomar as decisões sobre autorizar ou não, o uso de informações e dados pessoais.

Por outro lado, é sabido que a violação da proteção de dados pessoais de crianças e adolescentes, em nome de qualquer interesse que não o seu bem-estar, acarreta uma série de riscos, dentre os quais aqueles relacionados à sua segurança física, moral e psíquica, além de outros.

Assim, principalmente ao longo da última década, as legislações acerca da proteção de dados pessoais no mundo têm se afastado da perspectiva "adultocêntrica", indiferente à idade, que ignorava as necessidades especiais de indivíduos nessa fase específica da vida, e registrado, nas mais modernas normas que regem o uso de dados, regras distintas - mais restritas - para a gestão de dados pessoais de crianças e adolescentes.

Com isso, da mesma forma que as crianças e os adolescentes precisam de proteção especial em outras searas do Direito, também no que diz respeito à sua privacidade e proteção de dados pessoais merecem um olhar atento não só da legislação, mas de todo o Sistema de Justiça, a fim de terem sua garantia constitucional à absoluta prioridade devidamente efetivada.

Daí a necessidade de que crianças e adolescentes tenham a seu favor normas específicas,

como sujeitos de direitos que são, também no ambiente regulatório da proteção de dados pessoais, com especial atenção à garantia de sua integridade física, psíquica e moral, abrangendo a preservação da sua imagem, identidade, autonomia, valores, ideias, crenças, espaços e objetos pessoais nesse novo contexto sociotécnico.

O art. 1° da Constituição Federal de 1988 instaura, no Brasil, a doutrina da proteção integral da criança e do adolescente, reconhecendo-os como sujeitos de direito e titulares de direitos fundamentais, cuja condição de desenvolvimento peculiar deve ser respeitada, assegurando-se seu melhor interesse e a absoluta prioridade na garantia de todos os seus direitos.

Com a redemocratização e a promulgação da vigente norma constitucional, o país fez a escolha de priorizar, entre todos os entes que compõem a sociedade, justamente as crianças e os adolescentes - e, mais recentemente, por força da Emenda Constitucional 65/2010, também os jovens -, de forma que o Brasil é, hoje, uma nação que tem as crianças, os adolescentes e demais jovens que vivem em seu território no topo da importância nacional, nos termos do artigo 227 da Constituição.

Por força do dever constitucional, os direitos fundamentais assegurados à infância e à adolescência gozam de absoluta prioridade, de modo que devem ser respeitados e efetivados prioritariamente. Vale destacar que o cumprimento de tais direitos é de responsabilidade compartilhada entre Estado, famílias e sociedade, inclusive empresas, os quais devem somar esforços e tomar as medidas necessárias para cumprir esse que é um dever constitucional.

É com a Convenção sobre os Direitos da Criança da ONU, de 1989, que a doutrina da proteção integral se consagra no plano internacional, tendo sido ratificada pela quase totalidade dos países-membros da ONU (até hoje foram 196), com exceção apenas dos Estados Unidos. No Brasil, foi ratificada em 1990 e, posteriormente, promulgada pelo Decreto 99.710/1990.

A mudança de paradigma expressada na nova Constituição Federal, fruto de intensa participação social. está especialmente descrita no art. 227 da CF, que previu: ser dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de coloca-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão, conforme exposto acima.

Para viabilizar a garantia da regra constitucional da absoluta prioridade, o Estatuto da Criança e do Adolescente (ECA), reconhecendo o estágio peculiar de desenvolvimento

característico da infância e da adolescência - fato que coloca crianças e adolescentes em posição de vulnerabilidade presumida e justifica a proteção especial e integral que devem receber -, fixou no seu art. 4°, a primazia de receber proteção e socorro, precedência e preferência na formulação de políticas públicas e a destinação privilegiada de recursos públicos para sua tutela.

Pela leitura deste artigo, entende-se o cerne da regra da prioridade absoluta: crianças e adolescentes devem estar em primeiro lugar nos serviços, políticas e orçamentos públicos. Ao colocar crianças e adolescentes como absoluta prioridade no art. 227 da Constituição Federal, foi feita importante escolha política: infância e adolescência em primeiro lugar é um projeto da nação brasileira.

No Brasil, a privacidade e a proteção de dados decorrem do direito constitucional à intimidade e à vida privada; com advento da Emenda Constitucional de n° 115/2022[104], diante da previsão no art. 5°, LXXIX, da Constituição Federal que aborda a proteção de dados pessoais, inicia-se a observação do fenômeno da privacidade sob o prisma dos dados pessoais, e não da vida íntima ou privada.

Especificamente em relação a crianças e adolescentes, o art. 17 do Estatuto da Criança e do Adolescente assegura a inviolabilidade física, psíquica e moral, e o art. 71 do mesmo diploma legal estabelece o direito à informação, cultura, lazer, esportes, diversões, espetáculos, produtos e serviços, os quais devem respeitar a condição de pessoa em desenvolvimento.

Ressalta-se para melhor compreensão do presente estudo, que as expressões intimidade, vida privada, segredo ou privacidade serão consideradas sinônimos, pelas consequências jurídicas que culminam as mesmas disposições no que tange à responsabilidade civil, embora possuam terminologias e carga conceitual diversas.

O Código Civil, Lei 10.406/2002, em capítulo específico acerca dos direitos de personalidade, por sua vez, configura-os como intransmissíveis e irrenunciáveis, assim como deixa claro que compreendem o direito à integridade física, psíquica e moral, ao corpo, ao nome e à imagem. Não se trata de um rol exaustivo, podendo a proteção dos dados pessoais ser entendida como um direito da personalidade autônomo, aja vista serem a extensão da pessoa. O uso dos dados pessoais, com efeito, é capaz de impactar o próprio desenvolvimento da personalidade, na medida em que podem identificá-la, manipulá-la e, até mesmo, estigmatizá-la, além de ganharem especial relevância em um contexto de crescente desenvolvimento da tecnologia.

---

[104] Emenda Constitucional Nº 115/2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. D.O.U. Publicado em: 11/02/2022 | Edição: 30 | Seção: 1 | Página: 2.

No âmbito da Lei Geral de Proteção de Dados Pessoais, se estabeleceu os princípios básicos a nortearem o tratamento de dados pessoais para todas as pessoas: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas, conforme disposto no seu art. 6°. A norma veda o uso excessivo, inadequado e contrário à finalidade previamente estabelecida para o tratamento de dados pessoais, que somente poderá ser realizado tendo em vista a limitação do tratamento ao mínimo necessário, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades legítimas, específicas, explícitas e informadas ao titular dos dados, de acordo com o contexto do tratamento.

O que se verifica, portanto, é que já se reconhece que dados pessoais estão na esfera de direitos da personalidade e que o seu uso indiscriminado é capaz de objetificar pessoas, afetar o desenvolvimento da personalidade, promover manipulação e gerar discriminações. Quando essa realidade e os respectivos riscos são transpostos para a esfera desses menores, a questão deve ser tratada considerando, também, a proteção jurídica especial que lhes assiste por força constitucional, posto que devem ter seus direitos assegurados com absoluta prioridade.

Na seção III da LGPD, para além da regra geral das hipóteses do seu art. 7°, a nova LGPD trouxe um dispositivo específico para disciplinar o tratamento de dados pessoais de crianças e adolescentes, que, de alguma maneira, segue no mesmo sentido dos outros dispositivos já mencionados, colocando em destaque a imprescindibilidade do "melhor interesse" de crianças e adolescentes ser observado em todo e qualquer caso de tratamento de seus dados pessoais:

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
>
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
>
> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
>
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
>
> § 4º Os controladores não deverão condicionar a participação dos titulares de

> que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
>
> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
>
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Da análise do arcabouço legal sobre o tema, e especialmente por conta do previsto no caput do mencionado art. 14 da LGPD, o principal fundamento para o tratamento de dados pessoais de crianças e adolescentes, em quaisquer circunstâncias, sempre deverá ser o seu "melhor interesse".

Isso significa que o tratamento de dados de crianças e adolescentes só pode se dar exclusivamente com base no seu melhor interesse, ou seja, somente por meio de práticas que promovam e protejam seus direitos previstos no sistema jurídico nacional e internacional com absoluta prioridade, abstendo-se de práticas violadoras e exploratórias da vulnerabilidade infantojuvenil, inclusive as comerciais. Será considerado nulo de pleno direito o contrato, mesmo que realizado com consentimento parental - específico e em destaque, tal qual previsto no art. 14, § l.°, da LGPD, para o tratamento de dados pessoais de crianças e adolescentes, que não atenda ao melhor interesse das próprias crianças e adolescentes envolvidos.

Nada menciona, contudo, a LGPD no tocante ao consentimento parental no caso dos adolescentes, o que traz a necessidade de esse dispositivo da lei especial ser interpretado conjuntamente com a doutrina da proteção integral e a regra da absoluta prioridade estabelecidas pelo art. 227 da Constituição Federal e pelo próprio caput do art. 14, que estabelece a necessidade de o tratamento de dados pessoais ser realizado com vistas a garantir o melhor interesse também dos adolescentes. Assim, ainda que o § l.° não mencione os adolescentes, não faria sentido deixá-los desprovidos da igual e devida proteção, sob pena de se violar as garantias constitucionais dessas pessoas. Há que se defender, nesse caso, a aplicação do Código Civil, a fim de se promover a integralidade de seus direitos, uma vez que no meio virtual podemos notar que crianças e adolescentes, possuem capacidade de estabelecerem contratos de consumo.

De fato, a proteção de dados pessoais, entendida enquanto parte do contrato civil,

reforça a objeção à capacidade legal de crianças e de adolescentes consentirem quanto ao tratamento de seus dados, uma vez que, pelo exercício do poder familiar, compete a mães, pais e responsáveis representá-los até os 16 anos, nos atos da vida civil, e assisti-los, após essa idade, nos atos em que forem partes, suprindo-lhes o consentimento.

Dessa forma, entende-se indispensável o consentimento parental ou de pessoa responsável legal para o tratamento de dados pessoais de crianças e de adolescentes de até 16 anos de idade, observando-se a forma prevista no referido 14, § l.°, da LGPD, devendo, assim, o consentimento ser específico e em destaque. No caso de adolescentes entre 16 e 18 anos, será necessário o consentimento de ambos, não bastando o consentimento parental.

Ora, se adultos plenamente capazes para votar foram vítimas de um escândalo de manipulação em massa, decorrente do uso inadequado de seus dados pessoais, não podemos prever o que pode acontecer com crianças e adolescentes, em processo de desenvolvimento cognitivo e social. Indubitável, portanto, que o uso de dados pessoais de crianças e adolescentes precisa ser ainda mais parcimonioso.

É certo que a utilização das novas tecnologias da informação e da comunicação promove uma série de descobertas em crianças e adolescentes, podendo estimular diversas experiências comunicacionais, educativas e de entretenimento em uma profusão de possibilidades jamais vista na história da humanidade.

Por outro lado, é bem certo também que o monitoramento das atividades on-line de crianças e adolescentes tem crescido sobremaneira, bem como as denúncias de coleta indevida de seus dados pessoais. Por isso, é importante que novas formas de fiscalização e monitoramento do tratamento de dados pessoais de crianças e adolescentes sejam implementadas, a fim de que regulações já existentes no que concerne à proteção dos direitos de crianças e adolescentes tenham a devida efetividade.

Nesse contexto, de suma importância é a absoluta proibição do direcionamento de publicidade a crianças e adolescentes, por conseguinte, a proibição do tratamento de seus dados pessoais com tal finalidade, ainda que haja consentimento parental expresso, por conta do melhor interesse das crianças.

Por esta razão, o tratamento de dados pessoais de crianças e adolescentes deve, impreterivelmente, coadunar-se com o direito fundamental da criança à absoluta prioridade de seus direitos e melhor interesse, cujo dever de ser assegurado é determinado de forma solidária ao Estado, sociedade, inclusive, empresas e famílias.

5. A RESPONSABILIDADE CIVIL NO PLANO DA PROTEÇÃO DE DADOS PESSOAIS

Para análise das nuances de responsabilidade civil na proteção de dados pessoais, fundamenta-se a necessidade de impedir os ganhos ilícitos do causador do dano na responsabilidade civil, razão pela qual se percorre as funções e as possibilidades do instituto. Antes de tratar da responsabilidade civil pelo ilícito lucrativo, abordam-se lições que possibilitam um caminho não unitário, ou melhor, permitem que dois remédios sejam aplicados isolada ou cumulativamente, conforme o caso.

Para isso, a responsabilidade civil pelo ilícito lucrativo não se utiliza da função punitiva, pois não agrava a situação patrimonial do lesante, apenas o devolve à situação anterior à prática do ilícito, removendo-lhe o proveito obtido. A partir da concepção da responsabilidade civil, tem-se a atribuição de consequência de indenização do dano àquele que o causa a partir de um ato ilícito, com o escopo de restabelecer equilíbrio violado, bem como o de prevenir novos atos ilícitos e evitar novos prejuízos.

Avança-se, destarte, na maleável capacidade de ressignificação da responsabilidade civil examinada para além dos requisitos. Se o instituto caminha para alcançar o objetivo de restabelecer o equilíbrio até com seus elementos intrínsecos, o que dirá de suas funções, com evolução coerente à sua adaptabilidade, mormente com os novos olhares.

Em verdade, não se pode mais conceber a responsabilidade civil com função única, acima de tudo na sociedade da informação. Aqui vale lembrar que a Lei Geral de Proteção de Dados Pessoais estabelece como princípio, em seu artigo 6º, inciso VIII, a prevenção (“adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais”). Nos tempos atuais, a velocidade não se coaduna com a responsabilidade civil estanque, porém com aquela que mantém sua essência e amplia seus horizontes, o que, na prática, contribui significativamente para que essa essência seja preservada.

Na perpectiva dos requisitos usuais da responsabibilização, não será tarefa fácil ao lesado provar o preenchimento dos três requisitos da responsabilidade civil – ilicitude, dano e nexo de causalidade. Nessa temática, há diversos autores que defendem que a LGPD estabelece a responsabilidade civil objetiva, verificável por falha no dever de segurança, com a obrigação aos agentes da chamada proatividade, em que há o comando de promover as atividades de tratamento de dados com mecanismos hábeis na preservação da segurança, a fim de evitar danos aos titulares de dados e a terceiros.

Em outra frente, diversos são os autores como Gisela Sampaio da Cruz Guedes e Rose Melo Vencelau Meireles (2020), que lecionam não fazer sentido o regime da responsabilidade civil independer de culpa, haja vista que, para as autoras, a Lei Geral de Proteção de Dados

Pessoais, estabelece a responsabilidade no caso de descumprimento de deveres e de desvio de padrão de conduta. Isso, segundo afirmam, afastaria a responsabilidade objetiva.

Noutro estudo, Alvino Lima pondera que tanto dano quanto reparação devem ser aferidos, não por medida de culpabilidade, mas, "*do fato causador da lesão de um bem jurídico, a fim de se manterem incólumes os interesses em jogo, cujo desequilíbrio é manifesto, se ficarmos dentro dos estreitos limites de uma responsabilidade subjetiva*"[105]. É o que a Lei Geral de Proteção de Dados Pessoais estabelece: reponsabilidade ao lesante.

Entendem, ainda, as referidas autoras que o inciso II do artigo 43 da Lei Geral não teria equivalência no Código de Defesa do Consumidor (artigo 12, § 3º, inciso II). No CDC, o fornecedor que colocou o produto no mercado de consumo, só não é responsabilizado se o defeito inexistir, ao passo que, na LGPD, o agente, tendo realizado o tratamento de dados, somente não é responsabilizado na ausência de violação à Lei.

Acrescente-se que a apresentada culpa como desvio de conduta pode ser enfrentada em paralelo com a boa-fé, porque, entre as funções da boa- fé objetiva, estão a de estabelecer padrão de conduta e a de impor limites ao exercício de direitos, mormente pela consideração de que, ao ultrapassar o limite, ocorre abuso de direito.

Por sua vez, *"a concepção adotada em relação ao abuso de direito é objetiva, pois não é necessária a consciência de se excederem, com o seu exercício, os limites impostos pela boa-fé"*[106], nos termos, inclusive, do Enunciado 37 da I Jornada de Direito Civil, pelo qual "a responsabilidade civil decorrente do abuso de direito independe de culpa e fundamenta-se somente no critério objetivo-finalístico".

Esse raciocínio é utilizado por Bruno Miragem em construção acerca do abuso de direito, para atestar a ilicitude objetiva em consonância com o direito contemporâneo, com atuação para limitar o exercício do direito subjetivo, independentemente de culpa, pela boa-fé, pelos bons costumes, bem como pela finalidade econômica e social.[107]

Em sua análise, Felipe Braga Netto denomina abuso de direito de ilícito funcional, aduzindo que a teoria objetiva finalista foi acolhida no Código Civil pelo artigo 187, tendo em vista que o abuso está no desvio da função social ou da finalidade do direito.[108]

Acredita-se, nesse cenário, que o inciso II do artigo 43, ao contrário do defendido por

---

[105] LIMA, Alvino. Culpa e Risco. 2 ed. São Paulo: Revista dos Tribunais. 1998, p. 115-116

[106] CAVALIERI FILHO, Sérgio. Programa de responsabilidade civil. 9. ed. São Paulo: Malheiros, 2010.

[107] MIRAGEM, Bruno. Diretrizes interpretativas da função social do contrato. Revista de. Direito do Consumidor, v. 56. São Paulo: RT, 2005, p. 133.

[108] BRAGA NETTO, Felipe Peixoto; DE FARIAS, Cristiano Chaves; ROSENVALD, Nelson. Novo Tratado de Responsabilidade Civil. – 4. Ed. – São Paulo: Saraiva Educação, 2019. p. 149.

Gisela Sampaio da Cruz Guedes e Rose Melo Vencelau Meireles, traz a exigência de um tratamento de dados conforme a Lei, sem desvios funcionais, de acordo com padrões reconhecidos como adequados.[109] A partir dessa conjuntura, os agentes não devem ser responsabilizados se agirem sem a prática de abuso de direito. Sendo assim, os argumentos das autoras servem, a contrário senso, não para justificar a responsabilidade subjetiva, mas para contribuir com a percepção de que se trata de responsabilidade objetiva.

Além das investigações referentes ao regime jurídico, outras questões atinentes à responsabilidade civil da LGPD revelam-se instigantes. A Lei Geral de Proteção de Dados Pessoais conta com uma seção específica para responsabilidade e ressarcimento de danos (Seção III do Capítulo VI). Entre as previsões ali inseridas, registra-se a responsabilidade solidária entre controlador e operador.

Com efeito, o artigo 42 da Lei disciplina que o controlador ou o operador que causar danos a outrem, em decorrência de atividade de tratamento de dados pessoais e *"em violação à legislação de proteção de dados pessoais",* deve reparar o dano. Ainda na cabeça do artigo, prevê-se que o dano pode ser patrimonial, moral, individual ou coletivo.

Já o parágrafo primeiro, busca assegurar efetiva indenização e, para tanto, prevê a responsabilidade solidária entre operador e controlador, sendo que este responderá solidariamente com aquele sempre que envolvido diretamente na atividade lesante, ao passo que o operador será solidariamente responsável quando deixar de seguir as lícitas instruções do controlador ou quando descumprir obrigação da legislação.

Vale dizer que o agente que vier a indenizar tem direito de regresso contra os demais responsáveis, nos termos do § 4º do artigo 42. Observa-se que o inciso I do § 1º do artigo 42, que trata da responsabilidade do operador, repete a cabeça do artigo nesse particular, pois determina que a responsabilidade de controlador ou operador se dará mediante dano a outrem, em atividade que viole a legislação de proteção de dados pessoais.

As disposições de solidariedade e direito de regresso também encontram eco no Regulamento europeu, que estabelece a responsabilidade de cada responsável *"pela totalidade de danos, a fim de assegurar a efetiva indenização do titular dos dados",* cabendo direito de regresso.

Acrescente-se outra semelhança na LGPD com o (ou inspiração no) Código de Defesa do Consumidor. Tal qual a norma de proteção do consumidor, estabeleceu-se a possibilidade

---

[109] GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, "Término do tratamento de dados", IN: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato. Lei Geral de Proteção de Dados Pessoais, Editora RT: São Paulo, 2019, p. 231.

de inversão do ônus da prova. Todavia, com uma diferença: enquanto no CDC a inversão do ônus está prevista como direito básico, sendo cabível em ações indenizatórias e além destas, a Lei Geral de Proteção de Dados Pessoais trouxe a referida possibilidade especificamente no campo da responsabilidade civil.[110]

Ao lado da inversão do ônus, o titular poderá buscar por informações diretas com o encarregado ou com o controlador, exigindo prestação de contas para tentar encontrar de onde partiu a violação, com base nos princípios (artigo 6º) da responsabilização e prestação de contas (inciso X) e da transparência (VI), pelo qual há a "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial". Repisamos que a teia interconectada da Lei contribui com sua efetividade.

Esse cenário promete debates quanto ao nexo de causalidade que, em geral, pode ser entendido como um elemento referencial entre a conduta e o resultado. Da mesma forma, para responsabilizar o agente de tratamento que violar a LGPD e causar danos, deve haver prova do nexo de causalidade, uma vez que a despeito da previsão de inversão do ônus da prova, esta não é automática e somente terá lugar quando presentes um dos alternativos requisitos do artigo 42, § 2º. E nisso reside um desafio.

Assim sendo, em casos que envolvam uma relação de consumo, a responsabilização é bastante ampla e a única alternativa de exoneração seria, em tese, o rompimento do nexo de causalidade, em situações como a culpa exclusiva do consumidor ou de terceiros. Outra característica relevante das relações de consumo é a inversão do ônus da prova. Isso significa que é responsabilidade do fornecedor comprovar que não houve o nexo de causalidade, e não do titular dos dados pessoais.

Dessa forma, embora a legislação não seja clara, é possível sustentar que se aplica a responsabilidade subjetiva na LGPD, na qual o elemento da culpa deverá ser demonstrado, admitida, em algumas hipóteses específicas, a responsabilidade objetiva, de acordo com a natureza da atividade de tratamento realizada. Ressalta-se que, independentemente da responsabilidade subjetiva ou objetiva, é requisito para qualquer indenização a efetiva demonstração do dano. Seguindo a mesma dinâmica, não havendo demonstração do dano, não será procedente o pedido pela via judicial.

A este respeito Maria Candida do Amaral Kroetz defende a viabilidade de soluções variadas para o caso, vejamos:

---

[110] MAIMONE, F. H. C. d. P; RESPONSABILIDADE CIVIL NA LGPD: EFETIVIDADE NA PROTEÇAO DE DADOS PESSOAIS. 1. ed. Indaiatuba, SP.: Foco, 2021. p. 1-128.

> **a)** quando a intervenção é culposa e causa um dano cujo montante é superior ao lucro obtido, aplicam-se as regras da responsabilidade civil e a questão do lucro por intervenção perde o interesse, porque o lucro é absorvido pelo montante da indenização a ser paga; **b)** quando a intervenção não é culposa e implica a realização de um lucro, este deve ser restituído com base nas regras do enriquecimento sem causa; **c)** quando a intervenção é culposa mas não causa danos ou causa dano num montante inferior ao lucro obtido, é necessário mesclar as regras da responsabilidade civil e do enriquecimento sem causa para possibilitar o total equacionamento da questão (Kroetz, 2005, p. 161).

Portanto, ainda que sejam aprofundados os estudos alusivos ao enriquecimento sem causa, continua-se a enxergar a responsabilidade civil como remédio para tais casos. A responsabilidade civil, efetivamente, é a porta procurada quando há presença de conduta antijurídica a causar dano, sendo que a razão de ser do instituto é atuar no equilíbrio, tanto para as hipóteses de restabelecimento, de mesmo modo para sua preservação. Talvez por isso haja constante evolução na responsabilidade civil, sobre a qual jurisprudência e literatura jurídica debruçam-se cotidianamente.

Na lição de Rosenvald, o direito, por sua vez, pode ir além, *"transcendendo a epiderme do dano, para alcançar o ilícito em si, seja para preveni-lo, remover os ganhos indevidamente dele derivados ou, em situações excepcionais, punir comportamentos exemplarmente negativos"*; o olhar ultrapassaria, então, a vítima e o objetivo de promover o retorno desta ao estado anterior ao dano. Não obstante, mostra-se a necessidade da mudança de paradigmas como um fator importante da perspectiva após o fato para a anterior, focada em prevenir e modificar comportamentos não tem exatamente essa ideia, mas a de alterar no "campo do incentivo à criação de remédios adicionais *post-facto*, no interno da justiça corretiva, que permitam a remoção ou a restituição de benefícios ilícitos".[111]

A verificação de aspectos da responsabilidade civil contribui com a pretensa investigação, para se ratificar o liame do instituto seja com o dano, seja com o ilícito. Com efeito, a responsabilidade civil leva à reparação do dano aquele que o causa a partir de um ato ilícito, com o escopo de restabelecer o equilíbrio violado, bem como de prevenir outros atos ilícitos causadores de novos prejuízos.

Efetivamente, "a responsabilidade civil consiste justamente na imputação do evento

[111] MAIMONE, F. H. C. d. P; RESPONSABILIDADE CIVIL NA LGPD: EFETIVIDADE NA PROTEÇAO DE DADOS PESSOAIS. 1. ed. Indaiatuba, SP.: Foco, 2021. p. 1-128.

danoso a um sujeito determinado, que será, então, obrigado a indenizá-lo".[112] Há, assim, a perspectiva de a centralidade da responsabilidade civil ser o dano. Nesse sentido, segue o parecer de Ana Cláudia Côrrea Zuin Mattos do Amaral e Everton William Pona: *"num processo de antecedência lógica, eliminando-se o dano, desconfigura-se qualquer dever de indenizar. A ocorrência de danos gera instabilidade e provoca desequilíbrios na economia e na sociedade".*[113]

Com efeito, a responsabilidade civil almeja ao reequilíbrio, impondo o dever de indenizar pelo dano causado, considerando que "alguém civilmente responsável terá de indemnizar o lesado pelo dano causado. Indemnizar é, assim, tornar alguém indemne, isto é, sem danos. O dano constitui, simultaneamente, o pressuposto e o limite da indemnização".[114] Há, todavia, aparente paradoxo em oferecer ao dano (como pressuposto) o cerne da responsabilidade civil, sobretudo quando se pretende examinar a remoção do ganho ilícito, cujo eixo não é a vítima, mas sim o ofensor, aquele quem detém o ganho. De fato, trata-se exatamente disso: um aparente paradoxo, eis que os esforços para devolver a vítima à situação anterior ao dano mostram-se insuficientes para inibir condutas lesivas e, pois, para evitar o dano.

No decorrer da história, foram conferidas à responsabilidade civil funções variadas, mas correlatas*: "punir um culpado, vingar a vítima, indenizar a vítima, restabelecer a ordem social e prevenir comportamentos antissociais"*.[115] Fica evidente, diante disso, que a responsabilidade civil se reveste de adaptabilidade para cumprir seu propósito. Ademais, a realidade contemporânea está redimensionando-a como remédio ou "como instrumento de tutela dos direitos inerentes à pessoa e não apenas voltado à recomposição do patrimônio ou ao seu equivalente por meio da indenização".[116]

Vale mencionar que a incidência da Constituição, com os princípios da dignidade da pessoa humana e da solidariedade social, influencia e ilumina a responsabilidade civil. Nessa ordem de ideias, a dignidade humana, e sua cláusula irmã que postula o livre desenvolvimento da personalidade humana, além da solidariedade social, devem iluminar a solução de

---

[112] BODIN DE MORAES, Maria Celina. A caminho de um direito civil constitucional. in: Revista de Direito Civil, Imobiliário, Agrário e Empresarial, v. 17, n. 65, jul./set. de 1993, pp. 239.

[113] AMARAL, Ana Cláudia Corrêa Zuin Mattos do Amaral ; PONA, Everton Willian. . Autonomia da vontade privada e testamento vital: possibilidade de inclusão no ordenamento jurídico brasileiro. Revista do Direito Privado (Londrina) , v. I, p. 1-29, 2008.

[114] MONTEIRO, António Pinto. Cláusula Penal e Indemnização. Coimbra: Almedina, 2014, pg. 92.

[115] PÜSCHEL, Flavia Portella. Funções e princípios justificadores da responsabilidade civil e o art. 927, § único do Código Civil. In: Revista DIREITO GV 1 (2005), p. 91-107.

[116] VENTURI, Thaís Goveia Pascoaloto. Responsabilidade civil preventiva. A Proteção contra a Violação dos Direitos e a Tutela Inibitória Material. São Paulo: Malheiros, 2014.

controvérsias no direito dos danos do século XXI.

De fato, a defesa de inalterabilidade das funções da responsabilidade civil não se coaduna com sua capacidade de acompanhar as mudanças da sociedade e, por consequência, de conseguir se manter como remédio adequado para promover a harmonização social. A partir desse pressuposto, ou seja, de que a responsabilidade civil não tem funcionalidade estanque, deve-se perseguir o trilho em exame para incluir a remoção dos ganhos ilícitos com coerência no interno da responsabilidade civil. Portanto, as funções da responsabilidade civil modificam-se e atualmente agregam à função reparatória e compensatória as funções preventiva e dissuasória, e até mesmo a função punitiva. Tudo para garantir o acolhimento ressarcitório à vítima e ampliar a coesão social pela adequada gestão do risco.

De fato, acredita-se nessa tendência do campo da probabilidade para se declarar presente o nexo causal. Sendo assim, pondera-se que o ônus da prova da causalidade "é claramente facilitado para a vítima, que não precisa provar todos os elos da cadeia de causalidade se os tribunais aceitarem que um determinado resultado é o efeito típico de um certo desenvolvimento nessa cadeia".[117]

Ademais, devemos ter em mente que, além da inversão do ônus da prova a cargo do magistrado, tem-se a imposta pela LGPD, uma outra maneira para facilitar a carga probatória destinada ao lesado. A Lei Geral impõe que os agentes de tratamento apenas deixarão de ser responsabilizados quando eles próprios provarem (artigo 43): I – Que não realizaram o tratamento de dados pessoais que lhes é atribuído; II – que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

Essas situações excluiriam o nexo causal (incisos I ou III) ou a ilicitude (inciso II) e, por conseguinte, o dever de indenizar. Resta saber como a responsabilidade civil poderá cumprir os propósitos da Lei Geral. Para tanto, examinaremos se a indenização restitutória, com a remoção dos lucros indevidos dos ofensores, transferindo-os aos lesados, é o remédio apropriado.

Efetivamente, não se pode mais conceber a responsabilidade civil com função única, mormente na sociedade da informação, cabendo lembrar que a Lei Geral de Proteção de Dados

[117] CORONAVÍRUS E RESPONSABILIDADE CIVIL. IMPACTOS CONTRATUAIS E EXTRACONTRATUAIS. MONTEIRO FILHO, CARLOS EDISON DO RÊGO. ROSENVALD, NELSON. DENSA, ROBERTA. (COORDS.) 2ª ED. SÃO PAULO: FOCO, 2021 – P. 139-160]

Pessoais estabelece como princípio, no artigo 6º, inciso VIII, a prevenção, prescrevendo a *"adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais*". A velocidade destes tempos não se coaduna com instituto estanque, mas com aquele que mantém a essência e amplia seus horizontes. A bem da verdade, a ampliação contribui significativamente para que a essência da responsabilidade civil seja preservada. Com a finalidade de verificar a multiplicidade funcional desse instituto, é importante proceder uma particularizada menção de suas funções.

5.1. A função reparatória da responsabilidade civil na tutela dos dados pessoais

A função reparatória é a função clássica da responsabilidade civil, representada pela reparação do dano. Por meio dessa atribuição, o lesante é obrigado a promover o restabelecimento da vítima às condições anteriores à lesão e, na impossibilidade, compensá-la pelo prejuízo causado. Cumpre-se, portanto, a função reparatória com o ressarcimento do dano material e a compensação do dano imaterial.

Afirma-se, nessa seara, que tal reparação seria crucial à responsabilidade civil, que visa a apagar o prejuízo econômico causado (indenização do dano patrimonial), minorar o sofrimento infligido (satisfação compensatória do dano moral puro) ou compensar pela ofensa à vida ou à integridade.

Ao investigar o dano moral no direito do consumidor, Héctor Valverde Santana[118] menciona a função de ressarcimento do dano patrimonial, pela qual se almeja retificar a diminuição patrimonial derivada da lesão para promover o retorno do lesado ao estado anterior ao dano. Já a compensatória seria exclusiva função do dano moral, revelada pela lesão, privação ou violação de direitos da personalidade, o que pode se cogitar a hipótese de um desvio produtivo do consumidor em razão do uso de dados.

A função reparatória ressarcitória, de danos patrimoniais e compensatória, de imateriais – pode ser identificada e justificada mais facilmente. Por isso, é dita clássica e até fundamental. Revela-se como a tentativa de pronta resposta ao lesado e, nesse aspecto, tem seu inegável mérito, restando difícil conceber responsabilidade civil sem essa função. Não acreditamos tratar-se de função única, mas reconhecemos a dificuldade de vislumbrar a responsabilidade civil sem a função reparatória, à qual se soma a punitiva.

---

[118] SANTANA, Hector Valverde. Dano moral no direito do consumidor. 1. ed. São Paulo: Revista dos Tribunais, 2009. v. 1000. 269p.

5.2. A função punitiva da responsabilidade civil na tutela dos dados pessoais

No inverso da lógica reparatória, a função punitiva é alvo de grande inquietação nos tribunais e na literatura. Afinal, se a vítima já teve o dano reparado e compensado, questiona-se por que razão se deveria atribuir outra função à responsabilidade.

No entanto, Filipe Albuquerque Matos (2017, p. 47-48), examinando a compensação por danos extrapatrimoniais no Código Civil de Português, aduz que a vertente punitiva é inquestionável no que se refere à compensação de danos imateriais. O autor afirma que *"a compensação dos danos não patrimoniais, vai proporcionar à lesado certa satisfação, havendo mesmo quem nesta sede considere que nos encontramos perante uma pena privada"* em benefício do lesado.

Da mesma forma, Maria Celina Bodin de Moraes (2017, p. 263) admite a função punitiva como exceção e acredita (2017, p. 217-227) que *"a solução que se apresenta mais condizente com o instituto da pena privada, ou do caráter punitivo, na responsabilidade civil é normatizar"* para aclarar e determinar com segurança qual seriam as situações a ensejar a punição. De fato, como a jurisprudência é firme ao asseverar "a importância de punir o ofensor e coibir a repetição da conduta, tal função poderia ser mais bem alcançada mediante a condenação do ofensor ao pagamento de parcela autônoma" (MARINHO, 2018, p. 658). Já Caroline Vaz (2009, p. 170) vislumbra a função punitiva no sistema jurídico brasileiro com pertinência e compatibilidade.

Igualmente defensor da função punitiva, Nelson Rosenvald (2017, p. 340) afirma encontrar exigência no campo dos direitos da personalidade para ser estabelecida pena civil, dado que o Código Civil, em seu artigo 12, disciplina a admissibilidade tanto de fazer cessar ameaça e lesão a direito da personalidade, quanto de *"reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei".* Aproveita-se o mesmo dispositivo legal citado, em sua primeira parte, para vislumbrar a função preventiva, já que impõe que se faça cessar, não apenas a lesão, mas também – a ameaça a direito da personalidade.

5.3. A função preventiva da responsabilidade civil na tutela dos dados pessoais

Além de estar presente no artigo 12 do Código Civil, a função preventiva está constitucionalmente assegurada como direito fundamental, uma vez que o artigo 5º, inciso XXXV, da Constituição Federal estabelece *que "a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito".*

Há, por assim dizer, imperativo legal e constitucional para que se proceda à prevenção de dano, o que se extrai – infraconstitucionalmente da determinação de fazer cessar a ameaça de lesão a direito da personalidade e da Constituição, que estabelece o direito fundamental de garantir que o cidadão se socorra do Estado, em sua função jurisdicional, diante de *"ameaça a direito".* A seu turno, Nelson Rosenvald reconhece a função preventiva como anterior às demais funções, considerando, entretanto, a prevenção como princípio. Para o autor, *"a prevenção detém inegável plasticidade e abertura semântica, consistindo em uma necessária consequência da incidência das três funções (reparatória, punitiva e precaucional)",* sendo que a precaucional seria aquela com *"o objetivo de inibir atividades potencialmente danosas".*

Na Lei Geral de Proteção de Dados Pessoais, está positivado o princípio da prevenção (artigo 6º, inciso VIII: "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais"), ao lado do princípio da responsabilização e prestação de contas (artigo 6º, inciso X: "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas"). Anote-se que, no mesmo sentido, o Código de Defesa do Consumidor estabelece como direito básico do consumidor a prevenção de danos (artigo 6º, inciso VI: *"a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos").*

Assim, citados diplomas legais trazem textual previsão da prevenção de danos, o que nos leva a concluir que a função preventiva está presente em todo sistema jurídico brasileiro – nas relações de consumo e naquelas sobre as quais incide a LGPD. Dessa maneira, a função preventiva decorre, mais do que de interpretação da responsabilidade civil, da positivação de seus dispositivos. Exatamente aqui, no aspecto preventivo, somado ao reparatório, é que se ofereceria guarida à responsabilidade civil pelo ilícito lucrativo.[119]

Com o breve exame da responsabilidade civil, pode-se avançar no foco de incluir a restituição dos lucros ilícitos no interno desse instituto, com base em suas funções compensatória e preventiva. Começamos pelos empecilhos: a literatura jurídica reconhece a situação em que se verifica a presença do ilícito, bem como que dele adveio lucro ao infrator, porém sem dano, o que afasta a responsabilidade civil.

Ademais, "*o interesse em restabelecer o equilíbrio econômico-jurídico alterado pelo dano é a causa geradora da responsabilidade civil"* (DIAS, 2011, p. 43). Assim, deve-se questionar a manutenção do resultado do ilícito lucrativo em posse do ofensor, cuja conduta

[119] MAIMONE, F. H. C. d. P; RESPONSABILIDADE CIVIL NA LGPD: EFETIVIDADE NA PROTEÇAO DE DADOS PESSOAIS. 1. ed. Indaiatuba, SP.: Foco, 2021. p. 1-128.

estaria também mantendo um desequilíbrio justamente em favor do agente causador do ato ilícito, do responsável pela causação do dano, da violação a direitos alheios, da violação da confiança.

Noutras palavras, para que seja restabelecido equilíbrio econômico- jurídico, mostra-se adequada a remoção dos ganhos obtidos ilicitamente, devolvendo o agente causador do dano ao estado em que ele – lesante – estava antes do dano para, de fato, haver equilíbrio. Isso seria coerente, porque não parece equilibrado o caso de o agente causador do dano – tendo obtido ganhos indevidos – manter-se com o resultado do ilícito (ROSENVALD, 2017, p. 243).

O que não se pode admitir é o olhar estanque para um princípio da responsabilidade civil, utilizando-o na contramão da essência do próprio instituto. Se há autorização legal para alterar a indenização para aquém do dano em si, mormente diante de prejuízo de direitos patrimoniais e da personalidade, é razoável atribuir bilateralidade à exceção legal, haja vista o objetivo de a majoração ser totalmente conforme o Direito, possibilitando a repressão do ilícito e não permitindo ao ofensor beneficiar-se da própria torpeza.

A verdade é que, quando a quantia da indenização não é majorada nesses termos, não há harmonização ou equilíbrio restabelecido. Admitir ao ofensor que se beneficie de sua torpeza, não está de acordo com o Direito, pois não promove a pacificação social. A responsabilidade civil, portanto, é instituto a cumprir o intento de corrigir o indevido uso do Direito contra si mesmo, e pode, por conseguinte, ser o instrumento para buscar a restituição do ilícito lucrativo, sempre que preenchidos seus pressupostos.

Chama atenção, nesse ponto de vista, a presença da reponsabilidade civil em casos que geram lucros ilícitos, dada a verificação de conduta antijurídica, de dano e de nexo causal. Presentes os elementos ou requisitos, está caracterizada a responsabilidade civil. A crítica que se verifica, na prática, é ao montante, à possibilidade de quantificação do dano alcançar os lucros ilícitos quando superiores ao prejuízo, enfrentando os limites da extensão desse dano. Isso levaria a responsabilidade civil para uma hipotética insuficiência nos casos em que o lucro obtido pelo ofensor com o ilícito superasse o dano do lesado. Tal questionamento pode ser visto tanto em estudos realizados por adeptos do lucro da intervenção no interno do enriquecimento sem causa, quanto naqueles que comungam com a internalização na responsabilidade civil.

Em suma, a questão cinge-se à quantificação do dano e à (im)possibilidade de incluir o ilícito lucrativo quando em montante além do prejuízo. As funções da responsabilidade, sobretudo a reparatória em consonância com a preventiva, contribuem nesse desiderato de remover o ganho ilícito, desestimulando o infrator.

Por fim, deve-se olhar para o instituto sob a ótica dos remédios, isto é, instrumentos de

tutela de direitos e interesses jurídicos. Esse caminho, de fato, parece oportuno quando se investiga responsabilidade civil na Lei Geral de Proteção de Dados Pessoais, que enuncia remédios a serem utilizados para eventuais violações normativas, entre os quais a responsabilidade civil pelo ilícito lucrativo, na forma de indenização restitutória.

5.4. Perspectiva de uma função promocional e preventiva da responsabilidade civil no âmbito da Lei Geral de Proteção de Dados Pessoais no Brasil

Com efeito, não é a primeira vez que se argumenta que a responsabilidade civil deve cumprir com uma função promocional. Ilustrativamente, já há respeitáveis registros, inclusive com alusão à perspectiva funcional do direito atribuída a Bobbio, de que "os danos morais devem assumir sua função promocional para maximizar a proteção da pessoa humana".[120]

Ou mesmo que a função promocional da responsabilidade civil deve atuar como forma de premiar a "diligência extraordinária" de um agente econômico com a "exclusão de uma sanção punitiva (a privação de uma desvantagem)", de modo a beneficiar aqueles que atuam "no sentido de não medir esforços para mitigar a possibilidade de causação de danos a terceiros", cogitando-se a "criação de uma espécie de cadastro positivo de louváveis agentes econômicos em todos os setores da atividade econômica (...) capaz de gerar uma percepção positiva da sociedade em termos de imagem, com reflexos patrimoniais e morais para as empresas".[121]

Contudo, não obstante as elogiáveis construções em torno do conceito, crê-se que tais perspectivas não representam o melhor ponto de vista sobre o problema. É por essa razão que se faz necessário, de modo inaugural, que se apresente a noção que aqui se entende mais precisa de função promocional da responsabilidade civil, esclarecendo o que é e o que não é função promocional no âmbito do direito dos danos, bem como a sua real extensão. Para isso, mais uma vez se ancorará no marco teórico de Norberto Bobbio e em sua proposta de sistematização das chamadas sanções positivas, neste caso orientadas à responsabilidade civil.

5.4.1. A função preventiva e o princípio da precaução

A diluição da doutrina da responsabilidade civil preventiva (ou com função preventiva)

---

[120] RODRIGUES, Francisco Luciano Lima; VERAS, Gésio de Lima. Dimensão funcional do dano moral no direito civil contemporâneo. Civilistica.com. Rio de Janeiro, a. 4, n. 2, 2015, p. 18. Disponível em: http://civilistica.com/ tra-cos-sitivis-tas-das-teo-rias-pontes-de-miranda/.randa/. Acesso em: 11 jan. 2018.

[121] ROSENVALD, Nelson. As funções da responsabilidade civil, cit., p. 161.

é tamanha que não é incomum deparar-se o leitor com a defesa do chamado princípio da prevenção ou princípio da precaução.[122]

Costuma-se defender a natureza de princípio à prevenção e à precaução, tanto em razão de seu caráter genérico e abstrato, que agrega conteúdo de valor e fundamento do sistema da responsabilidade civil, como pelo seu caráter normativo, cujo descumprimento atrairá a reação sancionatória do direito.[123] Como "mandamento de otimização",[124] também há quem defenda a natureza principiológica da prevenção e da precaução, na medida em que "realiza os valores do neminem laedere, da prudência e da segurança (outro princípio) e estabelece diretrizes normativas para que o pior não aconteça individual e socialmente".[125] Em derradeiro, por não conviver como as regras, cujo sentido é antinômico, mas como princípios, em ambiente conflituoso perene, em busca da constante harmonização e ponderação, não ignora o fato de que há outros princípios em jogo que devem ser sopesados, sobretudo o da livre iniciativa.[126]

Oferecer um conceito de princípio é desafiador. Mesmo porque reflete realidades jurídicas múltiplas, não havendo equívoco, inexatidão ou contrariedade entre as mais variadas concepções. É que o próprio ordenamento positivo, a depender do desafio que propõe superar e do locus de sua atuação, apresenta uma ideia de princípio não necessariamente condizente com outra apresentada sob contexto normativo diverso. Portanto, mesmo o conteúdo normativo dos princípios não escapa à interpretação funcional.[127]

Do ponto de vista hermenêutico, podem-se aplicar princípios para integrar o conteúdo normativo de texto legal, cujo "tipo" apresenta "lacuna" ou "vácuo", no sentido de não ter

---

[122] VINEY, Geneviève. Traité de droit civil: introduction à la responsabilité, cit., p. 155-158; KOURILSKY, Philippe. Du bon usage du principe de précaution. Paris: Ed. Odile Jacobs, 2001, passim; ROBINEAU, Matthieu. Contribuition à l'ètude du système responsabilité: les potentialités du droit des assurances. Paris: Defré- nois, 2006, n. 214; PERLINGIERI, Pietro. Manuali di diritto civil, cit., p. 897; BI- ANCA, Massimo. Diritto civile, cit., p. 553-557; ALPA, Guido; BESSONE, Mario. La responsabilità civile, cit., p. 171-198; FRANZONI, Massimo. Trattato della respon- sabilità civile, v. II, cit., p. 733-756; BATTAGLIA, Franco; ROSATI, Angela. I costi della non scienza: il principio di precauzione. Milano: 21mo Secolo, 2004, passim, entre tantos outros.

[123] Sobre o "papel normativo da responsabilidade civil" (le rôle normatif de la responsabilité), cf. VINEY, Geneviève. Traité de droit civil: introduction à la res- ponsabilité, cit., p. 86 e ss. Acerca das mais diversas conotações sobre o desig- nativo "princípio", cf. ALPA, Guido. I principi generali. Milano: Giuffrè, 1993, p. 6-7.

[124] ALEXY, Robert. Teoría de los derechos fundamentales [1986]. Trad. Ernesto Valdés. Madrid: Ed. Alemana, 1993, p. 87.

[125] LOPEZ, Teresa Ancona. Princípio da precaução e evolução da responsabilidade civil, cit., p. 95.

[126] A aplicação do chamado princípio da precaução exigiria ponderação cons- tante com a realidade da atividade desenvolvida pelo agente, a fim de encontrar a justa medida, sem que determinadas atitudes de precaução sejam exigidas de modo desnecessário, causando pânico social ou bloqueando a inovação tecno- lógica. Neste sentido, LOPEZ, Teresa Ancona. Princípio da precaução e evolução da responsabilidade civil, cit., p. 96

[127] Certo é, apenas, que já se encontra superada toda e qualquer conotação que se pretende atribuir a princípios, no sentido de que seriam meras diretrizes mo- rais, extra ou metajurídicas. Já é lugar comum admitir que todo princípio tem força normativa. Cf. BARROSO, Luis Roberto. O direito constitucional e a efeti- vidade de suas normas: limites e possibilidades da Constituição brasileira. 2. ed. Rio de Janeiro: Renovar, 1993; BONAVIDES, Paulo. Curso de direito constitucional. 31. ed. São Paulo: Malheiros, 2016.

conseguido prever consequências jurídicas para alguns comportamentos juridicamente relevantes.[128] Porém, na realidade, faz-se mais: aplicam-se princípios do ordenamento positivo (categoria mais formal que os chamados "princípio gerais do direito"), como elemento integrante essencial a toda e qualquer operação hermenêutica.

Eis a vertente do princípio como valor de conteúdo normativo, de conteúdo aberto, ainda que identificado no ordenamento positivo. Todavia, orientado como mandamento de otimização, diante dos avanços da tecnologia ocorridos no século XX, fala-se sobre o fim da privacidade, que visa demonstrar a impossibilidade de se preservarem fatos e elementos da esfera privada diante do enorme fluxo informacional proporcionado pelas novas tecnologias. Na obra *"A era da informação: economia, sociedade e cultura"* de Manuel Castells, que defende que está em curso uma verdadeira revolução tecnológica, cujo núcleo se refere às tecnologias da informação, processamento e comunicação.

5.4.2. Distinções entre a função reparatória, preventiva e promocional

A função reparatória ou compensatória já foi amplamente exposta. O seu pressuposto é a ocorrência de dano. Caracteriza-se, fundamentalmente, pela perseguição de escopo material, ou substancial, no sentido de reequilibrar a relação jurídica abalada pela ocorrência da lesão a determinado interesse (ou feixe de interesses) juridicamente protegido.

Atende à finalidade primária da responsabilidade civil, da qual esta não cogita desvincular-se. Intenta recompor a situação patrimonial prejudicada indevidamente, ou compensar o abalo existencial injustamente imposto à vítima. A tal desiderato, estrutura-se de maneira a garantir, em regra, a reparação integral.

Organiza-se mediante a previsão de sanções negativas, naturalmente apresentadas como reação ao dano causado, constituindo-se em perfeita medida representativa de uma ordem jurídica coercitiva. A função promocional da responsabilidade civil, por sua vez, é aquela que visa a proporcionar um ambiente ético que estimule as partes, sobretudo o agente ofensor, a

[128] Ainda vigente o art. 4º do Decreto-lei 4.657/42 (Lei de Introdução às Normas do Direito Brasileiro), segundo o qual "quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais do direito". Importante salientar, de todo modo, que a ausência de omissão da lei não im- plica afirmar que princípios não serão aplicados na operação hermenêutica, mas apenas que não se recorrerá ao conteúdo específicos dos chamados "princípios gerais do direito", que representam cláusula geral valorativa do ordenamento jurídico. No fundo, partindo-se da premissa de que não há texto legal perfeito – de significado unívoco –, revelando-se falacioso o culto à máxima "*in claris fit interpretatio*", considerando toda operação interpretativa como fenômeno unitário, contém nela o momento "integrativo", onde a analogia, os costumes e os princípios gerais do direito contribuirão para ao alcance do significado norma- tivo do caso concreto. Cf. TEPEDINO, Gustavo. Normas constitucionais e di- reito civil na construção unitária do ordenamento. Temas de direito civil. Rio de Janeiro: Renovar, 2009, v. 3, p. 3-19.

reparar ou compensar espontaneamente os danos causados. Pressupõe, assim como a função reparatória, a ocorrência de dano.

Entretanto, caracteriza-se, essencialmente, pela perseguição de escopo instrumental, ou procedimental, no sentido de apresentar meios de estímulos a práticas de condutas desejadas, que se revelam a partir da materialização de comportamentos dos agentes que buscam a recomposição espontânea dos danos, em realização a valores fundamentais do ordenamento, especialmente a solidariedade, conferindo-lhe eficácia e concretude.

Atende à finalidade última da responsabilidade civil, como último nível da escada civilizatória, cujo ordenamento positivo atual já apresenta soluções. Mostra-se como construção teórica realista e amparada no primado da praxe, no sentido de que não existe ordem social perfeita. Ao desiderato perseguido, estrutura-se de maneira a garantir a reparação suficiente, propondo, assim, uma ressignificação do papel da reparação integral.

Organiza-se mediante a previsão de sanções positivas, premiando o devedor (agente causador do dano) pela resposta concreta, eficaz e eficiente à lesão causada, satisfazendo plenamente o interesse do credor (vítima).[129] Por seu turno, a função preventiva da responsabilidade civil também já foi suficientemente debatida.

O seu pressuposto de atuação é a realização, por parte de certos agentes, de atos ou atividades que produzam riscos de danos. Caracteriza-se, assim, pela perseguição de intencionalidade atuante sobre o comportamento dos agentes que, eventualmente, podem causar danos a outrem.

Atende à finalidade reflexa da responsabilidade civil, no sentido de que a prevenção do dano é o reflexo natural da rejeição que a ordem jurídica impõe sobre a realização de lesões a interesses juridicamente protegidos, tendo como finalidade primária a reparação dos danos e finalidade reflexa – e até anterior, cronologicamente – a prevenção aos comportamentos lesivos.

Intenta prevenir a sua ocorrência, evitando ao máximo a exposição ao risco, pelo controle prévio dos comportamentos. A tal desiderato, estrutura-se de maneira a garantir, em regra, a incolumidade das pessoas e bens alheios. Pode-se organizar-se mediante a previsão de sanções negativas, como reação ao dano causado (penas civis), extraindo daí um perfil coercitivo, ou por via de sanções positivas, com estipulação legal e prévia de prêmios ou

[129] Acerca de uma nova ideia de "satisfação" da vítima, superando a ideia da reparação patrimonial integral e da "compensação financeira" por obtenção de execução de obri- gações e meios outros que sejam suficientes para "restabelecer a legalidade", leciona Geneviève Viney que "l'évolution des idées sur la responsabilité civile a fait apparaître d'autres perspectives qui conduisent à assigner également à cette institution des objectifs nettement distincts de la réparation, même entendue de plus largement possible. (...) soit même afin d'obtenir l'exécution des obligations ou , plus largement, le rétablisseent de la légalité" (Traité de droit civil: la responsabilité – effets, cit., p. 4-5).

benesses pela prática reiterada de comportamentos preventivos esperados e exigidos pela ordem jurídica.[130]

Como esta última forma de concretização da função preventiva é de sua natureza, crê-se que não é correto identificar nela uma função autônoma, a denominar-se função promocional. Sedimentadas as funções que a responsabilidade civil brasileira persegue, passa-se, então, a demonstrar quais os instrumentos já previstos na ordem jurídica positiva que revelam a existência e a plena possibilidade de concretização da inovadora função promocional da responsabilidade civil.

Nesta investigação, preferiu-se optar por classificação que distingue uma medida de cunho processual das demais possibilidades materiais de identificação do perfil funcional promocional. Inicia-se pela primeira.

5.4.3. A função promocional nos danos individuais nas relações de consumo

Mesmo o Código Civil – norma geral a qual normalmente, e por equívoco, diz-se aplicado a relações paritárias – prevê que a autonomia privada pode ser unilateralmente reduzida em certos tipos de relações jurídicas.[131]

São aquelas nas quais não há paridade de armas na negociação, vale dizer, inexiste equivalência no exercício da autonomia privada por parte dos interessados. De um lado, figura uma parte designada de proponente, ou estipulante, em situação de plena liberdade contratual, que pré-estabelece os termos do acordo, de forma unilateral. De outro, aquele que só "adere" às cláusulas pré-formuladas, chamado de aderente, exercendo sua autonomia até certo ponto, na medida em que não contribui na conformação de seu conteúdo.

A este acordo de vontades desiguais, qualifica-se o contrato de adesão.[132] Contudo, a maior parte dos contratos de adesão são firmados no ambiente das relações de consumo, tendo o Código de Defesa do Consumidor (Lei n. 8.078/90) definido o negócio como "aquele cujas cláusulas tenham sido aprovadas pela autoridade competente ou estabelecidas unilateralmente pelo fornecedor de produtos ou serviços, sem que o consumidor possa discutir ou modificar

[130] "As sanções preventivas subdividem-se, em virtude dos mecanismos através dos quais atuam e dos seus objetivos específicos, em providências de (i) controle, (ii) encorajamento, (iii) intimidação e de (iv) preclusão" (TAMALINI, Eduardo. Tutelas relativas aos deveres de fazer e de não fazer e sua extensão aos deveres de entrega das coisas..., cit., p. 175-176)

[131] Prevê o art. 423 do Código Civil que, "quando houver no contrato de adesão cláusulas ambíguas ou contraditórias, dever-se-á adotar a interpretação mais favorável ao aderente", bem como o art. 424, o qual estipula que "nos contratos de adesão, são nulas as cláusulas que estipulem a renúncia antecipada do aderente a direito resultante da natureza do negócio".

[132] ROPPO, Enzo. O contrato, cit., p. 311-312.

substancialmente seu conteúdo" (art. 54, caput).

Ademais, destaca-se que: (i) na norma geral, há previsão de que "são nulas as cláusulas que estipulem a renúncia antecipada do aderente a direito resultante da natureza do negócio" (art. 424 do Código Civil); (ii) nas relações de consumo, prescreve-se que as cláusulas que implicarem "limitação do direito do consumidor deverão ser redigidas com destaque permitindo sua imediata e fácil compreensão" (art. 54, § 4º do Código de Defesa do Consumidor), sendo nulas de pleno direito quaisquer cláusulas contratuais relativas ao fornecimento de produtos ou serviços, que "impossibilitem, exonere ou atenue a responsabilidade do fornecedor de serviços por vícios de qualquer natureza dos produtos ou serviços ou que impliquem renúncia ou disposição de direitos" (art. 51, I do Código de Defesa do Consumidor), ou "estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada, ou sejam incompatíveis com a boa-fé ou a equidade".

Por fim, é um direito básico do consumidor a efetiva prevenção e reparação de danos materiais e morais, individuais, coletivos e difusos (art. 6º, VI do Código de Defesa do Consumidor). Pelo conjunto normativo, poder-se-ia imaginar que a transação é instrumento inviável ou inadequado para concretizar a função promocional no âmbito das relações de adesão, ou nas relações de consumo. É que a mínima unidade de efeitos do instrumento transacional pressupõe que os interessados realizem "concessões mútuas", o que inexoravelmente implicará na redução das situações jurídicas ativas da vítima, relativizando a reparação integral, por meio de cláusulas que limitam (rectius: reduzem) a responsabilidade do agente. Seria, assim, incompatível a utilização da transação nas relações não paritárias.

Sucede que não é essa a interpretação que merece prevalecer. Por variadas razões, aqui se defende que a transação é instrumento útil e eficaz, mesmo nas hipóteses de relações de adesão e de consumo.

Em primeiro lugar, como outrora elucidado, o contrato de transação não se confunde com a renúncia. Quando as partes abrem mão, ou aceitam reduzir proporcionalmente, algumas de suas situações jurídicas ativas, com a aquisição de outras vantagens em contrapartida, é equivocada toda e qualquer referência à renúncia, ainda que parcial, na medida em que esta se qualifica como "ato jurídico pelo qual o titular de um direito extingue-o em decorrência de sua própria vontade".[133]

[133] Ainda, "sua prática compete exclusivamente ao titular do direito e seus efeitos decorrem da lei, inclusive no plano da incidência destes em relação a outros sujeitos de direito" (TEPEDINO, Gustavo; BODIN DE MORAES, Maria Celina; BARBOSA, Heloísa Helena. Código Civil interpretado..., v. I, cit., p. 232). Na mesma rota, NERY JÚNIOR, Nelson; NERY, Rosa Maria de An- drade. Código Civil comentado. 5. ed. São Paulo: Ed. Ed. RT, 2007, p. 301-302.

Logo, seus efeitos estão previamente determinados pela ordem jurídica positiva, e não pela vontade do renunciante.[134] Não cabe a este definir os efeitos de sua renúncia.[135] Assim como a vontade do renunciante não é composta por interferência de vontades externas. Se determinado interessado opta por abrir mãos de certas posições jurídicas ativas em ambiente de negociação, para obter vantagens outras como contrapartida, trata-se de negócio jurídico bilateral que, se tiver por escopo evitar ou pôr termo a litígio, será qualificado como transação.

Neste caso, uma realidade não integra a outra. A renúncia não está contida na transação. É alheia a ela, porque cumpre função absolutamente distinta. Se a transação não abrange a renúncia, ainda que seja equívoco comum tal referência na realidade jurisprudencial,[136] a cláusula que elimina ou reduz certa posição jurídica, para a obtenção de outra, como contrapeso, não é nula por violação ao art. 424 do Código Civil ou ao art. 51, I do Código de Defesa do Consumidor. Sendo o negócio qualificado como transação, a declaração de nulidade do contrato (ou de uma cláusula) dependerá da análise do conteúdo do contrato no caso concreto, de modo a saber se ele se inclui em algumas das causas previstas no art. 166 e seguintes do Código Civil.[137]

Um segundo argumento importante, malgrado recaia sobre si a pecha de demasiadamente "formalista" ou "exegético-literal", é que a incidência do art. 51 do Código de Defesa do Consumidor parece restringir-se às "cláusulas contratuais relativas ao fornecimento de produtos e serviços", como bem delimita o caput do referido dispositivo legal. Como é

---

[134] Em sentido contrário, qualificando a renúncia de direitos como "negócio jurídico unilateral", entre tantos, cf. AMARAL, Francisco. Direito civil: introdução, cit., p. 60; e MELLO, Marcos Bernardes de. Teoria do fato jurídico: plano da existência. São Paulo: Saraiva, p. 239

[135] É que os atos jurídicos em sentido estrito correspondem àqueles "cuja vontade não tem aptidão para produzir o regulamento ou a normativa a ser aplicada, vez que está já está previamente regulamentada por lei ou por negócio jurídico" (REIS JÚNIOR, Antonio dos. O fato jurídico em crise..., cit., p. 33)

[136] Tal confusão é bastante comum na jurisprudência, atingindo mesmo as decisões do Supe- rior Tribunal de Justiça, como se pode verificar no Recurso Especial n. 1.115.265-RS, Rel. Min. Sid- nei Beneti, julgado em 24/4/2012, resumido no Informativo n. 469 da Corte Superior: "Cinge-se a controvérsia à análise da ocorrência da renúncia tácita à impenhorabilidade de pequena propri- edade rural familiar dada em garantia pelo recorrido, em acordo extrajudicial posteriormente homologado judicialmente, o qual nele figura como garantidor solidário de obrigação de terceiro. Na espécie, a recorrente alega que a garantia oferecida pelo recorrido equipara-se à garantia real hipotecária, prevista no art. 3º, V, da Lei n. 8.009/1990. Contudo, o Min. Relator salientou que a ressalva prevista nesse dispositivo legal não alcança a hipótese dos autos, limitando-se, unicamente, à execução hipotecária, não podendo tal benefício (o da impenhorabilidade) ser afastado para a execução de outras dívidas. Assim, salvo as situações compreendidas nos incisos I a VII do art. 3º da Lei n. 8.009/1990, descabe a penhora de imóvel ou a sua oferta em garantia. Além do mais, o bem é uma pequena propriedade rural, cuja impenhorabilidade encontra-se garantida constitucionalmente (art. 5º, XXVI, da CF). De modo que, a exceção à impenhora- bilidade do bem de família previsto em lei ordinária não pode afetar direito reconhecido pela Constituição, nem pode ser afastada por renúncia, por tratar-se de princípio de ordem pública que visa à proteção da entidade familiar. Precedentes citados: REsp 470.935-RS, DJ 01/3/2004, e REsp 526.460-RS, DJ 18.10.2004"

[137] Para um estudo abrangente das invalidades nas relações civis, cf., por todos, SOUZA, Edu- ardo Nunes. Teoria geral das invalidades: nulidade e anulabilidade no direito civil contemporâneo. São Paulo: Almedina, 2017

cediço, o contrato de transação que é realizado para pôr termo a determinado litígio não tem como objeto o "fornecimento de produtos ou serviços", mas a autocomposição do litígio.

Isso não significa que o intérprete ou aplicador do direito deva desprezar a situação de debilidade contratual do consumidor, especialmente por ser ele um sujeito presumidamente vulnerável (art. 4º, I do Código de Defesa do Consumidor), mas é necessário destacar que os critérios serão diversos daqueles constantes do art. 51 da Lei n. 8.078/90, e deverão ser apurados em cada caso concreto.

Cabe ao intérprete, portanto, verificar se na negociação entre agente e vítima consumidora, aquele impõe, por sua posição de superioridade contratual, "prevalecendo-se da fraqueza ou ignorância do consumidor" (art. 39, IV do Código de Defesa do Consumidor), alguma cláusula que exija da vítima vantagem manifestamente excessiva (art. 39, V do Código de Defesa do Consumidor).

Se assim o for, restará qualificada a conduta do fornecedor como "prática abusiva", expressamente proibida por lei, autorizando a declaração de sua nulidade na forma do art. 166, VII, parte final, do Código Civil.[138]

Finalmente, a transação não contraria o disposto no art. 6º, VI do Código de Defesa do Consumidor. A doutrina costuma identificar neste texto normativo a positivação, nas relações de consumo, do princípio da reparação integral, caracterizando-o como um direito elementar do consumidor.[139] Dada a sua natureza basilar, atrairia para si a característica da indisponibilidade. Afinal, as normas de proteção e defesa do consumidor são consideradas como de ordem pública e interesse social, traduzindo-se, assim, como normas cogentes.[140] Não se pretende aqui questionar a natureza imperativa das normas de proteção ao consumidor, cuja incidência é uma das mais expressivas manifestações do dirigismo contratual.

Contudo, é preciso reconhecer que o Código de Defesa do Consumidor (Lei n. 8.078/90), como demonstração clara de legislação avançada, optou, conscientemente, por não utilizar o tradicional termo reparação integral ao fazer referência ao direito básico do consumidor, preferindo conferir-lhe o direito elementar à "efetiva prevenção e reparação de

[138] Código Civil. "Art. 166. É nulo o negócio jurídico quando: (...) VII – a lei taxativamente o declarar nulo, ou proibir-lhe a prática, sem cominar sanção",

[139] Entre tantos outros, NUNES, Rizzato. Curso de direito do consumidor. São Paulo: Saraiva, 2013, p. 191-192

[140] BENJAMIN, Antônio Herman V.; MARQUES, Cláudia Lima; BESSA, Leonardo Roscoe. Ma- nual de Direito do Consumidor. São Paulo: Ed. RT, 2007, p. 53.

danos (...)".[141] A preferência pela efetiva reparação não é por acaso.[142]

A moderna legislação brasileira sabe que a ideia de reparação pela exata extensão dos danos sofridos (reparação integral) representa apenas uma das possibilidades de satisfação plena do interesse do consumidor lesado. Por vezes, ainda mais importante que a recomposição matematicamente perfeita das perdas, é a possibilidade de autocomposição célere, segura e eficaz, por vezes valendo-se de benefícios alternativos à indenização pecuniária,[143] mas sem perder de vista que a possibilidade de evitar ou extinguir um litígio judicial pela via do acordo é exigência que se impõe pelo princípio da solidariedade.

Na questão posta no início desde capítulo, apesar de suscitar dúvida a respeito da natureza da responsabilidade (contratual ou extracontratual), é preciso ter em mente que o direito de ação, como corolário do acesso à justiça (art. 5º, XXXV da CF), permite que toda e qualquer pessoa que entenda ter algum interesse violado possa demandar em juízo pelo seu reconhecimento.[144] Deste modo, interpretando o direito civil na legalidade constitucional, mesmo um acordo de transação bem sucedido não tem o condão impedir a propositura de uma ação por aquele que se comprometeu a evitá-la.[145] Seria, sim, matéria de defesa por parte do réu, que deve invocar e comprovar a existência de acordo prévio e extrajudicial, como fato impeditivo do direito do autor.[146]

É matéria de defesa forte, que só será ultrapassada se (i) a parte autora (consumidora) comprovar algum vício que possa eivar o acordo com alguma nulidade ou anulabilidade,[147] (ii) demonstrar alguma circunstância excepcional qualificada como prática comercial abusiva, seja

---

[141] "Art. 6º. São direitos básicos do consumidor: (...) VI – a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos (...)".

[142] Como bem destaca Gustavo Tepedino: "sublinhe-se a significativa alusão do legislador à efetividade da tutela, acentuando desse modo não somente a integralidade de eventual indeni- zação – danos emergentes e lucros cessantes – mas, principalmente, a sobreposição conceitual do conteúdo sobre a forma, ou seja, o preceito refuta qualquer classificação formal – espécies de danos ou de ritos – que pudesse sacrificar o resultado reparatório pretendido" (A responsabilidade civil por acidentes de consumo na ótica civil-constitucional, cit., p. 283)

[143] Na negociação, é possível ainda incluir instrumentos variados como a reparação física ou substituição de produtos ou reexecução de serviços, com oferta de upgrade, como alguns dos exemplos de reparação in natura que o consumidor tem à sua disposição no âmbito da autocom- posição (SCHREIBER, Anderson. Reparação não pecuniária dos danos morais, cit., p. 213-216).

[144] Conferindo ampla interpretação ao princípio constitucional do acesso à justiça (art. 5º, XXXV da CF), para além do corolário da inafastabilidade do controle jurisdicional (art. 3º do Código de Processo Civil), cf. MARINONI, Luiz Guilherme. Curso de Processo Civil. 3. ed. São Paulo: Ed. RT, 2008, v. 1, p. 221.

[145] Terá a parte autora, portanto, interesse de agir se o provimento jurisdicional for útil à sua satisfação. Não poderá, então, um juiz deixar de conhecer a demanda, por ausência de condição da ação, ao argumento de preexistir acordo de transação no qual as partes se comprometeram a não litigar judicialmente. Trata-se de matéria de mérito, em que o pedido deve ser apreciado, no sentido de sua procedência ou improcedência.

[146] Código de Processo Civil. "Art. 373. O ônus da prova incumbe: (...) II – ao réu, quanto à exis- tência de fato impeditivo, modificativo ou extintivo do direito do autor".

[147] É o mesmo fato impeditivo que é válido também para as relações paritárias, como já mencionado no capítulo infra.

porque se aproveitou da fraqueza ou ignorância do consumidor, ou porque exigiu dele, na negociação, vantagem manifestamente excessiva (art. 39, IV e V do Código de Defesa do Consumidor).

Como parâmetros para a aferição dos aspectos que tornariam a transação ineficaz, pela exploração da fraqueza ou ignorância do consumidor, ou pela exigência de vantagem manifestamente excessiva, propõe-se que os fornecedores de produtos e serviços (i) tenham o cuidado de emitir propostas de com linguagem clara e precisa; (ii) com razoável tempo de reflexão, evitando o acerto por impulso, de maneira a privilegiar o estudo e o conhecimento, por parte da vítima, acerca da amplitude da proposta; (iii) estejam abertos ao recebimento de contrapropostas, evidenciando a existência real de exercício da autonomia do consumidor, como ator relevante da modelação do conteúdo do contrato de transação; (iv) redijam com destaque as situações jurídicas ativas que o consumidor abrirá mão, como contrapartida para a rápida e eficaz resolução da controvérsia; (v) proponham concessões mútuas razoavelmente equilibradas e proporcionais, como forma de afastar o risco de haver exigência manifestamente excessiva., sem descuidar dos aspectos subjetivos que costumam nortear a autocomposição.[148]

Quanto maior a medida de cumprimento de tal itinerário, maior higidez será conferida à transação, tornando-a mais segura, de forma a potencializar o uso na praxe, fortificando a eficácia da função promocional da responsabilidade civil. Se, naquela hipótese concreta inaugural, comprovando José que houve a aceitação do acordo, por mera adesão, em contexto no qual lhe foi retirada a possibilidade de reflexão sobre a amplitude dos fatos danosos, havendo insistência em torno da aceitação imediata da composição civil, é possível vislumbrar prevalecimento do fornecedor sobre sua ignorância ou fraqueza (que se potencializa se o consumidor for idoso, ou portador de deficiência mental ou intelectual, ainda que não curatelado etc.).

Tais elementos ampliam a possibilidade de ver reconhecida a nulidade do contrato.[149] Mais poderoso será, ainda, o argumento de que a redução de sua situação jurídica ativa foi desproporcional, evidenciando-se a exigência de vantagem manifestamente excessiva. Deve-se apenas atentar para o fato de que a desproporcionalidade não deve ser apurada por meros

[148] Uma boa baliza para apurar a quantificação ideal do dano sofrido pela vítima é a verificar a média das indenizações pecuniárias impostas pela jurisprudência, para hipóteses seme- lhantes, evitando-se reduzir desproporcionalmente tais valores na negociação. Quando mais próximo os valores acordados estiverem daquilo que normalmente se reconhece em juízo para situações semelhantes, maior será a higidez do acordo, evidenciando que não houve exploração da fraqueza ou ignorância do consumidor, ou exigência de vantagem manifes- tamente excessiva. Maior será também, em última análise, a prova da boa-fé dos fornecedores na contratação.

[149] Nos termos do art. 166, VII do Código Civil c/c art. 39, IV do Código de Defesa do Consumidor.

critérios objetivos, na medida em que o interesse subjetivo que envolve a transação tem peso relevante na autocomposição.

Daí a razão pela qual a discrepância objetiva precisa saltar aos olhos para ser declarada sem maiores dificuldades, mas sempre em contexto com os demais critérios. Recheada de peculiares, outrossim, é o exercício da função promocional da responsabilidade nos chamados "danos coletivos", como agora se passa a analisar.

5.5. Autoridade Nacional de Proteção de Dados: Estrutura vital para fiscalização e penalização

A Autoridade Nacional de Proteção de Dados é um elemento substancial para a garantia da eficácia da Lei Geral de Proteção de Dados. De fato, o emprego de autoridades administrativas para a tutela da proteção de dados tem sido um recurso, francamente majoritário na vasta maioria dos marcos normativos sobre a matéria.

Neste ponto, impende mencionar que os esforços anteriores na busca pela efetivação à privacidade não devem ser desconsiderados ou postos de lado; pelo contrário, as proposições realizadas neste tópico visam a somar com as soluções já produzidas pelos estudiosos da temática e legisladores.

A implementação da ANPD, no entanto, é um dos pontos mais caudalosos das idas e vindas que marcam a formação do marco regulatório brasileiro sobre a matéria. Ainda, à medida que o debate em torno desta autoridade se tornou mais intenso e passou a interessar de forma mais ampla a diversos setores da sociedade, decidiu-se por dotá-la, como órgão consultivo auxiliar, de um Conselho Nacional de Proteção de Dados e Privacidade, com composição multissetorial.

Desta maneira, devemos ter cristalino que as medidas para anonimização de dados e a autodeterminação informativa, a necessidade de consentimento, dentre outras, devem ser pensadas em conjunto quando teorizamos e propomos em matéria regulação. Não custa ressaltar a premissa metodológica do trabalho - a salvaguarda dos direitos fundamentais, mormente a privacidade.

Neste intento, como várias vezes afirmado toda solução é bem-vinda. Isto superado, tem-se que a regulação do risco, como a própria nomenclatura sugere, consiste basicamente na tomada de medidas que visam projetar salvaguardas ante possíveis e eventuais perigos oriundos de determinada atividade. Risco, nesta perspectiva, é a chance de um perigo vir a ocorrer.

Destarte, a regulação do risco seria uma ferramenta adequada para basear decisões a

serem tomadas em face dos perigos em potencial. É propositura que surge, inclusive, na esteira da preocupação com o meio ambiente e sua preservação. Não é difícil imaginar o porquê, ainda mais quando já se vem fazendo analogias do uso dos dados pessoais com a indústria do petróleo e gás, extremamente nociva e degradante para com o ambiente que lhe circunda, e com a comparação com um material radioativo, que requer atenção e cuidados ainda mais intensos.

Os riscos inerentes à monetização desta nova matéria-prima social, a partir dos diferentes pontos de luz emanados dos interesses presentes na sociedade em rede, pode, como se demonstra, afetar a privacidade e seus valores conexos. A hipótese de manipulação dos discursos, da narrativa política, das ideologias que serão ou não propagadas, de quanta publicidade se dará a determinado fato político - tudo isto, conforme se demonstrou, é factível e, portanto, um risco; um risco que tem o condão de afetar o próprio tecido dos fluxos democráticos.

Se, como quer Harari, somos todos pequenos "chips", partes de um enorme processador de informações que é a humanidade, nossos dados pessoais são os bits que descortinam os nossos aspectos arcanos e que possibilitam certa margem de manipulação sobre nossa espécie humana[150]; havendo que se pensar em regular, portanto, quais informações circulam por esses "chips", quem as está promovendo e com qual intento, sob pena de pôr em xeque as liberdades e a própria democracia.

Desta forma, para nós, a atuação do Estado[151], seja qual for o modelo regulatório a ser escolhido, tem de tomar uma postura adequada para o risco em relação à monetização de dados pessoais. Neste intento, deve possuir capacidade normatizante suficiente para fazer valer a proteção da privacidade potencialmente descortinada e eventualmente danosa - tal qual um material radioativo, o agente que desejar monetizar os dados pessoais deve ter ciência de que a referida atividade ostenta deveres, responsabilidades e riscos - riscos estes que o agente deve assumir tanto para atuar na prevenção de sua ocorrência, como na reparação em razão de violação de direitos tutelados.

A modelagem institucional da Autoridade Nacional de Proteção de Dados, definida pelas modificações trazidas pela Lei 13.853/2019 à LGPD (Lei 13.709/2018), é a de um órgão integrante da Presidência da República (conforme o art. 2 da Lei 13.844/2019, que estabelece

---

[150] Essa vulnerabilidade é destacada por Yuval Harari, segundo o qual "se quisermos evitar a concentração de toda a riqueza e de todo o poder nas mãos de uma pequena elite, a chave é regulamentar a propriedade dos dados." HARARI, Yuval Noah. 21 lições para o século 21. São Paulo: Companhia das Letras, 2018. p. 107.

[151] CRESPO, Danilo Leme; RIBEIRO FILHO, Dalmo. A evolução legislativa brasileira sobre a proteção de dados pessoais: a importância da promulgação da lei geral de proteção de dados pessoais. Revista de Direito Privado, vol. 98, p. 161–186, mar./abr., 2019.

a organização básica dos órgãos da Presidência da República e dos Ministérios), conjuntamente com a Casa Civil, a Secretaria de Governo, a Secretária-geral, o Gabinete Pessoal do Presidente da República e o Gabinete de Segurança Institucional.

A estrutura organizacional da ANPD foi definida pelo Decreto 10.474/2020, que, ao momento do fechamento deste estudo, já se encontra em vigor. No presente artigo, discorrer-se-á sobre a natureza e importância de autoridades de proteção de dados, da fundamentação de seu caráter autônomo, do processo que levou à formação da ANPD e da sua natureza.

Quanto às possíveis críticas, nos atemos a rebater de antemão apenas aquela que é a mais frequente e, portanto, passível de se prever: a dos custos. Por este lado, parte-se da premissa de que é preciso uma Autoridade Nacional de Proteção de Dados, com poderes e capacidades técnicas suficientes para produzir estas ousadas sugestões; neste horizonte, sendo autarquia especial integrante da administração pública federal indireta, contaria como receita com as dotações consignadas no orçamento geral da União, além de outras fontes de renda típicas de uma agência reguladora.[152]

No caso do Brasil, organismos do gênero foram sistematicamente introduzidos na estrutura institucional do país basicamente para atender a demandas relacionadas à regulação de áreas do mercado das quais o Estado operava sua retirada como operador em caráter de monopólio, como a Agência Nacional do Telecomunicações (ANATEL) ou a Agência Nacional de Energia Elétrica (ANEEL); ou então com a busca de maior eficiência na regulação de aspectos críticos do mercado, como a defesa da livre concorrência (cuja tutela é função do Conselho Administrativo de Defesa Econômica - CADE) bem como para a imposição de normativas técnicas em setores especializados para a garantia de valores como, entre outros, a saúde pública, como ocorre com a Anvisa (Agência Nacional de Vigilância Sanitária).

O recurso a modelos do gênero, porém, não é propriamente uma novidade no Brasil, o que é perceptível quando verificamos instituições que desempenharam marcada função na regulação de setores do mercado e que gozaram de certa independência para atingir seus fins - como o Instituto Brasileiro do Café ou o Instituto do Açúcar e do Álcool, entre outros -, além de estruturas com importantes semelhanças, como a Comissão de Valores Mobiliários (CVM), o Conselho Monetário Nacional (CMN) ou o próprio Banco Central do Brasil.

Uma das principais razões de ser desses órgãos, desgarrados da estrutura administrativa tradicional e caracterizados pela sua independência, pela especificidade de sua atividade e pelo seu caráter eminentemente técnico, é a crescente complexidade das relações sociais, da

[152] LIMA, Caio César Carvalho. In: BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (coord.). Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters. Brasil, 2019.

organização do Estado e das demandas que o aparato público é instado a abordar. Diante dessa necessidade, demonstrou-se necessário que a administração pública se especializasse para atender a cada uma das grandes demandas com o particularismo e a dinâmica necessários. Mais recentemente, verificou-se que diversas características desses órgãos, moldados para responder de forma mais direta e dinâmica a determinadas demandas de natureza econômica, poderiam ser igualmente relevantes no papel da defesa e da promoção de direitos do cidadão, proporcionando o surgimento da figura da autoridade de garantia.

A distinção que pode ser feita quanto ao âmbito de atuação dessas autoridades, portanto, comporta que em uma taxonomia básica possam ser divididas entre "autoridades de regulação" e "autoridades de garantia". As autoridades de regulação, cuja competência costuma ser ligada a um determinado serviço público, são destinadas funções similares àquelas da própria administração pública, com vantagens quanto à dinamicidade de sua estrutura e outras. Por sua vez, as autoridades de garantia possuem a missão de proteção de direitos ou situações subjetivas específicos, para cuja defesa foram constituídas. Um organismo com a proposta de proteção de um direito como o da proteção de dados pessoais (a ANPD, por exemplo), estaria enquadrada, portanto, como uma autoridade de garantia.

Para a efetiva proteção dos direitos em questão na amplitude necessária, seja esta individual ou coletiva, cabe a devida consideração das características da matéria de proteção de dados pessoais a partir dos desafios específicos para a implementação de um sistema adequado de tutela 15. Conforme observamos, trata-se de seara na qual os danos de reduzidíssima monta são comuns, o que diminui a propensão para que se postule individualmente sua reparação a partir dos institutos tradicionais de responsabilidade civil. A utilização de uma tutela baseada na responsabilidade civil não é, por si só, um instrumento que tutele na medida necessária o direito fundamental à proteção de dados pessoais, podendo inclusive vir a incentivar a consolidação de práticas de utilização indevida de dados pessoais.[153]

A abordagem que a autoridade virá a empregar vai definir pontos cruciais e pautar matérias, podendo inclusive vir a ser o maior fator de indução da implementação da LGPD e da das expectativas dos cidadãos a respeito de suas garantias relacionadas à proteção de dados. Para que esta complexa e importante missão seja levada a cabo com bom êxito, aguarda-se que a criação da autoridade seja pautada por critérios técnicos tendo em vista o direito fundamental

[153] FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. Revista Direito e Práxis, [S.l.], v. 12, n. 2, p. 1002-1033, jun. 2021. ISSN 2179-8966. Disponível em: https://www.e-publicacoes.uerj.br/index.php/revistaceaju/article/view/46944/33907. Acesso em: 20 nov. 2021.

à proteção de dados, pela consciência da relevância fundamental da matéria e pelo reconhecimento da necessidade imperiosa de prover-lhe dos indispensáveis efetivos atributos de independência e autonomia, bem como seja garantida a autonomia de seu órgão consultivo, o Conselho Nacional de Proteção de Dados e Privacidade com o cessamento de sua subordinação à Presidência da República, seja quanto à escolha dos seus integrantes representantes setoriais, seja quanto à sua autonomia.

A LGPD corrobora, expressamente, o passo adiante na responsabilidade civil pelo ilícito lucrativo, mormente a partir de seu conjunto explícito de princípios, ladeados por demais dispositivos legais que instrumentalizam a desejada concretude de proteção a direitos fundamentais e da personalidade.

É daqui que se vislumbra mais uma contribuição para esse desiderato: a responsabilidade civil proativa da Lei Geral de Proteção de Dados Pessoais. Por tal regime, considera-se lesante não apenas quem, realmente, causa a lesão, mas também aquele que, por inércia, a permite. Volta-se, assim, à instrumentalização e à base principiológica.

A partir do princípio da responsabilidade e da prestação de contas, o legislador colacionou medidas aptas a nortearem a atuação dos agentes envolvidos. Nessa seara, determina-se minimização de tratamento, com os princípios da finalidade, adequação e necessidade, mas não só. Ao contrário, a LGPD pretende, sobretudo com a responsabilidade civil, que o ilícito seja evitado, que as atividades de tratamento tenham por base a boa-fé e seus princípios, como o da segurança e da prevenção, os quais impõem adoção e utilização de medidas que protejam os dados de tratamento indevido e previnam a ocorrência de danos. Tal sistema é absolutamente incompatível com o prêmio ao infrator, que teria cheque assinado para ficar com ganhos decorrentes da violação das citadas normas.

Por outro lado, a literatura jurídica investiga a situação do ofensor que obteve ganhos a partir de atos ilícitos a qual, pareada à imprescindibilidade de haver uma resposta a não permitir que isso aconteça (ou assim permaneça), situa o problema entre enriquecimento sem causa e responsabilidade civil. É necessário o enfrentamento do problema para que haja a remoção dos proveitos indevidos, tanto em questões patrimoniais quanto e, principalmente, naquelas que envolvem direitos da personalidade.

No que tange a responsabilização proeminente subjetiva, podemos notar que a Lei Geral de Proteção de Dados, deixou lacuna de entendimento, pois não deixou claro ser objetiva sua responsabilização, o que desagua no campo de subjetividade para apuração do ilícito de dados.

Em outra frente, as relações de consumo no ambiente digital, demonstram-se na vanguarda das demandas no âmbito do poder judiciário quando relativa aos violação de dados

pessoais, o que por analogia, aplica-se as regras atinentes ao código consumerista que prevê a responsabilização objetiva no âmbito das relações de consumo.

Assim, sobressai-se a viabilidade averiguada para que a remoção de ganhos ilícitos diante de violações a direitos da personalidade, como (os correlatos a) a privacidade, seja um remédio para conferir concretude à proteção dos dados pessoais. Ressalta-se, na construção da temática, que o instituto eleito para a solução do caso é a responsabilidade civil, que precisa superar a dificuldade de restituir o ganho indevido quando em montante superior ao prejuízo.

Para isso, a responsabilidade civil pelo ilícito lucrativo não se utiliza da função punitiva, pois não agrava a situação patrimonial do lesante, apenas o devolve à situação anterior à prática do ilícito, removendo-lhe o proveito obtido.

6. CONTORNOS LEGISLATIVOS E JURISPRUDENCIAIS NO ÂMBITO DA PROTEÇÃO DE DADOS EM COMPASSO AO DIÁLOGO DAS FONTES

A literal inscrição do direito à proteção de dados não é comum nas constituições e nos tratados internacionais aprovados e internalizados na legislação dos Estados soberanos. No âmbito do sistema universal de proteção da Organização das Nações Unidas, assim como na esfera do direito continental europeu, esse direito tem sido deduzido em especial do direito à privacidade, embora tecnicamente não se confunda com este.

Nesse sentido, a orientação adotada pela Comissão da ONU para Direitos Humanos ao interpretar o alcance do art. 17, do Pacto Internacional de Direitos Civis e Políticos e, de forma assemelhada, na jurisprudência da Corte Europeia de Direitos Humanos (CEDH) e no Tribunal de Justiça da União Europeia.

Rememore-se, inclusive, a importância da Convenção n° 108 para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais (datada de 1981), denominada Convenção de Estrasburgo, que foi posteriormente interpretada com maior clareza pelo art. 8 da Carta de Direitos Fundamentais da União Europeia, em 2000. Por esses documentos foi sendo construído e instituído um direito à proteção de dados que finalmente foi alçado à condição de direito fundamental, com natureza autônoma. Ocorre que apesar de se tratar de tema de interesse mundial, essa prescrição legislativa vinculou apenas os estados integrantes da União Europeia, inclusive valendo observar a importância da entrada em vigor do Tratado de Lisboa, em 2009.[154]

[154] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. Revista de Direito do Consumidor, vol. 120, p. 469–483, nov./dez. 2018.

No contexto brasileiro, ao tempo da promulgação da atual Constituição Federal, o universo digital ainda não era causa de repercussões maiores, razão pela qual nota-se referências indiretas representadas, por exemplo, pelo constante do art. 5°, XII, que refere ao sigilo das comunicações de dados (além do sigilo da correspondência, das comunicações telefônicas e telegráficas). Ou seja, o texto constitucional não contemplava, expressa e literalmente, um direito fundamental à proteção e livre disposição dos dados pelo seu respectivo titular. Contudo, a Emenda Constitucional nº 115, de 2022, acresceu a carta constitucional no art. 5°, LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Mas a popularização da internet e o melhor conhecimento dessa realidade do mundo online, suas vantagens e problemas, veio impor novas concepções que apontam para a importância da proteção dos seres humanos partícipes desse cenário, o que somente pode evoluir com o reconhecimento desse direito como fundamental, conforme contexto positivado na ordem jurídica brasileira.

Há que se ressaltar a necessidade de especificidade e de sistematização, para que nessa concepção (de sistema) se encontre completude de abrangência e adequado regramento da matéria. Na proteção dos dados pessoais, para além da referência ao sigilo da comunicação, cabe ampliar a ainda limitada salvaguarda parcial e indireta contida na previsão da ação de habeas data (art. 5°, LXXII, da CF), ação constitucional com status de direito-garantia fundamental autônomo, que precisamente busca assegurar ao indivíduo, o conhecimento e mesmo a possibilidade de buscar a retificação de dados constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, tudo se constituindo de uma garantia procedimental do exercício da autodeterminação informacional (MENDES, 2017, pg. 185).

E dissemos limitada, pois no que tange ao sigilo da comunicação de dados, há que se ter cautela, razão pela qual se impõe haver o registro, com base na lição de Danilo Doneda:

Se por um lado, a privacidade é encarada como um direito fundamental, as informações pessoais em si parecem, a uma parte da doutrina, serem protegidas somente em relação à sua "comunicação", conforme art. 5, XII, que trata da inviolabilidade da comunicação de dados. Tal interpretação traz consigo o risco de sugerir uma grande permissividade em relação à utilização de informações pessoais. Nesse sentido, uma decisão do STF, relatada pelo Ministro Sepúlveda Pertence, reconheceu expressamente a inexistência de uma garantia de inviolabilidade sobre dados armazenados em computador com fulcro em garantias constitucionais. O sigilo, no inciso XII do art. 5°, está referido à comunicação, no interesse da defesa da privacidade. Obviamente o que se regula é comunicação por correspondência e

telegrafia, comunicação de dados e telefônica. A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por um sujeito estranho. A decisão tem sido, desde então, constantemente mencionada como precedente em julgados nos quais o STF identifica que a natureza fundamental da proteção aos dados está restrita ao momento de sua comunicação. (DONEDA, 2006, Pg. 262)

Essa garantia de que o terceiro não coletará ou interceptará indevidamente dados em trânsito entre uma pessoa e outra precisa ser protegida, tanto quanto deve-se atentar para a obrigação do manuseio de boa-fé dessas informações por quem quer que seja, mesmo que autorizado (nesse sentido, além do CDC, art. 4º, que prevê a harmonia e transparência nas relações de consumo, vale destacar o que, em caráter geral, prescreve o art. 6º, da lei geral de proteção de dados). E boa-fé principia pelo cumprimento de, dentre outros, três principais deveres: coerência, informação e cooperação (SOUSA, 2017, pg. 40). E aonde existe dever, tal como uma sombra projetada, surge a responsabilidade para o(s) obrigado(s), incluindo-se aqueles que coletam, manuseiam, utilizam, têm acesso, comercializam ou por qualquer outra forma possuem contato com os dados.

Entretanto, em nível constitucional, pode-se considerar como embasamento direto mais próximo de um direito fundamental à proteção de dados, tanto o específico direito ao livre desenvolvimento da personalidade, intrinsecamente ligado ao princípio da dignidade da pessoa humana, quanto o direito geral de liberdade. Em específico no tocante a este último, de poder ter extimidade, ou seja, ser-lhe permitido participar do ambiente virtual mediante regras lícitas, condutas límpidas, transparentes e legítimas, todas conformes com essas condições da cláusula geral de proteção de todas as dimensões da personalidade humana (PINTO, 2018, pg. 36).

Por isso, paulatinamente, vem se consolidando na tradição jurídica (principalmente no direito constitucional estrangeiro e no direito internacional dos direitos humanos), o direito à livre disposição sobre os próprios dados pessoais, designado como direito à livre autodeterminação informativa (PINTO, 2018, pg. 642).

Assentando-se nessas bases, mediante uma leitura harmônica e sistemática do texto constitucional, fica patente a propriedade de aderir ao entendimento de que, atualmente, como vem se firmando no direito brasileiro, o direito fundamental à proteção de dados pessoais pode ser reconhecido como implícito na Constituição Federal. (BIONI, 2019, pg. 90).

Entretanto, esse contexto mostra a importância de haver uma raiz constitucional para esse direito fundamental a proteção de dados, uma base principiológica para a legislação infraconstitucional e respectiva interpretação, base essa que seja adequada e não se defase

facilmente no tempo, mostrando-se adaptável para servir de diretriz maior direcionada para reger inclusive as novas situações que surjam com o desenvolvimento tecnológico.

Essa possível inscrição formal expressa do referido direito na Carta Magna, tenderá a produzir uma carga positiva adicional, ou seja, agregar valor positivo substancial em relação ao atual estado da arte no Brasil.

Outro detalhe importante para o tema que estamos a abordar, adveio em manifestação da jurisprudência que sinalizou parâmetros de como essa questão deve ser tratada. O fato é que em 17 de abril de 2020, sob o argumento de enfrentar efeitos da pandemia provocada pela covid 19, foi editada a já extinta Medida Provisória nº 954. Nas discussões relativas à norma surgiram 344 emendas ao texto da MP, muitas delas com objetivos como reduzir a coleta de dados ao mínimo necessário, obrigação de elaborar relatório de impacto de segurança da informação anteriormente à coleta e uso de dados, maior transparência na definição da finalidade e no uso dos dados compartilhados, bem como, o argumento de que mesmo diante da gravidade da situação de saúde pública, o seu combate não poderia acontecer mediante atropelo de direitos fundamentais.

O fato é que a mencionada MP não foi convertida em lei e perdeu a validade, mas deixou um expressivo legado, pois foi atacada por diversas Ações Diretas de Inconstitucionalidade, as quais, em razão da unidade temática, foram reunidas para julgamento em conjunto na ação de distribuição mais antiga (ADI 6387-DF), com relatoria da Ministra Rosa Weber, sendo a decisão final um exemplo dos pressupostos de proteção que se espera nessa área.

Note-se que a referida MP versava sobre o temporário (até o final da pandemia, com destruição posterior dos arquivos) compartilhamento de dados pessoais entre as empresas de comunicação prestadoras de serviços de telefone fixo comutado e de serviços de telefonia móvel, com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE). Em seu texto haviam prescrições assegurando o caráter sigiloso das informações obtidas, a vedação de compartilhamento com empresas públicas ou privadas ou, ainda, órgãos da administração direta ou indireta, tudo com obrigação de elaboração de relatório no site da referida fundação informando como as informações teriam sido utilizadas e impactos causados pelo compartilhamento (vide artigos 3° e 4º).

Dentre as várias manifestações insertas nos processos, pode-se destacar que o Conselho Federal da OAB impugnou a referida MP pelos seguintes motivos: i) cabimento de controle judicial sobre os requisitos constitucionais de relevância e urgência para edição de Medidas provisórias; ii) ausência de relevância e urgência para pesquisa do IBGE durante a pandemia, o que desautoriza a edição dessa MP; iii) violação do direito à autodeterminação informativa,

privacidade e intimidade dos cidadãos; IV) ausência de correlação com precedente sobre caso Coaf (Recurso Extraordinário 1.055.941), de compartilhamento direto com Ministério Público, sem prévia autorização judicial, pois aquele precedente refere a procedimento formal de natureza penal, dotado de finalidade específica, destituído de controle administrativo externo e ausência de garantia de sigilo ou delimitação da responsabilidade dos agentes públicos responsáveis por assegurar o sigilo; V) violação do princípio da proporcionalidade ou proibição do excesso (adequação, necessidade, proporcionalidade).

De sua parte, o Ministério Público Federal (MPF), em parecer de lavra do Procurador Geral da República, opinou pela conformidade da MP em relação ao ordenamento jurídico brasileiro, baseado nos argumentos assim sintetizados: i) o controle judicial de requisitos constitucionais para edição de Medidas Provisórias deve ocorrer apenas em casos de flagrante desconformidade, o que não seria o caso; ii) referida Medida Provisória não atenta contra direitos fundamentais da intimidade e da vida privada; iii) tais medidas são proporcionais tendo em vista o direito à saúde; iv) necessidade de remessa de número de telefone e respectivo endereço residencial dos consumidores de serviços de telecomunicações, de pessoas naturais ou jurídicas ao IBGE, para elaboração da Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD-Contínua), que totaliza 200 mil domicílios visitados a cada trimestre, diante da impossibilidade de realização de entrevistas domiciliares; v) Relevância da inclusão de quesitos na PNAD-Contínua para monitoramento sobre a Covid-19, para orientar os processos decisórios dos gestores públicos das diversas esferas; vi) Temporalidade da medida, caráter sigiloso e descarte dos dados ao fim da pandemia (BRASIL, 2020).

Em complemento, cabe transcrever que a Advocacia-Geral da União (AGU), postulou pela manutenção da Medida Provisória com base nos seguintes argumentos: 1) As atribuições do IBGE estão previstas nas CF de 1988, como órgão incumbido pela União para organizar e manter os serviços oficiais de estatística, geografia, geologia e cartografia de âmbito nacional (art. 21, inciso XV) e nas Leis n.5.534/1968, 5.878/1973, que determinam a obrigatoriedade de pessoas físicas e jurídicas de prestar informações, assim como o dever de manutenção de sigilo em relação às informações recebidas; 2) O Instituto possui diretrizes, comitês e políticas internas de confidencialidade sobre segurança da informação; 3) A PNAD-Contínua (PNAD), de elaboração trimestral, não pode ser adiada uma vez que consiste na principal fonte de informação que o governo federal dispõe sobre emprego, educação, renda e condições de vida da população brasileira; 4) Em razão de convênio com o Ministério da Saúde, serão inseridas perguntas aos cidadãos sobre disseminação da Covid-19, que serão úteis para a formulação de políticas públicas de enfrentamento da doença; 5) Relevância e urgência da referida Medida

Provisória, cujo mérito seria indevassável por ato do Poder Judiciário, salvo caso de flagrante abuso ou excesso; 6) Inexistência de violação ao direito à privacidade, pois trata-se de compartilhamento de informações exclusivamente para fins estatísticos e não de conteúdo de comunicações telefônicas; 7) Referindo a precedentes relatados pelo ministro Dias Toffoli (ADI n.2.390, 2.386, 2.397 e 2.859), pugnou pela legalidade da transferência de dados entre duas entidades públicas que possuem dever de resguardar sigilo; desta forma haveria "transferência" de sigilo e não "quebra" de sigilo; 8) Proporcionalidade da medida tendo em vista os critérios de adequação, necessidade e proporcionalidade em sentido estrito; 9) Adequação da medida à Lei Geral de Proteção de Dados (mesmo que ainda não tenha entrado em vigor), a qual permite o acesso a dados pessoais aos serviços de pesquisa estatística, havido pela lei como sendo de finalidade pública (art. 5°, inciso XVIII).

Neste panorama fático e jurídico contendo argumentos divergentes, a ministra Rosa Weber, em decisão monocrática liminar (referendada pelos demais ministros do STF), amparando-se em fundamentos merecem ser ressaltados e difundidos referiu que essa pesquisa não indicava de forma adequada o objeto, a finalidade e a amplitude da estatística produzida, tampouco a necessidade de disponibilização dos dados. Igualmente que não havia detalhamento de como seriam utilizados os dados e até que a MP não mencionava, de forma explícita, possuir relação com políticas de enfrentamento da pandemia do Covid-19. Para os ilustres julgadores, a Medida Provisória não evidenciava interesse público legítimo envolvendo o compartilhamento de dados dos usuários, considerada eventual necessidade, adequação e proporcionalidade da medida. E ao não definir as razões e modo de uso dos dados pessoais, a MP não permitia a aferição dos requisitos de adequação e necessidade, vale dizer, de verificação da real compatibilidade entre as finalidades pretendidas e a máxima restrição para o atingimento desses objetivos, o que destoava do direito ao devido processo legal. Inclusive, que sob o ponto de vista estrutural, não constava na MP, menção alguma sobre quais seriam os mecanismos técnicos ou administrativos voltados à segurança da informação adotados pelo IBGE, vez que apenas referia a delegação dessa tarefa ao presidente da referida Fundação, motivo pelo qual não assegurava de forma adequada, a efetiva proteção aos direitos fundamentais em debate. Inclusive, esse aspecto chamava a atenção para o fato de poder haver responsabilização de agentes que, de alguma forma, contribuíssem para os danos causados pelo ilegítimo uso ou vazamento de informações confidenciais, inclusive considerando-se que na época a LGPD ainda não tinha começado sua vigência.

Com estas considerações, é possível extrairmos do presente julgado, ainda em caráter provisório, que o direito à privacidade, demasiadamente valioso em contextos democráticos,

precisa ser resguardado contra ingerências indevidas de pessoas físicas, jurídicas, de direito público e privado. Pode-se deduzir, portanto, que o direito fundamental a proteção de dados pessoais não é absoluto, mas que mesmo em casos extraordinários (como a pandemia impondo razões de saúde pública), procedimentos legítimos demandam que sejam atendidos aos princípios da proporcionalidade e transparência, representados pelo cumprimento de requisitos técnicos de segurança da informação, mais acurada e específica finalidade, anonimização dos dados coletados, factível e confiável auditabilidade dos procedimentos e emissão prévia de relatório de impacto, bem como, de haver instrumentos e procedimentos de responsabilização.

Resumindo, a MP não se tornou lei, mas nesse episódio, adveio da jurisprudência a demonstração prática e, pode-se afirmar, a consolidação na Corte Suprema, de que, realmente existe reconhecido o direito fundamental a proteção de dados pessoais, em especial como forma de proteger a dignidade da pessoa humana e seus direitos da personalidade.

6.1. Análise da jurisprudência sobre proteção de dados pessoais no âmbito do Supremo Tribunal Federal

No âmbito do Supremo Tribunal Federal, a pesquisa jurisprudencial por "proteção de dados", bem como suas variantes linguísticas, "proteção dos dados" e "proteção aos dados", bem como suas respectivas flexões no singular, retornou 4 (quatro) acórdãos[155], 19 (dezenove) decisões monocráticas[156] e 1 (uma) decisão da Presidência[157], excluídas as repetições de

[155] ADI n. 3623/DF, Rel. Min. Ricardo Lewandowski, Tribunal Pleno, julgado em 30/10/2019, DJe 04/11/2019; RE n. 766390 AgR/DF, Rel. Min. Ricardo Lewandowski, Segunda Turma, julgado em 24/06/2014, DJe 15/08/2014; MS n. 21729/DF, Rel. Min. Néri da Silveira, Tribunal Pleno, julgado em 05/10/1995 e HC n. 91867/PA, Rel. Min. Gilmar Mendes, julgado em 24/04/2012, DJe 20/09/2012.

[156] MS n. 36063/DF, Rel. Min. Cármen Lúcia, julgado em 26/10/2018, DJe 31/01/2018; RE n. 1064490/RS, Rel. Min. Cármen Lúcia, julgado em 03/03/2020, DJe 11/03/2020; HC n. 177650/RJ, Rel. Min. Luiz Fux, julgado em 29/10/2019, DJe 17/03/2020; RHC n. 169682/RS, Rel. Min. Luiz Fux, julgado em 21/05/2019, DJe 23/05/2019; HC n. 171381/PR, Rel. Min. Cármen Lúcia, julgado em 20/05/2019, DJe 22/05/2019; HC n. 167720/SP, Rel. Min. Luiz Fux, julgado em 08/04/2019, DJe 10/04/2019; ARE n. 1120771/RO, Rel. Min. Roberto Barroso, julgado em 22/08/2018, DJe 31/08/2018; RHC n. 159006/DF, Rel. Min. Luiz Fux, julgado em 02/08/2018, DJe 07/08/2018; RCL n. 23558/DF, Rel. Min. Edson Fachin, julgado em 07/06/2016, DJe 15/06/2016; INQ n. 4045/ES, Rel. Min. Dias Toffoli, julgado em 16/03/2016, DJe 05/04/2016; HC n. 124322/RS, Rel. Min. Roberto Barroso, julgado em 21/09/2015, DJe 29/09/2015; ARE n. 876231/RJ, Rel. Min. Rosa Weber, julgado em 07/05/2015, DJe, 12/05/2015; HC n. 124322 MC/RS, Rel. Min. Roberto Barroso, julgado em 29/10/2014, DJe 04/11/2014; RE n. 554989/SP, Rel. Min. Cezar Peluso, julgado em 16/07/2007, DJe 21/08/2007; AC n. 415 MC/PE, Rel. Min. Cezar Peluso, julgado em 09/09/2004, DJe 20/09/2004; INQ n. 1465/RS, Rel. min. Sydney Sanches, julgado em 08/08/2001, DJe 21/08/2001; RE n. 1100585/RO, Rel. Min. Gilmar Mendes, julgado em 11/04/2019, DJe 15/04/2019 e AI n. 789653/ES, Rel. Min. Ricardo Lewandowski, julgado em 16/03/2010, DJe 25/03/2010.

[157] MS n. 23864 MC/DF, Rel. Min. Carlos Velloso, julgado em 11/01/2001, DJe 02/02/2001.

resultados.[158]

Figura 3 - Nuvem de palavras das decisões monocráticas sobre dados pessoais no STF.

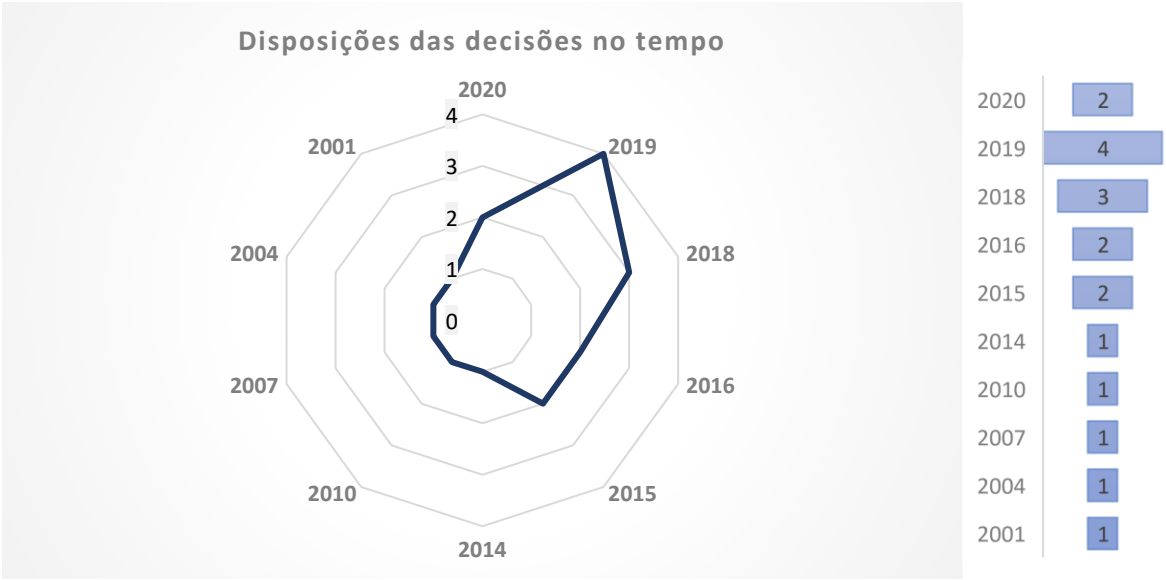


Figura 4 - Disposições das decisões no tempo, STF.

Através de detida análise do gráfico de radar, podemos identificar uma tendência na jurisprudência do Supremo Tribunal Federal, que passou a consolidar entendimento e enfrentar decisões a despeito da proteção de dados pessoais com maior frequência, após a segunda década deste século. Concentrando 11 decisões nos últimos cinco anos e ¼ após a promulgação da Lei Geral de Proteção de Dados Pessoais (2018), muito disso, oxigenados pela produção de

[158] LAPIN. O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS À LUZ DA JURISPRUDÊNCIA DO SUPREMO TRIBUNAL FEDERAL. Disponível em: https://lapin.org.br/2021/03/31/o-direito-fundamental-a-protecao-de-dados-pessoais-a-luz-da-jurisprudencia-do-supremo-tribunal-federal/. Acesso em: 2 mai. 2021.

comentários e literatura doméstica sobre a temática, o que demonstra o compasso jurídico-legislativo para efetivação de direitos fundamentais, como fator necessário, a simbiose do legislativo e judiciário.

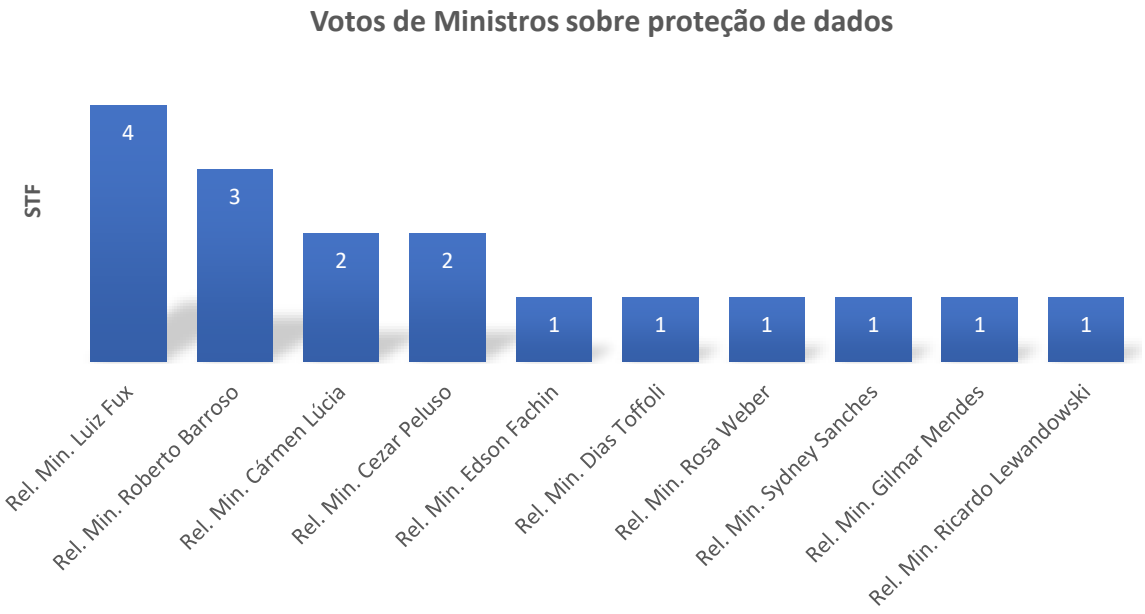


Figura 4 - Relatoria de Ministros acerca da proteção de dados, STF.

Em aporte aos acórdãos selecionados, temos o resultado de 3 (três) acórdãos que delineiam a conceituação considerada adequada no âmbito conceitual de proteção de dados pessoais. Oportunamente, no voto do Min. Carlos Velloso no MS n. 21729/DF, referente ao seu voto na Petição 55 -DF, ele defende que *"o direito à privacidade é inerente à personalidade das pessoas e que a Constituição consagra no art. 5º, inciso X, além de atender a uma finalidade de ordem pública*"[159], convergindo diretamente com a doutrina pátria sobre o tema.

No Recurso Extraordinário de n° 766390 AgR/DF, o relator Min. Ricardo Lewandowski aborda o tema ao explicar que "*a divulgação de dados referentes aos cargos públicos não viola a intimidade e a privacidade, que devem ser observadas na proteção de dados de natureza pessoal"*[160].

Ademais, no caso mais recente sobre o tema, referência na jurisprudência da Suprema Corte, o HC n. 91867/PA, o relator Min. Gilmar Mendes abordou importante diferenciação de conceitos que permeiam o conceito de privacidade e da proteção de dados:

[159] MS n. 21729/DF, Rel. Min. Néri da Silveira, Tribunal Pleno, julgado em 05/10/1995.

[160] RE n. 766390 AgR/DF, Rel. Min. Ricardo Lewandowski, Segunda Turma, julgado em 24/06/2014, DJe 15/08/2014.

> Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados.[161]

Outra frente, quanto às decisões monocráticas, apenas 14 (quatorze) decisões, referem-se à conceituação da proteção de dados pessoais. Das listadas acima, no âmbito do Supremo Tribunal Federal, apenas 10 (dez) citam o entendimento proferido pelo Min. Gilmar Mendes, ora relator, no HC n. 91867/PA, conforme reproduzido acima. Logo, verifica-se que é um entendimento recorrente utilizado nas decisões da Suprema Corte quando o tema "proteção de dados pessoais" é posto em discussão, conforme os casos paradigmáticos:

Leading Cases
MS n. 21729/DF, Voto Min. Carlos Velloso
RE n. 766390 AgR/DF, Relator Min. Ricardo Lewandowski
HC n. 91867/PA, Relator Min. Gilmar Mendes

No que tange aos 4 (quatro) restantes, o relator Min. Edson Fachin, em sua decisão na Rcl 23558/DF, exprime o entendimento de que, no caso concreto, *"a realização de carga dos autos e retirada de cópias referentes ao conteúdo das declarações prestadas por testemunha protegida, não legitima a subtração do conteúdo do depoimento com base na proteção aos dados da testemunha*"[162]. As decisões proferidas nos RE n. 554989/SP e AC n. 415 MC/PE, ambos de relatoria do Min. Cezar Peluso, compartilham do mesmo entendimento, qual seja:

> A proteção aos dados bancários configura manifestação do direito à intimidade e ao sigilo de dados, garantido nos incs. X e XII do art. 5º da Constituição Federal, só podendo cair à força de ordem judicial ou decisão de Comissão Parlamentar de Inquérito, ambas com suficiente fundamentação.[163]

A decisão monocrática proferida no Recurso Extraordinário de n°. 1.100.585/RO pelo relator Ministro Gilmar Mendes, revela importante entendimento recorrente do STF de que *"a*

[161] HC n. 91867/PA, Rel. Min. Gilmar Mendes, julgado em 24/04/2012, DJe 20/09/2012.

[162] RCL n. 23558/DF, Rel. Min. Edson Fachin, julgado em 07/06/2016, DJe 15/06/2016.

[163] AC n. 415 MC/PE, Rel. Min. Cezar Peluso, julgado em 09/09/2004, DJe 20/09/2004.

divulgação de dados referentes aos cargos públicos não viola a intimidade e a privacidade, que devem ser observadas na proteção de dados de natureza pessoal".[164] Por fim, a única decisão da Presidência que aborda as palavras-chave analisadas não tangencia o conceito de proteção de dados pessoais.

Portanto, em cuidadosa análise, verifica-se que a jurisprudência do STF com relação a proteção de dados é bem uniforme, constatando-se que (i) a jurisprudência do STF é pacífica em entender que há diferenças entre a proteção constitucional à comunicação de dados, e não dos dados em si; (ii) que a intimidade e a privacidade devem ser observadas na proteção de dados de natureza pessoal; e que (iii) o direito à privacidade é inerente à personalidade das pessoas.

Tudo isso parece ter se concretizado quando do julgamento das ADI's[165], de relatoria da Min. Rosa Weber. As ações diretas foram propostas em face da Medida Provisória 954/2020, que dispunha sobre o compartilhamento de dados não anonimizados – nomes, números de telefones e endereços de todos os brasileiros que têm acesso a telefonia fixa e móvel – por empresas de telecomunicação ao Instituto Brasileiro de Geografia e Estatística – IBGE.

Na ocasião, o Supremo Tribunal Federal, ao referendar com maioria expressiva de 10 votos a medida cautelar concedida pela relatora, reconheceu um **direito fundamental autônomo** – isto é, diferente da proteção à intimidade e à privacidade à proteção de dados pessoais, que seria decorrente:

> de uma compreensão integrada do texto constitucional lastreada (*i*) no direito fundamental à dignidade da pessoa humana, (*ii*) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (*iii*) no reconhecimento da centralidade do *Habeas Data* enquanto instrumento de tutela material do direito à autodeterminação informativa. (voto do Min. Gilmar Mendes na ADI n. 6387 MC-Ref/DF, Rel. Min. Rosa Weber, julgado em 7/5/2020, pendente de publicação.

A começar de seu reconhecimento – ressaltado, todavia, sua natureza não absoluta –, no caso concreto, o Tribunal suspendeu a vigência da MP 954/2020, por entender que não estava definido como e para que os dados pessoais seriam coletados, uma vez que, ao definir como objetivo apenas "produção estatística oficial", o diploma não seria necessário nem proporcional.

---

[164] RE n. 1100585/RO, Rel. Min. Gilmar Mendes, julgado em 11/04/2019, DJe 15/04/2019.

[165] ADI n. 6387 MC-Ref/DF, ADI n. 6388 MC-Ref/DF, ADI n. 6389 MC-Ref/DF, ADI n. 6390 MC-Ref/DF e ADI n. 6393 MC-Ref/DF, de relatoria da Min. Rosa Weber.

A partir da definição dessa finalidade ampla, não seria possível mensurar os efeitos futuros de tal coleta de dados, o que poderia causar impactos relacionados à democracia a partir da vigilância expressiva do Estado.[166]

A MP impugnada caducou[167] e as ADI's devem ter a perda de seu objeto reconhecida sem o julgamento de mérito. De todo modo, ainda que não se possa declarar a inconstitucionalidade da medida provisória, incontestável é o reconhecimento da proteção de dados pessoais como um direito fundamental autônomo.

Com essa decisão histórica, com a entrada em vigor da Lei Geral de Proteção de Dados (Lei 13.709/2018) e com a operacionalização da Autoridade Nacional de Proteção de Dados, a proteção constitucional aos dados pessoais parece tomar contornos concretos, devendo o Estado garantir a sua proteção e observância. Nesse sentido, torna-se relevante a discussão a respeito de possíveis abordagens à operacionalização desse direito pelo Supremo Tribunal Federal à luz do surgimento e das doutrinas de proteção de dados nacionais e internacionais.

Além disso, outro caso histórico foi iniciado pelo STF duas semanas depois (maio de 2020), com dois juízes já divulgando seus pareceres. A principal questão neste segundo caso é se as plataformas da Internet poderiam implementar a tecnologia de criptografia a um nível que pudesse limitar e até mesmo evitar o acesso das autoridades policiais aos dados armazenados ou em trânsitos necessários para investigar crimes. Novamente, o processo ADPF 403, que tem os mesmos efeitos das ADIs, discutiu a violação dos direitos fundamentais à privacidade e ao sigilo da comunicação de dados.

"Direitos Digitais são Direitos Fundamentais": com essa forte afirmação, o ministro Edson Fachin, relator, deu seu voto excluir qualquer interpretação da constituição que permitiria a uma ordem judicial fornecer acesso excepcional ao conteúdo de mensagem criptografada de ponta a ponta ou que, por qualquer outro meio, enfraqueceria a proteção criptográfica de aplicativos da Internet.

A Min. Rosa Weber destacou em sua decisão *que "as últimas 3 décadas foram uma corrida armamentista de tecnologias de proteção e violações de privacidade. A lei não pode ser ignorada e deve preservar o equilíbrio entre a privacidade e o bom funcionamento do Estado".* Afirmou ainda que "*a criptografia, como recurso tecnológico, tem assumido especial*

[166] MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. JOTA. Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020>. Acesso em: 02 maio 2021.

[167] ATO DECLARATÓRIO DO PRESIDENTE DA MESA DO CONGRESSO NACIONAL Nº 112, DE 2020. Diário Oficial da União de 20/8/2020. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Congresso/adc-112-mpv954.htm. Acesso em: 02 maio 2021.

importância na concretização dos direitos humanos". O caso ainda está em trâmite e aguarda a votação dos outros 9 Ministros. No entanto, as duas opiniões já publicadas são um avanço e mostram uma mudança drástica na percepção e no entendimento do mais alto Corte do Brasil em relação aos direitos de privacidade e proteção de dados.

Apesar dessa decisão histórica, o Brasil ainda carece de uma infraestrutura institucional para supervisionar e fazer cumprir os direitos de proteção de dados. ANPD foi criada pela Lei Geral de Proteção de Dados ("LGPD"), mas ainda não foi estabelecida.

A LGPD foi aprovada em 2018, com um período de adaptação inicial de 18 meses, que logo foi alterado para ser aumentado em 6 meses, deixando a vigência para agosto de 2020. Paralelamente, uma proposta de alteração da Constituição Federal que visa incluir a proteção de dados pessoais na lista dos direitos fundamentais. A proposta foi aprovada por unanimidade pelo Senado e por uma comissão parlamentar especial da Câmara dos Deputados. Agora, ele precisa ser aprovado por dois terços desta casa.

Devido à pandemia do COVID-19, um novo projeto de lei e outro decreto adiou a entrada em vigor da LGPD para 2021. O projeto já foi votado pelo Senado e pela Câmara dos Deputados e foi para a Presidência que ratificou, mantendo a nova lei com a data de vigência até agosto de 2020.

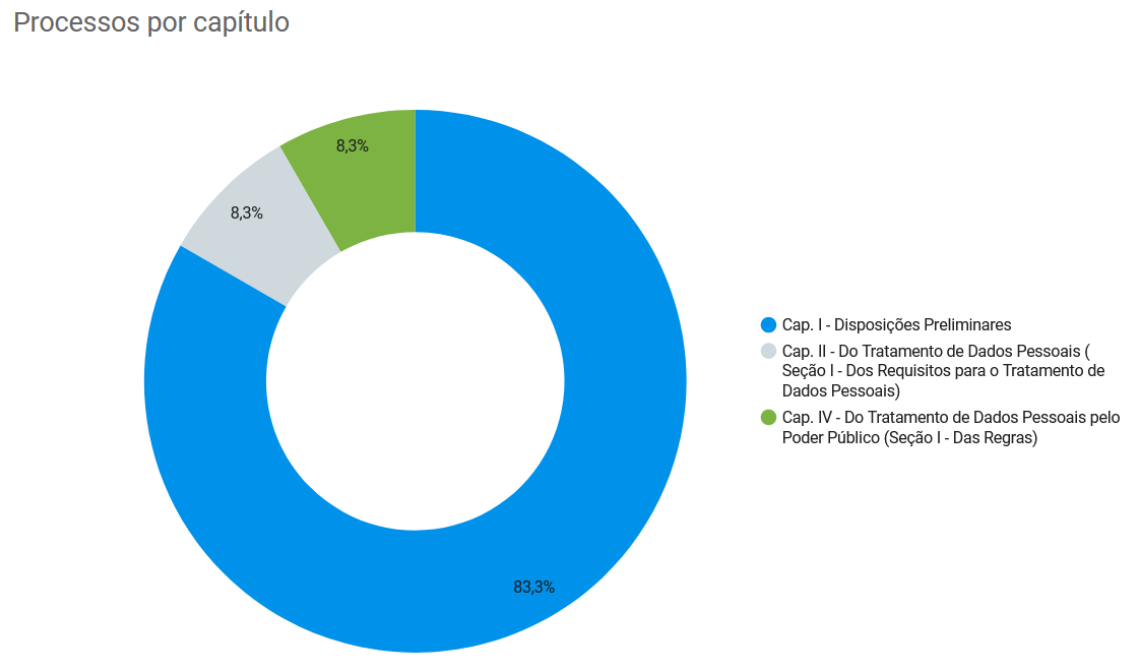
No entanto, ela altera LGPD para permitir penalidades e ações de execução apenas até agosto de 2021. Ademais, a Autoridade Nacional de Proteção de Dados (ANPD), criada em dezembro de 2018, agora criada, porém vinculada ao Executivo.

O que é notável é que até que o projeto de emenda à constituição não seja aprovado, o que pode não acontecer em um futuro próximo devido a distúrbios políticos, essa decisão do Supremo Tribunal Federal já abre caminho para o reconhecimento do direito à proteção de dados na prática.

Quando avaliamos as decisões judiciais no âmbito da corte suprema, relativos à interpretação da Lei 13.709/2018, retornamos as pesquisas nas bases de dados com 13 (treze)[168]

[168] (STF - MS: 37574 DF 0110268-37.2020.1.00.0000, Relator: GILMAR MENDES, Data de Julgamento: 26/05/2021, Data de Publicação: 28/05/2021); (STF - MS: 37574 DF 0110268-37.2020.1.00.0000, Relator: GILMAR MENDES, Data de Julgamento: 26/02/2021, Data de Publicação: 02/03/2021); (STF - MS: 37537 DF 0108673-03.2020.1.00.0000, Relator: GILMAR MENDES, Data de Julgamento: 25/05/2021, Data de Publicação: 28/05/2021); (STF - MS: 37537 DF 0108673-03.2020.1.00.0000, Relator: GILMAR MENDES, Data de Julgamento: 26/02/2021, Data de Publicação: 02/03/2021); (STF - MS: 37636 DF 0036489-15.2021.1.00.0000, Relator: ROSA WEBER, Data de Julgamento: 19/01/2021, Data de Publicação: 22/01/2021); (STF - MS: 37636 DF 0036489-15.2021.1.00.0000, Relator: ROSA WEBER, Data de Julgamento: 29/01/2021, Data de Publicação: 02/02/2021); (STF - ADI: 4829 DF 9965406-75.2012.1.00.0000, Relator: ROSA WEBER, Data de Julgamento: 22/03/2021, Tribunal Pleno, Data de Publicação: 12/04/2021); (STF - MS: 38061 DF 0057683-71.2021.1.00.0000, Relator: RICARDO LEWANDOWSKI, Data de Julgamento: 12/07/2021, Data de Publicação: 13/07/2021); (STF - MS: 38043 DF 0057413-47.2021.1.00.0000, Relator: RICARDO LEWANDOWSKI, Data de Julgamento: 08/07/2021, Data de

casos já devidamente apreciados pelo Supremo Tribunal de Justiça em ações que versem sobre a proteção de dados pessoais, vejamos:



LGPD - Capítulo subjacente	Decisões
Cap. I - Disposições Preliminares	4
Cap. IV - Do Tratamento de Dados Pessoais pelo Poder Público (Seção I - Das Regras)	3
Cap. II - Do Tratamento de Dados Pessoais (Seção I - Dos Requisitos para o Tratamento de Dados Pessoais)	1

Figura 5 - Demonstrativo de processos por capítulo da LGPD.

Ainda na perspectiva qualitativa temos a subdivisão de importância no âmbito de julgamento das demandas, classificadas para fim de sedimentação teórica entre "didática", "polêmica", "regular", sendo duas consideradas didáticas, quatro decisões polêmicas e sete regulares, no que tange à repercussão da decisão no âmbito da proteção de dados e duas delas merecem relevo, pois contribuem para consolidação da interpretação da norma federal que instituiu a Lei Geral de Proteção de Dados no país, e que são consideradas didáticas para boas as práticas e interpretação da proteção de dados na ADI 4829/DF que versava sobre a dispensa de licitação na contratação de serviços de tecnologia da informação estratégicos:

Publicação: 12/07/2021); (STF - MS: 38006 DF 0056313-57.2021.1.00.0000, Relator: NUNES MARQUES, Data de Julgamento: 28/06/2021, Data de Publicação: 30/06/2021); (STF - MS: 37968 DF 0055744-56.2021.1.00.0000, Relator: NUNES MARQUES, Data de Julgamento: 14/06/2021, Data de Publicação: 17/06/2021); (STF - Pet: 9697 DF 0054832-59.2021.1.00.0000, Relator: EDSON FACHIN, Data de Julgamento: 07/07/2021, Data de Publicação: 09/07/2021); (STF - AO: 2549 DF 0054222-91.2021.1.00.0000, Relator: GILMAR MENDES, Data de Julgamento: 21/06/2021, Data de Publicação: 23/06/2021).

> [...] 5. Os postulados constitucionais da inviolabilidade do sigilo de dados pessoais (art. 5º, XII e XXXIII, da CF) e da soberania nacional (arts. 1º, I, e 170, I, da CF) reclamam a imposição de restrições ao tratamento de dados pessoais, por entidades privadas, para fins de segurança pública, defesa nacional ou segurança da informação do Estado e dos administrados. 6. Os arts. 170, parágrafo único, e 173, caput, da CF autorizam o legislador a restringir o livre exercício de atividade econômica para preservar outros direitos e valores constitucionais, destacando-se, no caso de serviços estratégicos de tecnologia da informação contratados pela União, os imperativos da soberania, da segurança nacional e da proteção da privacidade de contribuintes e destinatários de programas governamentais. Interesse público a legitimar decisão do legislador no sentido da prestação de serviços estratégicos de tecnologia da informação com exclusividade por empresa pública federal criada para esse fim. 7. Inocorrência de vulneração aos arts. 2º, 22, XXVII, 37, XXI, 173, caput e § 4º, e 246 Constituição da República. 8. Ação direta de inconstitucionalidade julgada improcedente. (STF - ADI: 4829 DF 9965406-75.2012.1.00.0000, Relator: ROSA WEBER, Data de Julgamento: 22/03/2021, Tribunal Pleno, Data de Publicação: 12/04/2021)

Logo, podemos concluir que a proteção de dados pessoais foi utilizada como subsídio para declarar constitucional dispositivo de lei em que se dispensa a licitação a fim de permitir a contratação direta do Serviço Federal de Processamento de Dados (Serpro), pela União, para prestação de serviços de tecnologia da informação considerados estratégicos, assim especificados em atos de ministro de Estado, no âmbito do respectivo ministério. Há evidente interesse público a justificar que serviços de tecnologia da informação a órgãos como a Secretaria do Tesouro Nacional e a Secretaria da Receita Federal, integrantes da estrutura do Ministério da Economia, sejam prestados com exclusividade por empresa pública federal criada para esse fim, como é o caso do Serpro (ADI 4829/DF).

Outra decisão sumariamente didática, trata-se de petição 9697/DF, instaurada a fim de proceder ao cumprimento referente às questões sanitárias para a prevenção e combate à COVID-19 nas comunidades quilombolas tais como determinado na ADPF 742, *in verbis*:

> [...] “A LGPD permite que dados anonimizados ou pseudonimizados sejam disponibilizados sendo os dados pessoais gerados com o devido tratamento nas hipóteses de cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, inciso II), devendo ser considerada a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização (art. 7º, § 3º). Ressalta-se que os dados anonimizados são considerados como dados pessoais para a LGPD (art. 12). Após o

tratamento de dados pessoais pelo poder público como realizado com a base existente em questão, eles ‘deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral"(art. 25). Destaca-se que o Ministério da Saúde tem sistematizado e publicizado microdados de casos sobre internações, óbitos e vacinados, informando-os de modo anonimizado ou pseudonimizado. Nos microdados de vacinação, há a identificação de tratar-se de quilombolas, identificam características pessoais, disponibilizando agregação espacial. O Ministério da Saúde publiciza dados sobre a situação do coronavírus em indígenas (https://saudeindigena.saúde.gov.br/corona). A base Sivep-Gripe (https://opendatasus.saúde.gov.br/dataset/bd-srag-2021 e https://opendatasus.saúde.gov.br/dataset/bd-srag-2020), que reúne a quase totalidade de internações, casos graves e óbitos, identifica, para o caso dos indígenas, a etnia, junto com um banco que detalha os procedimentos de saúde, identifica o estabelecimento de atendimento, município e diversas características pessoais. O acesso público aos dados permite um acompanhamento da sociedade de forma transparente e permite estudos e pesquisas que auxiliam na compreensão da dinâmica do vírus bem como no seu enfrentamento mais assertivo e tempestivo.” E os requerentes: “É evidente que para cumprimento da decisão colegiada é insuficiente a simples existência, em formulário próprio, de campo destinado à informação de contaminação de quilombolas pelo Coronavírus, sobretudo se essas informações não forem sistematizadas e disponibilizadas publicamente. Tanto o é que, conforme informações prestadas nos autos (mov. 63), apenas 02 (dois) casos de Covid foram notificados entre quilombolas até o momento em todo o país. A ineficiência da ação do estado fica ainda mais evidente quando o dado irrisório é confrontado com levantamento autônomo da Conaq que identifica, sem utilizar as ferramentas e estruturas oficiais de Estado, 5429 casos confirmados, 1487 casos monitorados e 279 óbitos. (...) A ausência de ampla e periódica disponibilização dos dados não permite aferir se as informações relacionadas ao tema existem e se as poucas políticas públicas adotadas são eficientes. No mesmo sentido, a ausência de informações inviabiliza o controle social democrático das políticas públicas, inclusive para aferir se as medidas adotadas pela União em função da decisão proferida por esse E. Tribunal têm atingido os objetivos esperados.” E requerem seja a União intimada para que: 7) Adote medidas de fiscalização quanto ao controle da obrigatoriedade do preenchimento das informações disponibilizadas referentes ao quesito raça/cor/etnia no registro de casos de Covid, eis que não existem dados fiáveis no tema, a despeito da obrigatoriedade de registro; 8) Adote medidas de coordenação, promoção e meios orçamentários para formação de agentes locais na operacionalização dos registros de casos de Covid-19 em comunidades quilombola; 9) Adote as medidas necessárias destinadas a dar ampla

> e periódica publicidade aos dados relativos à contaminação de quilombolas pelo Coronavírus, de forma a viabilizar a realização de políticas públicas e o controle social destas. De fato, consta no acórdão deste Supremo Tribunal Federal: "A verificação da efetividade de certa política pública exige monitoramento e avaliação qualificada, garantindo-se a adequada alocação de recursos considerados os objetivos e metas propostos. Para a consecução desse objetivo, é imprescindível a consolidação de insumos a subsidiarem a adequada atuação dos órgãos, autarquias e instituições. O rígido acompanhamento da doença, levando em conta evolução do contágio, da taxa de recuperação e de letalidade, pressupõe consideração das especificidades da população que se pretende atender. A inclusão do quesito raça/cor/etnia no registro dos casos propicia o levantamento, pelo Poder Público, de marcadores sociais que permitem a definição de programas destinados à adequada resposta à crise sanitária." A determinação da inclusão do quesito raça/cor/etnia nos registros de casos serve justamente a permitir o levantamento e a transparência desses dados a fim de aprimorar a execução das políticas públicas, com as advertências e cuidados necessários no seu tratamento e anonimização, na forma do art. 5º, XI, da Lei n.º 13.709/2018, como bem alertou a PGR. É nesses termos que se permitiu aos indígenas, como ora se determina à comunidades quilombolas, que se proceda à publicização dos dados na forma requerida. Defiro, assim, os pedidos da requerente. Intime-se a União e, pessoalmente, o Ministro da Saúde, para comprovar o cumprimento, no prazo de 15 dias. Publique-se. Intimem-se nos termos acima. Brasília, 7 de julho de 2021. Ministro Edson Fachin Relator Documento assinado digitalmente. (STF - Pet: 9697 DF 0054832-59.2021.1.00.0000, Relator: EDSON FACHIN, Data de Julgamento: 07/07/2021, Data de Publicação: 09/07/2021)

Neste período, compreendido de setembro de 2020 a agosto de 2021, temos a flutuação de decisões no âmbito do STF, que vieram a fundamentar suas decisões sobre proteção de dados pessoais, no mesmo compasso em que a lei se difundia no âmbito acadêmico e por consequência no leito jurisdicional.

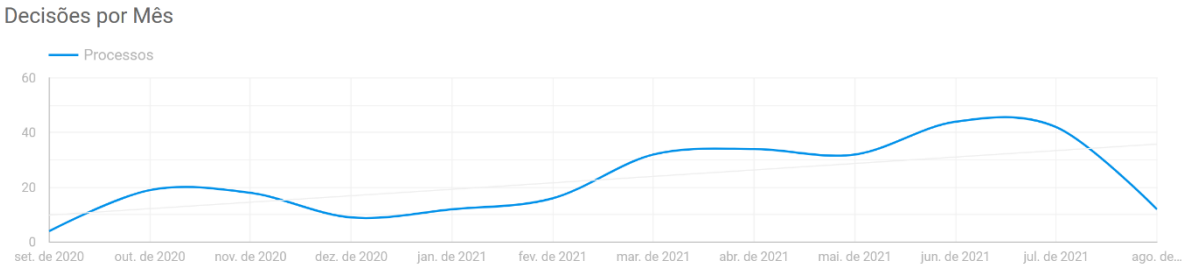


Figura 6 - Linha do tempo de decisões por mês – Set.2020 a Ago.2021.

Não obstante, a referida pesquisa buscou compreender, em alguma medida aferir atuação dos membros daquela Corte, no que tange as suas fundamentações sobre a proteção de dados pessoais, que tem por objetivo ao fim e ao cabo, parametrizar as probabilidades de construção da interpretação no âmago da privacidade e proteção de dados no Brasil.

Figura 7 - Gráfico com número de decisões por ministro do STF.

Embora as decisões sejam reduzidas frente ao emaranhado de litígio judicial pendente no país, o referido estudo é parâmetro para início de interpretação da consolidação jurisprudencial no âmbito do STF quanto relativo a privacidade e proteção de dados pessoais.

Ademais, alocou-se no presente trabalha a visualização de natureza das demandas, conforme sua amplitude, natureza jurídica, causa de pedir e efeitos práticos, onde foi possível verificar que das discussões tangentes à dados no âmbito do Supremo Tribunal Federal, temos o Mandado de Segurança como remédio mais acionado para tutelar garantias no âmbito dos dados, o que revela em alguma medida ausência de adequação do ente público à LGPD.

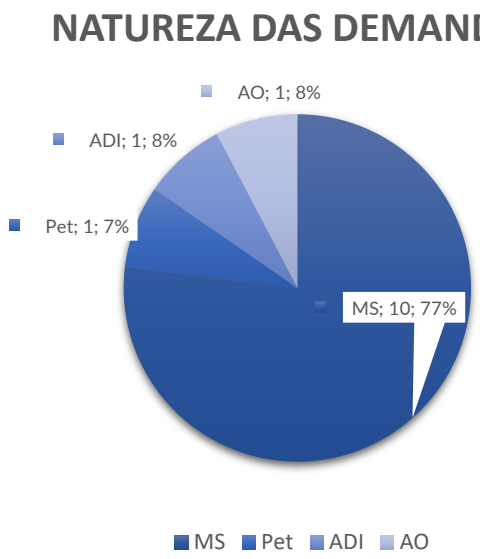


Figura 8 - Gráfico com ocorrência de demandas no STF sobre o tema

Quanto a linha do tempo do proferimento das decisões, podemos notar duas decisões no início do ano de 2021, e posteriormente a Corte concentrando quatro decisões sobre o tema na iminência da sua eficácia no plano normativo, em que pese a Medida Provisória 959/2020 incidiu na prorrogação da Lei 13.709/2018, que passou a expandir seus efeitos em 3 de maio de 2021, vindo posteriormente, de forma simbólica e muito pertinente a pautar e julgar nos entre os dias 25 e 26 de maio de 2021, quatro demandas no âmbito da proteção de dados pessoais.

Figura 9 - Linha do tempo com ocorrência por data das decisões no âmbito do STF.

Não menos importante e de forma a instruir o observador para qualidade das decisões apreciadas, buscou-se sistematizar o presente cotejo para classificação das decisões a partir de duas perspectivas, sendo elas: a) classificação das decisões propriamente ditas, distribuídas em didáticas, polêmica e regular; b) sua relevância, a partir da classificação entre relevantes e muito relevantes, de acordo com seu nível de acuidade e sua contribuição teórica-jurisprudencial.

CLASSIFICAÇÃO DAS DECISÕES

	Didática	Polêmica	Regular
EDSON FACHIN	1	0	0
ROSA WEBER	1	0	1
RICARDO LEWANDOWSKI	0	2	0
NUNES MARQUES	0	2	0
GILMAR MENDES	0	0	3

Figura 10 - Classificação das decisões proferidas pelo STF.

RELEVÂNCIA DAS DECISÕES

	Muito Relevante	Relevante
RICARDO LEWANDOWSKI	2	0
NUNES MARQUES	2	0
EDSON FACHIN	1	0
ROSA WEBER	1	1
GILMAR MENDES	1	2

Figura 11 - Classificação da relevância das decisões proferidas pelo STF.

Diante de tais elementos, é possível inferir que a Ministra Rosa Weber e o Ministro Gilmar Mendes se destacam dentro da corte, concentrando cinco decisões entre elas duas consideradas muito relevantes para o tema da proteção de dados pessoais, o que indica inclinação para eventuais trilhas de construção teórica naquele Tribunal e para sedimentação da privacidade e sua correta aplicação.

Não obstante, as demais decisões, seguem referidamente catalogadas na listagem abaixo, enquanto parâmetro qualitativo e quantitativo da tutela dos dados pessoais no STF.

Natureza	Número CNJ	Tipo de decisão	Temática	Ministro	Data do Julgamento
Pet	0054832-59.2021.1.00.0000	Didática	Muito relevante	EDSON FACHIN	07/07/2021
ADI	9965406-75.2012.1.00.0000	Didática	Muito relevante	ROSA WEBER	22/03/2021
MS	0057413-47.2021.1.00.0000	Polêmica	Muito relevante	RICARDO LEWANDOWSKI	08/07/2021
MS	0057683-71.2021.1.00.0000	Polêmica	Muito relevante	RICARDO LEWANDOWSKI	12/07/2021
MS	0055744-56.2021.1.00.0000	Polêmica	Muito relevante	NUNES MARQUES	14/06/2021
MS	0056313-57.2021.1.00.0000	Polêmica	Muito relevante	NUNES MARQUES	28/06/2021
MS	0036489-15.2021.1.00.0000	Regular	Relevante	ROSA WEBER	19/01/2021
MS	0110268-37.2020.1.00.0000	Regular	Relevante	GILMAR MENDES	26/05/2021
MS	0036489-15.2021.1.00.0000	Regular	Relevante	ROSA WEBER	19/01/2021
AO	0054222-91.2021.1.00.0000	Regular	Muito relevante	GILMAR MENDES	21/06/2021
MS	0108673-03.2020.1.00.0000	Regular	Relevante	GILMAR MENDES	25/05/2021
MS	0108673-03.2020.1.00.0000	Regular	Relevante	GILMAR MENDES	25/05/2021
MS	0110268-37.2020.1.00.0000	Regular	Relevante	GILMAR MENDES	26/05/2021

Figura 12 - Classificação completa das decisões mencionadas

Obviamente é cedo para trazer qualquer tipo de conclusão sobre a tendência da Corte para o tema. Em especial, porque o universo de dados ainda é limitante para maiores afirmações. Todavia, podemos inferir com base nas decisões até aqui proferidas e avaliadas, que a Corte se mantém integrada ao espírito do legislador em aspectos que tangem à construção da norma prevista nos capítulos preliminares da Lei. Em igual medida, quando se debruçou sobre o tratamento de dados pessoais entre particulares, na perspectiva de freios e contrapesos; e na órbita do Poder Público, desaguando ao espírito de suas decisões pautando o titular dos dados como cerne de sua eficácia, preservando à integridade dos dados em caráter coletivo, preservando o espírito maior da tutela de dados pessoais e sua eficácia no plano prático mediante tutela do Poder Judiciário.

6.2. Análise da jurisprudência sobre proteção de dados no âmbito do Superior Tribunal de Justiça

Discute-se, neste artigo, a transformação da jurisprudência do Superior Tribunal de Justiça no tocante à proteção de dados pessoais, desde o reconhecimento, na década de 1990, de um novo sentido de privacidade que a tutela da autodeterminação informativa passou a lhe emprestar na Europa, sobretudo, mas, também, entre nós brasileiros, até a edição da Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais ou LGPD.

Parte-se da análise da evolução do conceito de privacidade, que inicialmente era relacionado à ideia de exclusão de terceiros, para a atual acepção do termo como a possibilidade

de cada indivíduo determinar as informações sobre si que merecem ser protegidas. Prossegue-se com o exame dos julgados do STJ que interpretaram o artigo 43 do Código de Defesa do Consumidor e sua incidência sobre os cadastros negativos de crédito. Em seguida, dirige-se o foco para os cadastros positivos objeto da Lei 12.414/2001, a qual serve de importante fundamento para as teses aprovadas nos recursos repetitivos que cuidaram dos sistemas de avaliação de risco de crédito, ou *credit scoring*, que têm em seu núcleo a preocupação de proteger adequadamente os dados pessoais, a fim de evitar discriminações injustas e indevidas.

Por fim, estuda-se a jurisprudência a respeito da remoção de dados pessoais da internet, antes e depois do Marco Civil da Internet, bem como a emergência, em um único caso, de discussão acerca da possibilidade de se reconhecer, entre nós, a despeito da ausência de norma legal específica, a existência de um direito ao esquecimento, no sentido de um direito à desindexação de conteúdos da internet, ao modo daquele positivado no Regulamento Geral de Proteção de Dados, editado pela União Europeia em 2016.

A propósito, em 2013, o STJ julgou dois casos, com resultados diametralmente opostos, nos quais se discutia se a divulgação televisiva de matérias jornalísticas sobre crimes de grande repercussão, ocorridos há muito tempo, poderia comprometer o direito ao esquecimento dos interessados. Nessa acepção, o direito ao esquecimento não se confunde com o direito à desindexação ou ao apagamento de dados pessoais. Por isso, tais casos não foram incluídos no presente texto.

6.2.1. Análise dos cadastros negativos e positivos de crédito

Muito antes de se cogitar, no Brasil, a adoção de lei específica destinada à proteção de dados pessoais, já se fazia referência em julgados do Superior Tribunal de Justiça à emergência de um novo conceito de privacidade, a merecer tutela distinta daquela tradicionalmente reservada à privacidade como exclusão de terceiros. Em 1995, o Ministro Ruy Rosado, no REsp 22.337-8/RS, fazia alusão ao direito fundamental à autodeterminação informativa, tal como reconhecido na Alemanha, no contexto de uma crescente vulnerabilidade do indivíduo ante a coleta e o armazenamento de informações que invadem sua intimidade sem o seu consentimento e sem dispor de meios eficazes para ter acesso a essa informação, retificá-la ou cancelá-la.

É bem verdade que os primeiros acórdãos a mencionar esse novo conceito de privacidade diziam respeito à aplicabilidade do Código de Defesa do Consumidor aos cadastros negativos de crédito. Foram as primeiras oportunidades em que o STJ se debruçou sobre o tema.

Como se sabe, o art. 43 do CDC garante ao interessado o direito de acesso a seus registros, bem como o direito de corrigir a informação neles existentes, além de conter regra de prescrição. Assim é que o Ministro Ruy Rosado, no julgamento do mencionado recurso especial, associou expressamente a tutela consumerista do direito de acesso e retificação de registros (art. 43 do CDC) à matriz constitucional da proteção da intimidade e da vida privada (art. 5º, X, da Constituição Federal), indicando o avanço significativo de nosso ordenamento rumo a uma proteção adequada a essa outra dimensão da privacidade.

Em 2001, no julgamento do Resp. 306.570, Relatora a Ministra Eliana Calmon, reconheceu-se que o "contribuinte ou o titular da conta bancária tem direito à privacidade em relação aos seus dados pessoais". No Resp. 1.168.547/RJ, Relator o Ministro Luís Felipe Salomão, julgado em 2010, assentou-se a existência de um novo conceito de privacidade, bem como a necessidade de consentimento do interessado para a divulgação de informação pessoal a seu respeito, pois, com o desenvolvimento da tecnologia, a tutela da privacidade passa a ter por ponto de referência o consentimento do interessado para "dispor com exclusividade sobre as próprias informações, nelas incluindo o direito à imagem".

Posteriormente, o STJ passa a examinar questões atinentes ao cadastro positivo de crédito, instituído pela Lei 12.414/2011, que ampliou o alcance das normas referentes aos bancos de dados e aos cadastros de consumidores, visto que, além do direito de acesso e do direito à correção da informação, já previstos no CDC, incluiu, expressamente, entre os direitos do cadastrado: a) o direito de obter o cancelamento do cadastro; b) o direito de conhecer os principais elementos e critérios considerados para a análise de risco; c) o direito de ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento; d) o direito de solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados e) o direito de ter os seus dados pessoais utilizados de acordo com a finalidade para a qual foram coletados.

Válido destacar, o REsp 1.348.532/SP, relatado pelo Ministro Salomão, que se extrai o seguinte teor:

> [...] **3. É abusiva e ilegal cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, sem que seja dada opção de discordar daquele compartilhamento.** (STJ - REsp: 1348532 SP 2012/0210805-4, Relator: Ministro LUIS FELIPE SALOMÃO, Data

> de Julgamento: 10/10/2017, T4 - QUARTA TURMA, Data de Publicação: DJe 30/11/2017)

Com a leitura da decisão acima, podemos notar a presença do consentimento e a autodeterminação informativa, que formam importante base legal para o tratamento e fundamento da proteção de dados, além de serem instrumentos do livre desenvolvimento da personalidade, um outro fundamento legal. E, assim, a Lei Geral parece formar uma teia de proteção, em que cada fundamento está ligado a um direito que, por sua vez, conecta-se a um princípio, formando um todo coerente que confere efetividade e concretude à proteção de dados pessoais.

6.2.2. O (*credit score*) ou avaliação de risco de crédito no mercado de consumo

O grande desafio, no que tange ao cadastro positivo e aos direitos dos cadastrados, apareceu quando o STJ foi levado a analisar a enorme gama de processos nos quais se discutia os sistemas de avaliação de risco de crédito (escore de crédito ou *credit score*), tema que originou dois recursos repetitivos e uma súmula.

No primeiro dos recursos repetitivos sobre a questão, REsp 1.457.199/RS6, foram aprovadas as seguintes teses:

> **1)** O sistema *credit scoring*, é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito) **2)** Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art., da Lei 12.414/2011 (lei do cadastro positivo). **3)** Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei 12.414/2011. **4)** Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas. **5)** O desrespeito aos limites legais na utilização do sistema credit scoring187, configurando abuso no exercício desse direito (art. do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados

> incorretos ou desatualizados. (STJ - REsp: 1457199 RS 2014/0126130-2, Relator: Ministro PAULO DE TARSO SANSEVERINO, Data de Julgamento: 12/11/2014, S2 - SEGUNDA SEÇÃO, Data de Publicação: DJe 17/12/2014)

Na ocasião, o relator, Ministro Paulo de Tarso Sanseverino, de maneira inovadora, já que anteriormente à edição do novo Código de Processo Civil não havia previsão legal a respeito, realizou a primeira audiência pública no STJ, o que muito contribuiu para o exame de todos os pontos de vista envolvidos, assim como para o aprofundamento da discussão acerca das lacunas existentes em nosso ordenamento no que tange à proteção de dados pessoais, em contraste com o que já se via em outros países.

O voto-vogal do Ministro Ricardo Villas-Boas, enfatizou a importância daquele julgamento para consolidar, no Brasil, a partir dos poucos dispositivos existentes em nosso ordenamento, especialmente no CDC e na lei do cadastro positivo, alguma proteção à privacidade dos consumidores, a fim de evitar que sejam injustamente discriminados no acesso ao crédito. Ademais, com lastro na doutrina de Laura Mendes, procurou-se demonstrar que os sistemas de avaliação de crédito têm por finalidade identificar os melhores consumidores, ou seja, aqueles que apresentam menor risco, e que isso pressupõe, por outro lado, a identificação daqueles que poderiam ser considerados os piores consumidores, os quais, por essa razão, supostamente teriam negado seu acesso a bens e serviços. A ausência de uma adequada proteção dos dados pessoais pode, assim, causar graves danos aos consumidores. Não é à toa que, em regra, os sistemas automatizados de decisão somente são admitidos se existirem medidas que assegurem que o titular dos dados possa apresentar sua defesa e se a decisão relacionar-se à celebração ou à execução de um contrato.

Os sistemas de avaliação de risco de crédito, muitas vezes, funcionam como verdadeiras "caixas pretas", sem transparência quanto aos parâmetros e critérios utilizados para chegar à nota que informará a decisão de conceder ou não o crédito. Para que o sistema se legitime perante as autoridades de proteção de dados, é fundamental que se baseie em critério matemático-estatístico reconhecido e auditável. Além disso, o titular dos dados deve ter acesso não apenas à nota que lhe é atribuída, mas, também, ao próprio algoritmo utilizado, ou seja, à lógica do sistema e aos fatores que influem positiva e negativamente para que se alcance tal ou qual valor.

Não é admissível, por exemplo, que o exercício de direitos pelo titular dos dados seja usado contra ele, como na situação em que empresa de cadastro de crédito categorizava como fator negativo o pedido do consumidor de acesso aos próprios dados, o que levou à mudança

da legislação alemã para impedir abusos dessa natureza. O uso de geolocalização pode, também, conduzir a discriminações injustas, se o endereço, isoladamente, gerar suposição quanto à solvabilidade do consumidor.

A discussão acerca do escore de crédito, que foi objeto dos recursos repetitivos acima discutidos, julgados pela Segunda Seção do STJ, resultou na Súmula 550:

> A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.

A referida súmula vem para aquilatar conceitos sobre o posicionamento jurisprudencial daquela Corte, pacificando através do efeito uniformizante, previsto no Código de Processo Civil de 2015, aplicando uniformemente para todo território nacional, preservando dessa forma integridade do cidadão no mercado de consumo.

6.2.3. Remoção de conteúdos da internet e o direito ao apagamento de dados pessoais

No Brasil, o Marco Civil da Internet (Lei 12.965/2014) consagrou a reserva de jurisdição para a remoção da rede mundial de computadores de conteúdo ilícito, ou seja, somente o Poder Judiciário pode determinar a retirada do conteúdo infringente. O controle da ilicitude do conteúdo bem como a ordem para seu bloqueio ou exclusão ocorrem no âmbito do processo, por provocação do interessado, e a posteriori.

O Marco Civil da Internet estabelece, como regra geral, que o provedor de conexão à internet não pode ser civilmente responsabilizado por conteúdo gerado por terceiros (art. 18). Para garantir a liberdade de expressão e impedir a censura, o provedor de aplicações na internet só pode ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, em descumprimento a ordem judicial específica, deixe de tornar indisponível o conteúdo apontado como ofensivo (art. 19). Em se tratando de cenas de nudez ou de atos sexuais de caráter privado, o provedor pode ser responsabilizado subsidiariamente pela violação da intimidade se deixar de atender a notificação que contenha indicação precisa do conteúdo a ser removido (art. 21).

Quanto à possibilidade de remoção do conteúdo da internet, o Superior Tribunal de Justiça já havia decidido que os provedores de pesquisa não respondem pelo conteúdo inserido por terceiros e não podem ser obrigados a exercer controle prévio das buscas efetuadas por usuários. No Recurso Especial 1.407.271, de relatoria da Ministra Nancy Andreis, ficou

assentado que:

> não se pode, sob o pretexto de dificultar a propagação de conteúdo ilícito ou ofensivo na web, reprimir o direito da coletividade à informação. Sopesados os direitos envolvidos e o risco potencial de violação de cada um deles, o fiel da balança deve pender para a garantia da liberdade de informação assegurada pelo art. 220, § 1º, da CF/88, sobretudo considerando que a Internet representa, hoje, importante veículo de comunicação social de massa. (STJ - REsp: 1407271 SP 2013/0239884-1, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 21/11/2013, T3 - TERCEIRA TURMA, Data de Publicação: DJe 29/11/2013)

De forma mais recentemente, no REsp 1.342.640/SP, também de relatoria da Ministra Nancy Andrighi, julgado em 07.02.2017, a Terceira Turma assentou que:

> **(i)** não respondem objetivamente pela inserção no site, por terceiros, de informações ilegais; **(ii)** não podem ser obrigados a exercer um controle prévio do conteúdo das informações postadas no site por seus usuários; **(iii)** devem, assim que tiverem conhecimento inequívoco da existência de dados ilegais no site, removê-los imediatamente, sob pena de responderem pelos danos respectivos; **(iv)** devem manter um sistema minimamente eficaz de identificação de seus usuários, cuja efetividade será avaliada caso a caso. (STJ - REsp: 1342640 SP 2012/0186042-0, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 07/02/2017, T3 - TERCEIRA TURMA, Data de Publicação: DJe 14/02/2017)

Ano seguinte, em 08.05.2018, a Terceira Turma do STJ, ao julgar o REsp 1.660.168/RJ, concluiu, por maioria, vencidos os ministros Nancy Andrighi e Ricardo Cueva, que o direito ao esquecimento, conquanto não previsto no ordenamento, deve ser o fundamento para a remoção de conteúdo considerado ofensivo. Conforme pode se extrair da ementa da decisão:

> 3. A jurisprudência desta Corte Superior tem entendimento reiterado no sentido de afastar a responsabilidade de buscadores da internet pelos resultados de busca apresentados, reconhecendo a impossibilidade de lhes atribuir a função de censor e impondo ao prejudicado o direcionamento de sua pretensão contra os provedores de conteúdo, responsáveis pela disponibilização do conteúdo indevido na internet. Precedentes.
> 4. Há, todavia, circunstâncias excepcionalíssimas, em que é necessária a intervenção pontual do Poder Judiciário para fazer cessar o vínculo criado, nos bancos de dados dos provedores de busca, entre dados pessoais e resultados da busca, que não guardam relevância para interesse público à informação, seja pelo conteúdo eminentemente

> privado, seja pelo decurso do tempo.
> 5. Nessas situações excepcionais, o direito à intimidade e ao esquecimento, bem como a proteção de dados pessoais deverá preponderar, a fim de permitir que as pessoas envolvidas sigam suas vidas com razoável anonimato, não sendo o fato desabonador corriqueiramente rememorado e perenizado por sistemas automatizados de busca.
> 6. O rompimento do referido vínculo sem a exclusão da notícia compatibiliza também os interesses individual do titular dos dados pessoais e coletivo de acesso à informação, na medida em que viabiliza a localização das notícias àqueles que direcionam sua pesquisa fornecendo argumentos de pesquisa relacionados ao fato noticiado, mas não àqueles que buscam exclusivamente pelos dados pessoais do indivíduo protegido.

Tratava-se de situação em que, ao ser realizada uma busca pelo nome da autora da ação na internet, as primeiras referências dos resultados sempre aludiam a antigo concurso público sobre o qual foram levantadas suspeitas, não confirmadas em investigações subsequentes. Embora as informações não fossem ofensivas ou inverídicas, prevaleceu o entendimento de que deveriam ser removidas dos mecanismos de busca. Interpretação, portanto, divergente daquela que se vinha emprestando ao Marco Civil da Internet, no sentido de que os provedores de pesquisa não podem ser obrigados a eliminar do seu sistema os resultados da busca de determinado termo ou expressão, e em afronta ao §1º do art. 19 do Marco Civil da Internet, pois referido dispositivo de lei dispõe expressamente que a ordem judicial de remoção de conteúdo dessa espécie (gerado por terceiros) padece de nulidade quando desacompanhada da *"identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material".* Referida decisão foi objeto de crítica por Ingo Scarlet e Arthur Ferreira Neto, ponderando que:

> O fato de a autora da demanda ser pessoa exercendo cargo público relevante (promotora de Justiça) e a natureza do fato investigado pelo CNJ (possível fraude em concurso público para a Magistratura) indicam – ao contrário do que referido na posição majoritária – que diferentemente da situação de Mario Costeja (Caso Google Europeu) – o interesse público no acesso à informação a respeito dos fatos tem um peso significativo que deveria ter sido considerado.[169]

[169] SARLET, Ingo Wolfgang; FERREIRA NETO, Arthur M. O direito ao "esquecimento" na sociedade da informação. Porto Alegre: Livraria do Advogado, 2019. p. 181.

Ademais, o que restou reconhecido pelo Tribunal de Justiça da União Europeia no caso Google Spain SL, Google inc. vs. Agencia Espanõla de Protección de Datos, Mario Costeja Gonzáles foi que, à luz da Diretiva 95/46/CE, os provedores de busca na internet praticam atividade que se qualifica como tratamento de dados e, portanto, são responsáveis por esse tratamento no âmbito de um Estado-membro, sempre que criem, nesse território, uma filial ou sucursal que promova venda de espaços publicitários, incumbindo-lhes, em consequência de suprimir os respectivos links que remetiam ao interessado, ainda que a divulgação da informação fosse em si lícita. Ou seja, mesmo na hipótese em comento, o que se determinou foi a remoção de conteúdo específico. Não há no referido precedente ordem para que o provedor de pesquisa promovesse a criação de filtros ou mecanismos capazes de realizar o controle prévio de conteúdo virtual.

Seja como for, é importante destacar, para o propósito deste artigo, que a Lei 12.965/2014 disciplina o uso da internet no Brasil de modo genérico e não contempla especificamente as redes sociais. A remoção de conteúdos ilícitos é tratada de modo abrangente, sem uma definição expressa do que seja conteúdo infringente e sem a imposição de prazos para sua remoção. O legislador parece ter-se fiado em amplíssima discricionariedade judicial para assegurar a observância dos princípios e das garantias associados ao uso da internet, entre eles, a garantia das liberdades de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal.

Recentemente, a Terceira Turma do STJ reafirmou a jurisprudência assentada sobre o tema, no sentido de que, anteriormente ao Marco Civil da Internet, bastava a ciência inequívoca do conteúdo ofensivo para que o provedor se tornasse responsável por sua remoção em prazo razoável. O novo diploma introduz a reserva de jurisdição, ou seja, a responsabilidade do provedor pela retirada do conteúdo infringente tem início a partir da notificação judicial, que deve determinar claramente o conteúdo a ser removido, mediante a indicação específica da URL, sob pena de nulidade.[170]

A reforçar o caráter excepcional da decisão da Terceira Turma proferida no Resp. 1.660.168/RJ, convém lembrar, ainda, que a Segunda Seção do STJ, antes mesmo do Marco Civil da Internet, já havia fixado que:

> a filtragem do conteúdo das pesquisas feitas por cada usuário não constituiu atividade intrínseca ao serviço prestado pelos provedores de pesquisa virtual, de modo que não se pode reputar defeituoso o site que

[170] REsp 1.694.405/RJ, rel. Min. Nancy Andrighi, 3ª T., j. 19.06.2018, DJe 29.06.2018.

> não exerce esse controle sobre o resultado das buscas. Os provedores de pesquisa virtual realizam suas buscas dentro de um universo virtual, cujo acesso é público e irrestrito, ou seja, seu papel se restringe à identificação de páginas na web onde determinado dado ou informação, ainda que ilícito, estão sendo livremente veiculados. Dessa forma, ainda que seus mecanismos de busca facilitem o acesso e a consequente divulgação de páginas cujo conteúdo seja potencialmente ilegal, fato é que essas páginas são públicas e compõem a rede mundial de computadores e, por isso, aparecem no resultado dos sites de pesquisa. Os provedores de pesquisa virtual não podem ser obrigados a eliminar do seu sistema os resultados derivados da busca de determinado termo ou expressão, tampouco os resultados que apontem para uma foto ou texto específico, independentemente da indicação do URL da página onde estiver inserido. Não se pode, sob o pretexto de dificultar a propagação de conteúdo ilícito ou ofensivo na web, reprimir o direito da coletividade à informação assegurado pelo art. 220 § 1º, da CF/88, sobretudo considerando que internet representa, hoje, importante veículo de comunicação social de massa. (STJ - REsp: 1660168 RJ 2014/0291777-1, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 08/05/2018, T3 - TERCEIRA TURMA, Data de Publicação: DJe 05/06/2018)

Anteriormente, ao julgar caso emblemático que envolvia conhecida apresentadora de televisão que pretendia retirar da rede mundial de computadores qualquer menção à sua alcunha, idêntica, aliás, à de renomado jogador de tênis, a Terceira Turma já havia decidido que a filtragem prévia das buscas é inadmissível por se confundir com atividade censória.[171]

Vale notar que essas duas últimas decisões são anteriores ao Marco Civil da Internet. Após sua entrada em vigor, passou-se a reconhecer que:

> a atividade dos provedores de busca, por si própria, pode causar prejuízos a direitos de personalidade, em razão da capacidade de limita ou induzir o acesso a determinados conteúdos. Como medida de urgência, é possível determinar que os provedores de busca retirem determinados conteúdos expressamente indicados pelos localizadores únicos (URLs) dos resultados das buscas efetuadas pelos usuários.

Assentou-se, porém, que, *"mesmo em tutela de urgência, os provedores de busca não podem ser obrigados a executar monitoramento prévio das informações que constam nos resultados das pesquisas".* É que a única exceção à reserva de jurisdição prevista no Marco Civil da Internet está contida em seu artigo 21, que diz respeito a vídeos ou a outros materiais que contenham cenas de nudez ou de atos sexuais de caráter privado.[172]

---

[171] REsp 1.316.921/RJ, rel. Min. Nancy Andrighi, 3ª T., j. 26.06.2012, DJe 29.06.2012.

[172] REsp 1.679.465/SP, rel. Min. Nancy Andrighi, 3ª T., j. 13.03.2018, DJe 19.03.2018.

Como se viu, há um significativo escólio jurisprudencial que alude ao novo conceito de privacidade e à proteção de dados pessoais, que tem origem na discussão acerca do alcance do art. 43 do CDC, no tocante aos cadastros negativos de crédito, e também, posteriormente, aos cadastros positivos de crédito.

Além disso, o STJ tem se debruçado há vários anos – antes mesmo da edição do chamado Marco Civil da Internet (Lei 12.965/2014), que não trata especificamente da proteção de dados pessoais, embora guarde inequívoca relação com esse novo campo do direito – sobre a remoção de conteúdos inseridos por terceiros e considerados infringentes pelo Poder Judiciário da rede mundial de computadores.

Pode-se dizer, assim, que a jurisprudência do STJ consolidou-se no sentido de que a remoção da internet de conteúdo infringente deve obedecer à reserva de jurisdição, mediante a indicação precisa de sua localização na rede mundial de computadores, vedada a imposição aos provedores de um monitoramento que implique cerceamento à liberdade de informação e de expressão, com exceção das situações que envolvam cenas de nudez ou de sexo, mas, ainda assim, também somente a partir da indicação precisa de URLs. A exigência de que os envolvidos indiquem precisamente os conteúdos a serem removidos tem dupla função: impedir, por um lado, que os provedores exerçam atividade de censura e, por outro, permitir a controlabilidade das decisões de exclusão de conteúdo.

6.3. Como a jurisprudência decide sobre a proteção de dados pessoais em determinados Tribunais de Justiça do País

Tal aferição é objeto de análise no presente estudo, quando estamos diante de uma legislação (LGPD) relativamente nova e pouco desbravada por parte do judicado brasileiro, em que pese, fruto deste estudo no âmbito do poder judiciário estadual realizou-se acurácia, a partir da apuração de decisões judicias, pautados nas classes processuais, nos moldes do (CNJ) que continham os termos: LGPD; Lei Geral de Proteção de Dados Pessoais; Lei Geral de Proteção de Dados; e Lei 13.709. Ao realizar recorte dos referidos termos, foram encontradas 714 decisões, publicadas entre setembro de 2020 e agosto de 2021.

Fato subsequente, as decisões foram apuradas de forma qualitativa, resultaram na análise precisa de 242 decisões, que efetivamente aplicam a LGPD em seus mais diversos aspectos.

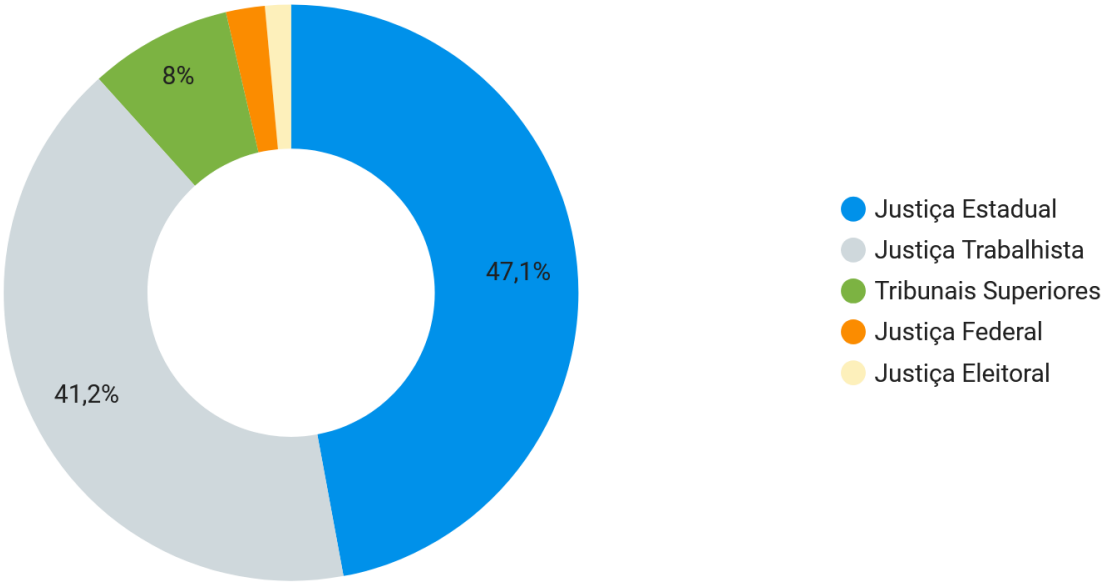


Figura 13 - Gráfico de distribuição das demandas entre justiça comum e especializada.

Em proporção diversa do que se esperava, os resultados demonstram que a Justiça Estadual não inaugurou em disparado a vertiginosidade de casos que demadem tutela com base na proteção de dados pessoais. Isso, em virtude da proporcionalidade relativa de demandas processuais adstritas à Justiça do Trabalho que em sua totalidade, considerando inclusive o Tribunal Superior do Trabalho abarcam 102 demandas judiciais sobre a Proteção de Dados Pessoais dos jurisdicionados, conforme pode ser percebido na figura abaixo.

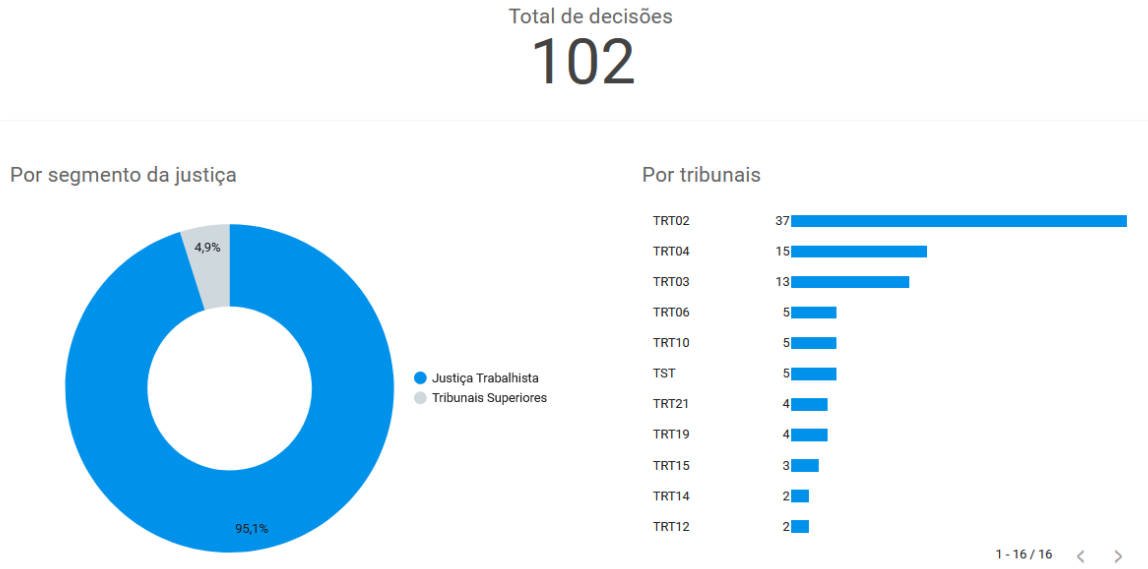


Figura 14 - Gráfico de distribuição das demandas no âmbito da Justiça do Trabalho.

Contudo, apontamento válido a ser prestigiado no âmbito da Justiça do Trabalho, que retornou com frequência os termos de “LGPD”, “dados pessoais”, e se justificam exclusivamente pelo Ato TST.GP nº 190, de 29 de maio de 2020, que instituiu a comissão, em caráter permanente, no âmbito do Tribunal Superior do Trabalho – TST e do Conselho Superior da Justiça do Trabalho – CSJT, com a finalidade de estabelecer regras de segurança, de boas práticas e de governança, e procedimentos envolvendo a proteção de dados pessoais, denominada "ComLGPD".

A referida comissão elaborou diretrizes que culminaram na maior acuidade ao nome das partes envolvidas nos processos, inclusive testemunhas, conferindo tratamento adequado aos dados pessoais que permitam a identificação do reclamante e outras pessoas físicas (art. 5º, I, Lei 13709/2018 - “LGPD”), o nome das partes e testemunhas que passaram a ser devidamente fundamentado nas sentenças e posteriormente abreviados. A iniciativa, dentre outras encampadas por diversos tribunais, atende à Resolução 363/2020 do Conselho Nacional de Justiça, que estabeleceu medidas para o processo de adequação à LGPD a serem adotadas pelos tribunais pátrios.

Na figura abaixo, podemos notar a concentração de demandas no âmbito do Poder Judiciário, como um todo. Contudo, alguns tribunais quando aglutinados compreendem quase cinquenta por cento de toda demanda, em especial o Tribunal de Justiça de São Paulo, que proferiu em 29 de setembro de 2021 a primeira sentença[173] com base na Lei Geral de Proteção de Dados Pessoais, proferida pelo juízo da 13ª Vara Cível de São Paulo e que condenou uma construtora a indenizar em R$ 10 mil um cliente que teve informações pessoais enviadas a outras empresas.

Referido Tribunal concentrou 68 processos de análise do presente trabalho, sendo seguindo pelo Tribunal Regional do Trabalho da 2ª Região que exerce jurisdição na Grande São Paulo e parte da Baixada Santista e traz consigo 37 processos no âmbito do Trabalho e sob a perspectiva dos dados pessoais, acompanhados pelo Tribunal de Justiça do Paraná com 16 ocorrência e o Tribunal Regional do Trabalho da 4ª Região que exerce jurisdição no Estado do Rio Grande do Sul com ocorrência de 15 processos no âmbito da Lei Geral de Proteção de Dados Pessoais.

[173] (TJ-SP - AC: 10802339420198260100 SP 1080233-94.2019.8.26.0100, Relator: Donegá Morandini, Data de Julgamento: 28/01/2021, 3ª Câmara de Direito Privado, Data de Publicação: 28/01/2021)

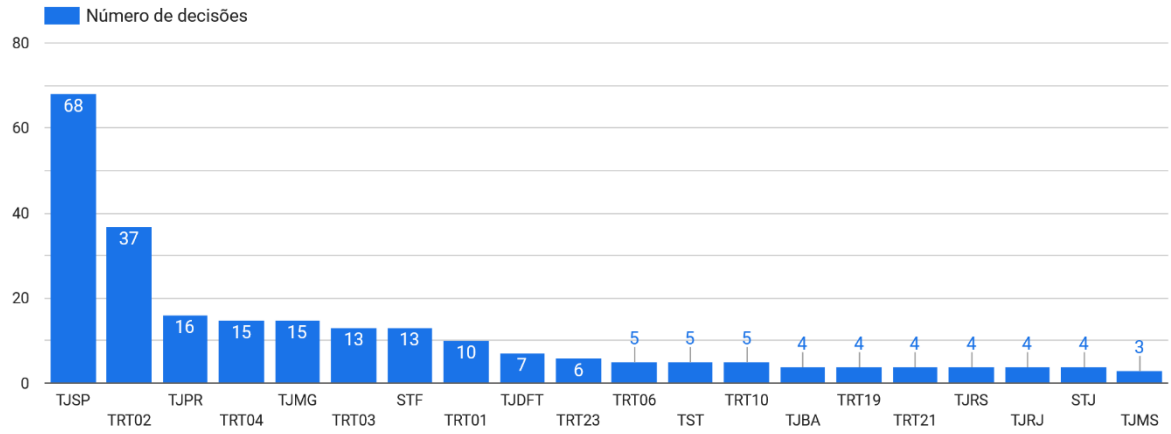


Figura 15 - Gráfico de distribuição de alocação das demandas por Tribunal

Quando da análise das decisões entre o período de setembro de 2020 a agosto de 2021, podemos notar que existe um pico de elevação das decisões a partir do mês de maio de 2021, até julho de 2021, quando passa a ter uma redução no número de decisões sobre proteção de dados.

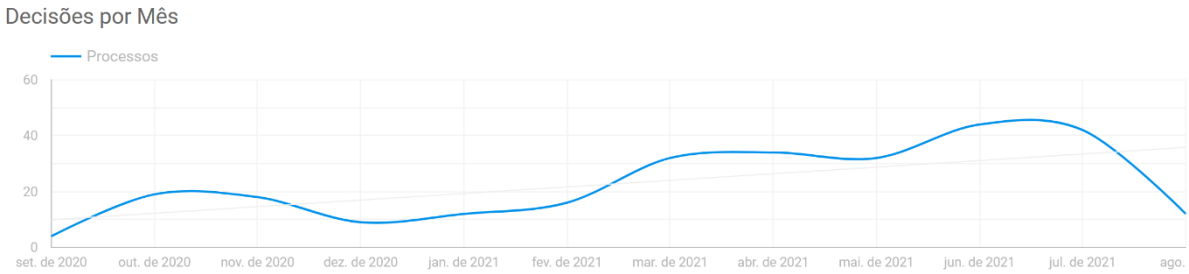
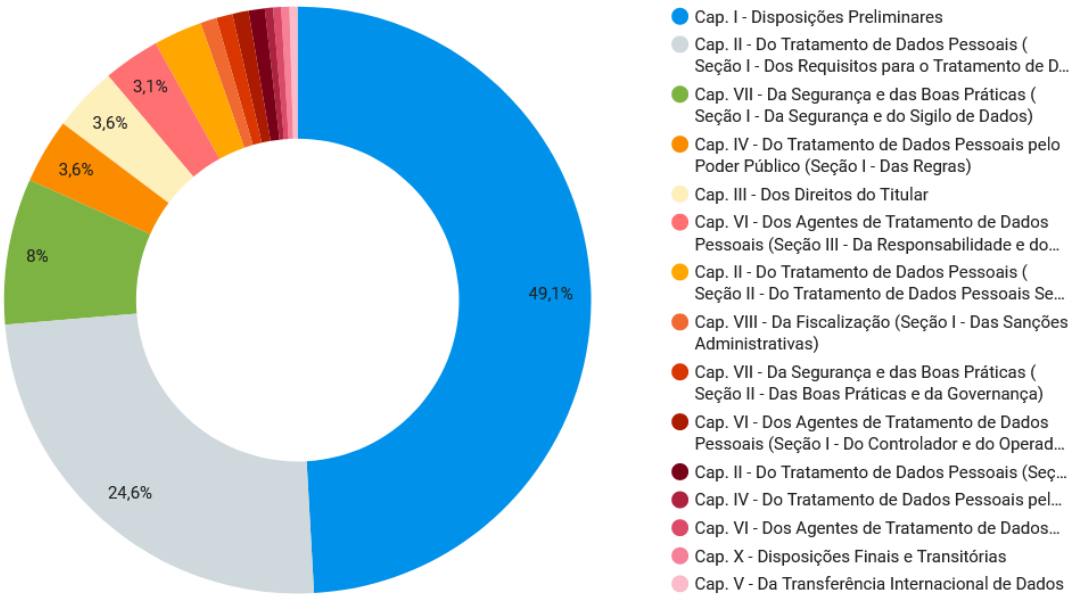


Figura 16 - Linha do tempo de decisões por mês



LGPD - Capítulo subjacente	Decisões
Cap. I - Disposições Preliminares	35
Cap. II - Do Tratamento de Dados Pessoais (Seção I - Dos Requisitos para o Tratamento de Dados Pessoais)	34
Cap. III - Dos Direitos do Titular	16
Cap. II - Do Tratamento de Dados Pessoais (Seção II - Do Tratamento de Dados Pessoais Sensíveis)	14
Cap. VII - Da Segurança e das Boas Práticas (Seção I - Da Segurança e do Sigilo de Dados)	9
Cap. IV - Do Tratamento de Dados Pessoais pelo Poder Público (Seção I - Das Regras)	7
Cap. VI - Dos Agentes de Tratamento de Dados Pessoais (Seção III - Da Responsabilidade e do Ressarcimento de Danos)	5
Cap. IV - Do Tratamento de Dados Pessoais pelo Poder Público (Seção II - Da Responsabilidade)	4
Cap. II - Do Tratamento de Dados Pessoais (Seção IV - Do Término do Tratamento de Dados)	2
Cap. VI - Dos Agentes de Tratamento de Dados Pessoais (Seção II - Do Encarregado pelo Tratamento de Dados Pessoais)	2
Cap. IX - Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (Seção II - Do Conselho Nacional d...	1
Cap. II - Do Tratamento de Dados Pessoais (Seção III - Do Tratamento de Dados Pessoais de Crianças e de Adolescentes)	1
Cap. V - Da Transferência Internacional de Dados	1

Figura 17 - Gráfico de alocações de demandas por capítulo da LGPD

Tantas foram as decisões em instâncias superiores e até mesmo nos tribunais superiores que abordaram a limitação de tratamento de dados pessoais nos processos e investigações criminais. Muitas foram as abordagens ressaltando princípios esculpidos na LGPD como à menção expressa ao artigo 4°, §1° da Lei. A referida lei também foi utilizada pelo Tribunal de Justiça do Estado de São Paulo para tutelar o sigilo profissional do médico, determinando o trancamento de ação penal iniciada pelo compartilhamento de dados do hospital em caso de aborto.[174] Em outra decisão importante, o mesmo tribunal amparou-se no Marco Civil da

[174] - Habeas Corpus. Pretensão voltada ao trancamento da ação penal sob a tese de que as provas que serviram de base para sua propositura foram obtidas com violação do dever de sigilo profissional. Viabilidade - Na hipótese, o estabelecimento hospitalar que atendeu a paciente comunicou à polícia que ela apresentava sinais de prática de aborto, comunicação da qual se originaram todas as demais provas que serviram de base para a

Internet e na Lei Geral de Proteção de Dados para impedir a coleta de dados de pessoas indeterminadas e não suspeitas de plataforma da internet.[175]

No que tange reclamações trabalhistas houveram diversos pedidos para que as ações pudessem correr em sigilo e/ou para que os dados pessoais dos jurisdicionados fossem anonimizados, sob a ótica da coexistência de uma lista de funcionários litigantes. As decisões não são consenso, ainda. Muitas delas, como já dito anteriormente, preservam nomes das partes, enquanto outras entendem que a proteção conferida pelas regras vigentes já seria suficiente, indeferindo tal pleito.

Amparados nos princípios da finalidade, adequação e necessidade, os Tribunais vêm compreendendo que o compartilhamento de dados pelo Poder Público tem limites estabelecidos para situações e finalidades específicas.[176] No campo eleitoral existem decisões que indeferiram o pedido de obtenção de documentos que contêm dados pessoais de eleitores, como listagem de eleitores e cadernos de votação.

No âmbito do Código de Defesa do Consumidor, destacando a responsabilidade civil por defeito do serviço e utilizando a LGPD como entendimento complementar.[177] Ainda nesse espectro, em recente decisão o Superio Tribunal de Justiça compreendeu fraude bancária em

---

propositura da ação penal - Aparente conflito entre, de um lado, os princípios constitucionais da intimidade e da vida privada e, de outro, o dever de sigilo profissional e os princípios gerais de proteção à segurança pública e acesso à informação. Solução que desafia aplicação, em cada caso concreto, de critérios de razoabilidade e proporcionalidade, sem perder de vista que, não obstante o entendimento de que inexistem direitos e obrigações de caráter absoluto, a quebra do dever de sigilo profissional só se justifica pela via excepcional, isto é, diante de situação de grande convulsão ou comoção social, do contrário haverá que prestigiar o direito à intimidade e à privacidade. Por isso mesmo, não pode ser admitida como premissa para todos os casos a de que qualquer prática de crime é causa justa apta a afastar as garantias constitucionais do indivíduo - In casu, infere-se que a paciente, antes de buscar socorro médico, sangrava muito, encontrava-se entre a vida e a morte. De tal forma que, se havia algum interesse legítimo da coletividade, só poderia ser o de que ela fosse salva, não submetida à persecução penal - Ausente, ao que se conclui, causa que justificasse a quebra do dever de sigilo profissional. Quebra que, por ser o cerne da investigação policial – investigação que serviu de base para a propositura da ação penal – , contaminou todas as demais provas produzidas nos autos, com destaque para a prova oral e para a remessa da ficha médica da paciente à autoridade policial que a requisitou de ofício - Ordem concedida para trancar a ação penal. (TJ-SP - HC: 21619412720208260000 SP 2161941-27.2020.8.26.0000, Relator: Amable Lopez Soto, Data de Julgamento: 13/04/2021, 12ª Câmara de Direito Criminal, Data de Publicação: 11/06/2021)

[175] (TJ-SP - MS: 20765463320218260000 SP 2076546-33.2021.8.26.0000, Relator: Álvaro Castello, Data de Julgamento: 06/07/2021, 3ª Câmara de Direito Criminal, Data de Publicação: 14/07/2021)

[176] (STF - MS: 37636 DF 0036489-15.2021.1.00.0000, Relator: ROSA WEBER, Data de Julgamento: 19/01/2021, Data de Publicação: 22/01/2021)

[177] (TJ-BA - RI: 00818783120208050001, Relator: MARY ANGELICA SANTOS COELHO, QUARTA TURMA RECURSAL, Data de Publicação: 08/07/2021)

operação de empréstimo bancário, configurando a responsabilidade civil objetiva, nos termos da Súmula nº 479/STJ.[178]

Até o momento não foi possível estabelecer uma uniformidade de entendimentos em relação à caracterização de dano *in re ipsa* em casos envolvendo incidentes de segurança de dados pessoais. Quando pleiteados pelos titulares dos dandos a caracterização de danos morais em razão de vazamento ou uso indevido de dados pessoais, a jurisprudência se dividiu [179] [180] Determinadas decisões seguiram a compreensão de que o incidente de segurança gera presunção de danos morais, em outro passo, alguns magistrados declararam ser necessário a demonstração do prejuízo para a configuração de danos de natureza moral derivados do vazamento ou uso indevido de dados pessoais.[181]

6.4. Do entendimento jurisprudencial dos dados pessoais enquanto direito fundamental

Na ordem jurídica brasileira, a tutela da proteção sob a perspectiva de um direito fundamental e autônomo, até o advento da emenda 115/2022, não derivou-se de uma consideração literal do tratamento automatizado, como no caso das legislações anteriores, e sim, de um matiz de garantias espraiadas pelo texto constitucional que davam suporte à

[178] (TJ-RJ - APL: 04954082320158190001 RIO DE JANEIRO CAPITAL 48 VARA CIVEL, Relator: MARIA CELESTE PINTO DE CASTRO JATAHY, Data de Julgamento: 22/03/2017, VIGÉSIMA TERCEIRA CÂMARA CÍVEL CONSUMIDOR, Data de Publicação: 24/03/2017)

[179] RECURSO INOMINADO – AÇÃO DE CONHECIMENTO – LEI GERAL DE PROTEÇÃO DE DADOS – DIVULGAÇÃO DE DADOS ARMAZENADOS – NECESSÁRIA MANIFESTAÇÃO DE VONTADE DO TITULAR – VAZAMENTO DE INFORMAÇÕES – AUSÊNCIA DE PROVA DE OMISSÃO QUALIFICADA DA EMPRESA (FALHA REITERADA NOS SISTEMAS DE INFORMÁTICA) – ATAQUE HACKER – EXCLUDENTE DE RESPONSABILIDADE – ARTIGO 43, INCISO III, DA LEI Nº 13.709/2018 – SENTENÇA MANTIDA – RECURSO DESPROVIDO. (TJ-SP - RI: 10026943920218260405 SP 1002694-39.2021.8.26.0405, Relator: ANDRE LUIZ TOMASI DE QUEIROZ, Data de Julgamento: 25/06/2021, 2ª Turma Cível, Data de Publicação: 25/06/2021)

[180] Por conseguinte, diferente do que alega o réu, é de se reconhecer que a mera exposição das informações a terceiros é, *in re ipsa,* suficiente para abalar o bem-estar psíquico do indivíduo de forma que foge à normalidade. (Autos n° 0001036-57.2019.8.19.0212 – TJ/RJ)

[181] RESPONSABILIDADE CIVIL. Ação de obrigação de fazer e indenização por danos morais. Alegação da autora de que teve seus dados pessoais vazados pela empresa ré. Consideração de que inexiste prova cabal das consequências danosas do vazamento de seus dados. Hipótese em que a falta de comprovação cabal da verificação concreta de consequências danosas, em virtude do vazamento de dados pessoais, importa na conclusão de que a postulação deduzida pela autora está lastreada em meros danos hipotéticos, ou seja, à possibilidade da ocorrência de fatos lesivos, à expectativa de prejuízo potencial, em decorrência de suposto receio de uso futuro e incerto dos seus dados em eventuais fraudes no comércio, o que só poderia mesmo ter resultado no decreto de improcedência do pedido inicial. Postulação deduzida pela autora baseada em mera possibilidade da ocorrência de dano. Danos morais não caracterizados. Pedido inicial julgado improcedente. Sentença mantida (RI, 252). Recurso improvido. Dispositivo: negaram provimento ao recurso. (TJ-SP - AC: 10252264120208260405 SP 1025226-41.2020.8.26.0405, Relator: João Camillo de Almeida Prado Costa, Data de Julgamento: 10/09/2021, 19ª Câmara de Direito Privado, Data de Publicação: 10/09/2021)

liberdade, dignidade da pessoa humana em compasso com a intimidade e a vida privada.

O contexto de estruturação da privacidade de dados no Brasil possui diversas origens normativas, inicialmente pelo intermédio das garantias à liberdade de expressão[182], do direito à informação[183] [184], posteriormente confrontados com à tutela da personalidade, em especial atenção ao direito a privacidade. Em mesmo turno, o texto constitucional considera invioláveis a intimidade e a vida privada por força do (art. 5°, X), interpretação esta inicialmente projetada para garantia da tutela nas interceptações telefônicas, telegráficas ou dedados (art. 5° XII), com consequente previsão do remédio constitucional do *habeas data* (art. 5° LXXII), que possibilita o direito à retificação dos dados pessoais e acesso destes.

No seio infraconstitucional, em especial destaque temos à relevância do Código de Defesa do Consumidor, que aborda um capítulo específico para normatização dos "bancos de dados e cadastros", conforme esculpido no (art. 43, Lei 8.078,90), trazendo a sistemática baseada no *Fair Information Principies*, inaugurando o marco normativo dos princípios de proteção de dados pessoais no direito brasileiro, conforme sustentado pela doutrina.[185]

No que tange a essa proteção de dados no Brasil, observa-se que *"a proteção de dados pessoais no ordenamento jurídico brasileiro somente se estruturou em torno de um conjunto normativo unitário muito recentemente"*[186], sendo seu contexto de formação decorrente das disposições de direitos fundamentais previstas na Constituição Federal:

> No Brasil, assim como em outros diversos Estados, o direito à privacidade é assegurado constitucionalmente como direito humano fundamental. A Constituição Federal brasileira não se restringe apenas ao direito à privacidade, apresentando abrangência em relação à preservação da vida privada e da intimidade da pessoa, a inviolabilidade da correspondência, do domicílio e das comunicações

[182] Constituição Brasileira, art. 5°, IX; art. 220.

[183] SIQUEIRA, D. P.; FERRARI, C. C. O direito à informação como direito fundamental ao estado democrático. Revista Direitos Sociais e Políticas Públicas - UNIFAFIBE, v. 4, p. 124-153, 2016.

[184] Constituição Brasileira, art. 5°, XIV; art. 220; incluindo o direito ao recebimento de informações de interesse coletivo ou particular dos órgãos públicos (art. 5°, XXXIII), bem como o direito à obtenção de certidões de repartições públicas (art. 5°, XXXIV).

[185] CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional. Revista de Direito do Consumidor, n. 46, p. 77-119, abr./jun. 2003. p. 77-119.

[186] DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters, 2019. p. 259.

> [...][187]

Logo, torna-se necessário que a arranjo jurídico estabeleça critérios proporcionais de tutela da pessoa nesta área, que é muito fortemente ligada ao desenvolvimento da tecnologia, tendo em vista que a internet constitui um ambiente de exercício de diversos direitos fundamentais como a exemplo a proteção da privacidade e dos dados pessoais apresenta-se como um propósito para o exercício desses direitos.[188]

À vista disso, no ordenamento brasileiro a defesa do usuário está conferida tanto pelo Marco Civil, como da Lei Geral de Proteção de Dados, além de algumas disposições do CDC. Nesse sentido, este último traz disposições referentes aos bancos de dados e cadastros dos consumidores, garantindo a eles questões referentes às suas informações, prazos, correção de dados, entre outros.[189] A respeito do Marco Civil da Internet destaca-se que:

> Na oportunidade, o legislador houve por bem sedimentar a proteção à privacidade e trouxe um capítulo exclusivo para a salvaguarda dos dados pessoais, cuja aplicação, contudo, depende do uso da internet. Ainda que a referida Lei não estivesse voltada, fundamentalmente, à autonomia dos dados pessoais, sua contribuição foi de grande valia.[190]

Até porque conforme exposto "*o tratamento autônomo da proteção de dados pessoais é uma tendência hoje fortemente enraizada em diversos ordenamentos jurídicos"*[191], especialmente diante do fluxo informacional e de dados decorrentes da sociedade da

---

[187] FORTES, Vinícius Borges; BOFF, Salete Oro. 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: Estudos Jurídicos e Políticos, Florianópolis, v. 35, n. 68, p. 109-128, jun. 2014. ISSN 2177-7055. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2013v35n68p109. Acesso em 02 maio 2021. p. 119

[188] MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. Revista de Direito do Consumidor, São Paulo, v. 106, p. 38, jul./ago. 2016.

[189] OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro, São Paulo: Thomson Reuters Brasil, 2019. p. 67.

[190] CRESPO, Danilo Leme; RIBEIRO FILHO, Dalmo. A evolução legislativa brasileira sobre a proteção de dados pessoais: a importância da promulgação da Lei Geral de Proteção de Dados Pessoais. Revista de Direito Privado, São Paulo, v. 98, p. 171, mar./abr. 2019.

[191] Cf. DONEDA, 2011. p. 96

informação na era tecnológica. Salienta-se que

> Em uma visão prospectiva, deve haver uma preocupação estatal no sentido de fazer germinar a percepção de que, enquanto indivíduos e enquanto sociedade, diante das dimensões digitais agora existentes, viver em um grupo social democraticamente organizado tomou outro sentido, e isto inclui, em primeira linha, ter a nítida noção do que efetivamente significa hoje *divulgar* informações.[192]

No ponto, observa-se que essas alterações de legislação e de enfoque demonstra o caso emblemático de uma predisposição que, a princípio, parecia tão apenas objetivada em alterar determinado patamar tecnológico e a requerer previsões pormenores ao ordenamento.[193]

Todavia, na esteira dessas mesmas mudanças, é possível verificar que não pode o Estado se furtar de regulamentar as questões relativas as informações dos indivíduos, uma vez que é importante que haja uma proteção adequada em face de seus registros, distorções e manipulações. Esta é uma tarefa crucial na sociedade de informação, mas por demais negligenciada pelos Estados.[194]

Esse conjunto doutrinário e legal faz demonstrar que o direito à privacidade e à proteção de dados pessoais, apesar de ligados entre si, podem ser vistos como direitos autônomos no ordenamento jurídico brasileiro dado o particular âmbito de proteção de cada um. A sistemática pode ser inclusive extraída da redação do Marco Civil da Internet, que traz como princípios diferentes a proteção da privacidade e a proteção de dados pessoais em seu artigo 3°.[195] No

---

[192] RUARO, Regina Linden; RODRIGUEZ, Daniel Pineiro; FINGER, Brunize. O direito à proteção de dados pessoais. Revista da Faculdade de Direito - UFPR, Curitiba, n. 53, p. 45-66, 2011. Disponível em: https://revistas.ufpr.br/direito/article/view/30768/19876. Acesso em 02 maio 2021. p. 51.

[193] Cf. DONEDA, 2011. p. 96

[194] Cf. RUARO, 2011. p. 50.

[195] Lei nº 12.965 de 23 de abril de 2014 - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Art. 3o A disciplina do uso da internet no Brasil tem os seguintes princípios:
I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;
IV - preservação e garantia da neutralidade de rede;
V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
VII - preservação da natureza participativa da rede;

mesmo sentido, observa-se que a disciplina de proteção de dados também deve observar o respeito à privacidade.

Dessa maneira, observa-se que o ordenamento pátrio vem conferindo a necessária releitura de determinados direitos no âmbito da internet, trazendo inovações no que tange à proteção de dados e à privacidade, e, agora, também no que tange aos direitos fundamentais.

Para completa compreensão do estado da arte acerca da garantia da privacidade de dados como direito fundamental, necessário transcorrer uma breve análise da decisão liminar na ADI n°. 6387, posteriormente referendada pelo Plenário do Supremo Tribunal Federal no julgamento das ADI's n°. 6387, 6389, 6388, 6390 e 6393, que suspendeu a eficácia da Medida Provisória n°. 954/2020.[196]

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

[196] EMENTA MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteçâo de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados. 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas b e d). 4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteçâo de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº

A decisão prolatada pelo Supremo Tribunal Federal inaugurou um novo paradigma no que se refere à proteção de dados no ordenamento jurídico brasileiro, agora com o patamar consolidado jurisprudencialmente a categoria dos direitos fundamentais. O entendimento decorre do fato de que as condições em que se dá a manipulação de dados pessoais digitalizados, por agentes públicos ou privados, consiste em um dos maiores desafios contemporâneos do direito à privacidade. Pode-se, então, nessa linha, dizer que conforme lições de Marinoni:

> A proteção dos dados pessoais alcançou uma dimensão sem precedentes no âmbito da sociedade tecnológica, notadamente a partir da introdução do uso da tecnologia da informática. A facilidade de acesso aos dados pessoais, somada à velocidade do acesso, da transmissão e do cruzamento de tais dados, potencializa as possibilidades de afetação de direitos fundamentais das pessoas, mediante o conhecimento e o controle de informações sobre a sua vida pessoal, privada e social.

Nesse sentido, a relatora acatou o pedido da parte postulante na ADI 6387, onde apontou para a existência, no desenho constitucional brasileiro, de um direito fundamental à proteção de dados, na concepção de um direito à autodeterminação informativa, em que fundamenta, inclusive, a edição da Lei Geral de Proteção de Dados. Nesse espectro, é importante a lição de Mendes e Fonseca, onde, comentando a decisão, afirmam que:

> O Tribunal formulou, assim, uma tutela constitucional mais ampla e abstrata do que o direito à inviolabilidade da esfera íntima e da vida privada. Essa tutela poderá ser aplicada em inúmeros casos futuros envolvendo a coleta, o processamento e o compartilhamento de dados pessoais no Brasil. O conteúdo desse direito fundamental exorbita aquele protegido pelo direito à privacidade, pois não se limita apenas aos dados íntimos ou privados, ao revés, refere-se a qualquer dado que identifique ou possa identificar um indivíduo.[197]

954/2020. 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada. (STF - ADI: 6387 DF 0090566-08.2020.1.00.0000, Relator: ROSA WEBER, Data de Julgamento: 07/05/2020, Tribunal Pleno, Data de Publicação: 12/11/2020)

[197] MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados Comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. Revista de Direito do Consumidor, São Paulo, v. 130, p. 473, jul./ago. 2020.

A caracterização da proteção de dados como direito fundamental contribui para o fenômeno da "constitucionalização da pessoa"[198] cuja extensão decorre da própria dignidade da pessoa e da sua liberdade em desenvolver a personalidade humana, posto que a inviolabilidade da pessoa deve ser reconfigurada e reforçada na dimensão eletrônica.[199] A esfera de defesa da personalidade vem demonstrada pelo caráter do objeto, que não diz respeito exclusivamente aos dados em si, mas sim ao titular desses dados,[200] ou seja, não se trata da defesa do dado por si só como um objeto próprio, ou mesmo como um direito de propriedade da pessoa, mas um direito decorrente da própria personalidade individual.

É essa a importância de se erigir um direito fundamental de proteção de dados também na dimensão privada. Com esse entendimento Mendes e Fonseca referem que não parece adequado enxergar a incidência do direito fundamental à proteção de dados somente no que diz respeito à atuação do Poder Público. Aduzindo ser necessário que essas disposições sejam aplicadas na esfera privada e suas relações, permitindo uma eficácia horizontal desse direito.[201]

O julgado histórico do Supremo Tribunal Federal esclarece que, no Estado Democrático de Direito, não se pode fornecer um cheque em branco para instituições públicas ou privadas, por mais respeitadas que sejam e por mais nobres os motivos envolvidos. O amplo acesso aos dados pessoais dos cidadãos brasileiros exige, no mínimo, balizas jurídicas claras e seguras quanto a essa coleta ou transferência, a partir da previsão de medidas de segurança e critérios de intervenção proporcionais à gravidade da restrição a esse direito fundamental.

Para além disso, já tramitam iniciativas legislativas para a maior proteção dos dados, inclusive em sede de Emenda à Constituição. Tal proposta vem pela PEC 17/2019[202], em tramitação junto ao Poder Legislativo Brasileiro, sendo já aprovada pelo Senado Federal e encaminhada para a Câmara dos Deputados, que pretende acrescentar "o inciso XII-A, ao art. 5°, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria". Contudo, em parecer da comissão de Constituição e Justiça, houve alterações,

---

[198] RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 17.

[199] Cf. RODOTÀ, 2008. p. 19.

[200] Cf. Mendes, 2020. p. 473.

[201] Cf. Mendes, 2020. p. 474.

[202] BRASIL. Congresso Nacional. Proposta de Emenda à Constituição n° 17, de 2019. Câmara dos Deputados, Aguardando Deliberação no Plenário (PLEN), 2019. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=C24363F8FA4238CCAF3F82BD581A4E9F.proposicoesWebExterno1?codteor=1773684&filename=PEC+17/2019>. Acesso em: 02 maio 2021.

propondo-se uma nova redação ao artigo XII do artigo 5° da Constituição da República:

> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal, bem como é assegurado, nos termos da lei, **o direito à proteção dos dados pessoais, inclusive nos meios digitais.** (BRASIL, 2019).

A importância da alteração vem demonstrada já no início da justificação da matéria, onde os autores da proposta apresentam que justificativas aduzindo que A proteção de dados pessoais é derivada da evolução histórica da própria sociedade internacional: diversos são os Países que adotaram leis e regras sobre privacidade e proteção de dados. Isso porque o assunto, cada vez mais, na Era informacional, representa riscos às liberdades e garantias individuais do cidadão.

Importante destacar que a iniciativa vem de há muito na seara internacional. Esta abordagem reflete-se em inúmeros documentos nacionais e internacionais, principalmente na Carta de Direitos Fundamentais da Comunidade Europeia, na qual a proteção de dados é reconhecida como um direito fundamental autônomo.[203] Para além disso, iniciativas jurisprudenciais igualmente paradigmáticas devem ser citadas, como é o caso do Tribunal Constitucional Alemão que, em julgamento semelhante ao brasileiro, reconheceu um direito de autodeterminação informativa ainda em 1983.

Diante disso, é evidente e acertada a releitura do direito fundamental, como decorrência da própria personalidade humana. Ao final, o direito de proteção de dados pessoais como direito fundamental é o mais expressivo da condição da condição humana contemporânea. Relembrar isto a cada momento não é verbosidade, pois toda mudança afeta a proteção de dados tem impacto sobre o grau de democracia que nós podemos experimentar.[204] Dessa maneira, considerar e efetivá-lo como fundamental é expressão da dignidade e liberdade humanas no ambiente da internet.

6.5. Uma agenda regulatória convergente com a proteção de dados pessoais no Brasil

No cenário nacional, a entrada em vigência da Lei nº 13.709/2018 (LGPD) foi muito saudada como momento marcante na questão relacionada à proteção de dados pessoais.

[203] Cf. RODOTÀ, 2008. p. 13.

[204] Cf. RODOTÀ, 2008. p. 21.

Entretanto, não se pode olvidar a existência de outras disposições de natureza comercial e tributária que anteriormente já vigiam e seguem com essa condição, tais como o sigilo dos agentes do fisco (art. 198 do CTN), das Leis 9.296/1996 e 10.217/2001, que tratam da interceptação telefônica e da gravação ambiental e também da Lei Complementar nº 105/2001 que dispõe sobre o sigilo das operações de instituições financeiras (que permite às autoridades administrativas, a quebra do sigilo bancário, com ou sem autorização judicial, conforme o tipo de caso concreto).

E, com destaque especial, o Código de Proteção e Defesa do Consumidor (Lei nº 8078/90), que é de ordem pública e interesse social, e em seu art. 43 dispõe sobre dos bancos de dados envolvidos nas relações de consumo, elencando direitos e garantias para o consumidor em relação às suas informações pessoais, tudo em busca de limites para os fornecedores como forma de viabilizar que possa existir equilíbrio e a harmonia nessas relações. Muito embora adstrito às relações de consumo, o CDC desde sua promulgação vem influindo na interpretação acolhida por expressiva doutrina, constituindo-se em marco normativo dos princípios de proteção de dados pessoais no Brasil (DONEDA, 2011, pg. 103.

Refira-se que esse arcabouço principal conta ainda com a Lei de Acesso à Informação (Lei n° 12.527), que estabelece o livre acesso a informações, a exceção das informações pessoais e as informações sigilosas, com objetivo de garantir o máximo de transparência aos atos da Administração Pública, o Marco Civil da Internet (Lei 12.965/14) seu regulamento o Decreto 8.771/16. Nesse contexto, sobressai uma certa dispersão e, como já foi referido, a carência de uma atualizada raiz constitucional direta, a servir de suporte e diretriz para a legislação infraconstitucional. Rememore-se que desde 1974, com o surgimento nos Estados Unidos, do Fair Information Practice Principles (“FIPP”) do Privacy Act, as premissas básicas que nessa área vem sendo adotadas nas diversas legislações centram-se em haver, principalmente: (i) transparência; (ii) participação individual e consentimento; (iii) propósito; (iv) minimização de dados; (v) limitação temporal; (vi) qualidade, integridade e segurança; (vii) accountability; e (viii) auditagem (IBRAC, 2019, pg. 979).

O advento do Século XXI, entretanto, deve provocar que sejam revisitadas e analisadas essas premissas à luz da evolução tecnológica, seja para confirmá-la, seja para aprimorar seu conteúdo e elenco. E sempre as mantendo compatíveis com os valores e princípios constitucionais. Assim, o primeiro marco assegurando a proteção de dados da pessoa natural deve estar na Lei Maior que já contém o direito à autodeterminação informativa (artigo 5°, incisos X e XII) e assegura a inviolabilidade da intimidade e da vida privada, bem como, o sigilo das comunicações em geral. Assim sendo, esse conjunto laborará no sentido de haver

condições para o exercício do direito à liberdade previsto no caput do artigo 5° da Constituição Federal.

Mesmo considerando esse contexto fragmentado composto por várias normas, são válidas as considerações emitidas por Rony Vainzof que ao comentar a Lei nº 13.709/18 assim manifestou:

> Outrossim, independentemente dos fundamentos da LGPD, que veremos na sequência, buscarem um equilíbrio na manutenção do desenvolvimento econômico e tecnológico de modelos de negócios inovadores, públicos ou privados, com a inviolabilidade de direitos constitucionais dos cidadãos, a parte final do art. 1º não deixa qualquer dúvida que o seu objetivo está intrinsecamente vinculado à proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. E a utilização do verbo "proteger", no art. 1º, também demonstra essa necessidade coerente que o legislador enxergou no titular dos dados como vulnerável em comparação com os agentes de tratamento (BLUM, 2019, pg. 20).

Realmente a pessoa natural, titular dos dados é vulnerável nesse contexto e seus direitos da personalidade precisarão de adequada proteção, condizente com o que promete nossa República instituída como Estado Democrático de Direito[205]. Assinale-se que não se mostra absolutamente necessário que os direitos da personalidade sejam representados em um único direito subjetivo, ou ainda que sejam classificados em múltiplos direitos da personalidade com rol difícil de precisar em termos de quantidade (TEPEDINO, 2004, pg. 47). A técnica mais apropriada, deve centrar-se em buscar proteger amplamente a pessoa humana em todos os seus aspectos; e principalmente mediante prescrições gerais. Ademais, pode-se afirmar que a dignidade representa fundamento da República, configurando verdadeira cláusula geral de tutela e promoção da pessoa humana.

Outro detalhe: nessa área, tanto a limitação do poder estatal de, indevidamente, interferir no plano individual dos cidadãos, quanto a exigência de que mantenha postura proativa nas prestações estatais para proteção desses direitos (TEPEDINO, 2004, pg. 48), são autoaplicáveis no território brasileiro (LIMBERG, 2019, pg. 239). O ideal, como já frisamos, é haver uma raiz constitucional a amparar um sistema de proteção, sem que enquanto este não está constituído, se possa deixar de adotar a proteção de dados da pessoa natural, como direito fundamental

[205] SIQUEIRA, D. P.; FERRARI, C. C. O direito à informação como direito fundamental ao estado democrático. Revista Direitos Sociais e Políticas Públicas - UNIFAFIBE, v. 4, p. 124-153, 2016.

amparado implicitamente na Constituição Federal.

6.6. A proteção de dados pessoais em simbiose com a dignidade da pessoa humana e o direito ao livre desenvolvimento da personalidade no ordenamento jurídico brasileiro em compasso com o diálogo das fontes

A Constituição Federal, em seu art. 1º, III, ao reconhecer o princípio da dignidade humana, por consequência protegeu os direitos da personalidade, incluindo nesse contexto, garantias como a da liberdade de expressão (art. 5°, inc. IX) e do direito à informação (art. 5°, inc. XV), da inviolabilidade da vida privada e da intimidade (art. 5°, inc. X), a garantia do Habeas Data (art. 5°, inc. LXXII), a proibição da invasão de domicílio (art. 5°, inc. XI) e violação de correspondência (art. 5°, inc. XII) (DONEDA, 2017, pg. 323).

Enfim, deixou indelével a relação entre o princípio da dignidade da pessoa humana e os direitos fundamentais, com destaque para os direitos de liberdade, intimidade, privacidade e proteção de dados pessoais, tudo acentuando essa vinculação entre esses direitos e os princípios fundamentais (SARLET, 2015, Pg. 23).

Recentemente, com advento da Emenda Constitucional de n° 115/2022[206], diante da previsão no art. 5°, LXXIX, da Constituição Federal que aborda a proteção de dados pessoais, inicia-se a observação do fenômeno da privacidade sob o prisma dos dados pessoais, e não da vida íntima ou privada. Note-se que o aspecto de subjetividade do direito, mesmo no tocante aos direitos fundamentais, envolve (além da exigibilidade) uma relação trilateral entre o titular, o objeto e o destinatário (do direito e obrigações), ocupando posições jurídicas atribuídas pelo direito objetivo (CANOTILHO, 2001, pg. 541) e (SARLET, 2014, pg. 203).

E no que diz respeito ao direito à proteção de dados pessoais, em conformidade com a legislação respectiva (art. 5° da LGPD), os titulares do direito são, em primeira linha, as pessoas naturais identificadas e identificáveis, sendo que a interpretação sistemática de nosso ordenamento jurídico mostra em quanto o referido direito é relacionado com a dignidade humana.

Assim, o respeito à dignidade da pessoa humana é forma pela qual vários outros princípios constitucionais se irradiam, e mesmo se tornam efetivos dentro dos pilares que estruturam o próprio Estado Democrático de Direito, posto ser inegável a relação do primeiro

[206] Emenda Constitucional Nº 115/2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. D.O.U. Publicado em: 11/02/2022 | Edição: 30 | Seção: 1 | Página: 2.

com a liberdade, a intimidade, a privacidade e a proteção de dados pessoais, todos direitos fundamentais (SARLET, 2015, pg. 27). Em relação à privacidade, por exemplo, o doutrinador Ingo Sarlet interpreta que:

> [...] por dignidade da pessoa humana a qualidade intrínseca e distintiva reconhecida em cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da comunidade, implicando, neste sentido, um complexo de direitos e deveres fundamentais que assegurem a pessoa tanto contra todo e qualquer ato de cunho degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável, além de propiciar e promover sua participação ativa e corresponsável nos destinos da própria existência e da vida em comunhão com os demais seres que integram a rede da vida.

É possível perceber que essa concepção segue linha concordante com o aporte teórico sustentado por Stefano de Rodotà que em sua obra "A vida na sociedade da vigilância" (RODOTÁ, 2007, pg. 237/238), aduz que a função sociopolítica da privacidade – que em muito se relaciona com o tratamento de dados -, se projeta como elemento constitutivo da cidadania compatibilizando-se com o respeito intrínseco para haver condições consentâneas com almejada igualdade.

Considerada a tríade liberdade, privacidade e dignidade, em especial nessa área é importante atentar para a questão da vulnerabilidade da pessoa humana (envolvendo o que se denomina de corpo eletrônico do ser humano (RODOTÁ, 2007, pg. 255), sendo que ausência de proteção específica nessa seara, mesmo que eventual, por reflexo, representa descumprir garantias e direitos fundamentais.

A luz, portanto, de construir-se previsão adequada para o direito à proteção dos dados pessoais deve ser associado a vários princípios insertos nos direitos fundamentais (caráter geral e especial), como é o caso do princípio da dignidade da pessoa humana, do resguardo à privacidade, intimidade e liberdade, bem como, a proteção e direito ao livre desenvolvimento da personalidade, todos valores constitucionais (DONEDA, 2019, pg. 41).

Considerada a intimidade que os seres humanos têm direito no tocante a coleta, tratamento, armazenamento e comercialização dos dados pessoais (repita-se a imprescindibilidade do consentimento do titular) é fundamental manter hígidas as premissas expressas e implícitas insertas nos valores constitucionais.

Desta forma, diante de existência de qualquer espécie de vácuo legislativo ou lacuna(s) na(s) lei(s), sobressai a imprescindibilidade sempre urgente de haver um arcabouço legislativo de qualidade (e que seja mantida atualizada), que seja específico para realização dos desideratos já mencionados. E mais, que nessa legislação particularizada, ou seja, que nos instrumentos legais dispostos para essa área, estejam presentes, significativamente, prescrições consentâneas com os melhores valores éticos e morais inscritos no texto constitucional.

Assim, a solução para o aparente conflito de leis está na coordenação destas para oferecer unidade e coerência ao sistema jurídico. Não se faz necessária a exclusão de uma para prevalecer outra, mas a aplicação concomitante de diferentes fontes com o intuito de encontrar o remédio ao problema sob análise. É o que afirma Claudia Lima Marques (2012, p. 26-27), ao expor que a expressão "diálogo" é autoexplicativa, uma vez que se refere a diálogos, duas "lógicas", nesse caso duas fontes que conversam "em uma aplicação conjunta e harmoniosa guiada pelos valores constitucionais" (MARQUES, 2012, p. 27).

A propósito, observa-se que uma das inspirações da Lei Geral de Proteção de Dados Pessoais é o Código de Defesa do Consumidor. Tanto neste quanto naquela, há previsão dessa convivência pacífica em que as fontes não se excluem. As normas previstas nessas leis estabelecem a coexistência com outros direitos e princípios constantes do ordenamento jurídico cuja aplicação deve ser orientada pela Constituição Federal. Diante de impactante pluralismo de fontes legislativas, para que permaneçam harmonicamente coexistentes, utiliza-se o método do diálogo das fontes, representado por essa concomitante vigência e aplicabilidade normativa a uma mesma situação.

Trata-se de uma construção da literatura jurídica que reconhece no diálogo das fontes um "método da teoria geral do direito" que "eleva a visão do intérprete para o tê-los do conjunto sistemático de normas e dos valores constitucionais" (MARQUES, 2012, p. 66), uma "espécie de interpretação sistemática, fundada na unidade do ordenamento e supremacia da Constituição, cuja contribuição original resulta da diretriz de compatibilização de normas e sua aplicação simultânea ao caso, sob o signo da complementaridade" (MIRAGEM, 2012, p. 109).

Daí a solução normativa encontrada no interior da Lei Geral de Proteção de Dados ao disciplinar a responsabilidade civil, uma vez que, em possível antinomia com o Código de Defesa do Consumidor, estatui a permanência de validade desse Código em casos de violação de direitos de titulares de dados de consumidores. A LGPD, não exclui sua própria aplicação em violações de dados de consumidores, todavia declara que permanecem tais situações "sujeitas às regras de responsabilidade previstas na legislação pertinente".

Portanto, tratando-se de uma situação jurídica em que o titular de dados seja, também, consumidor, haverá aplicação simultânea tanto da Lei Geral de Proteção de Dados quanto do Código de Defesa do Consumidor (e, eventualmente, de outra legislação). O que deve ocorrer de forma harmônica e, pois, orientada pela Constituição Federal, para realização dos direitos fundamentais de proteção de dados e de promoção da defesa do consumidor.

Outras normas devem incidir não só na responsabilidade civil e nas relações de consumo, mas também, igualmente, na proteção de dados pessoais, no propósito de atribuir efetividade a essa proteção e ao direito à privacidade. A mencionada possibilidade (e viabilidade) está expressa no artigo 64 da Lei Geral. Claudia Lima Marques (2020, p. 25) entende que são três os fundamentos ou as bases para aplicação simultânea de várias leis (de maneira coordenada e coerente) a um dado caso concreto diante de antinomias ou conflitos de leis. Nesse sentido, é oportuna a conclusão de Gustavo Tepedino e Milena Donato Oliva (2020, p. 394), ao analisarem a proteção do consumidor no ordenamento brasileiro. Os autores, diante de situação em que há incidência do CDC e de lei especial, asseveram que "*uma vez presentes seus pressupostos de aplicação, o CDC incide ainda que haja legislação especial para reger a atividade, tendo em vista ser norma de ordem pública e tutelar direito constitucionalmente protegido*".

Estabelecido o cenário, considera-se que muitos são os casos de incidência de multiplicidade de fontes legislativas, desde o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados Pessoais, até o Marco Civil da Internet, a Lei do Cadastro Positivo e mesmo o Código Civil. Com efeito, o diálogo das fontes propicia a imediata recepção de novas situações jurídicas que venham a ser normatizadas, bem como a pronta saída para solucionar casos que tangenciem outras leis, em que eventual e melhor resposta esteja na conjugação de normas com a LGPD. Assim é o caso da responsabilidade civil nas hipóteses de tratamento irregular pelo encarregado, a responder em solidariedade com o controlador, sob a égide da norma de proteção de dados, do Código Civil e, não raras vezes, também de outras legislações.

Percebe-se, assim, que tanto a responsabilidade civil quanto a Lei Geral de Proteção de Dados Pessoais buscam por efetividade. Deveras, há escopo de concretude na LGPD, o que se revela um ponto fundamental na ressignificação do princípio da reparação integral cuja utilização, para autorizar o benefício da própria torpeza pelo transgressor, é contrária ao Direito, tirando-lhe coerência e efetividade. Deve-se, pois, como salientado por Daniel de Andrade Levy (2012, p. 110) ao se referir aos estudos de Rodolphe Mèsa, alargar a concepção.

Aborda essa questão Nelson Rosenvald (2019, p. 450-456), para quem é preciso nova leitura ao princípio, tornando-o apto para (r)estabelecer o desequilíbrio violado, utilizando o

remédio tradicionalmente adotado – o compensatório – com o escopo de restabelecer o ofendido à situação pré-dano; *"mas também pelo resgate de lucros antijurídicos e restituição de benefícios indevidos (restaurando-se o ofensor à situação anterior ao ilícito)"* (ROSENVALD, 2019, p. 456).

A Lei 13.709/2018 protege e cria mecanismos para salvaguardar as informações das pessoas naturais, desafiador papel para cumprir, eis que engloba intangíveis direitos fundamentais e da personalidade. De fato, eventuais práticas de violação desses direitos e interesses podem passar despercebidas pelos lesados. Em enfrentamento a essa situação, o princípio da responsabilidade e da prestação de contas, acompanhado dos dispositivos da Lei, pode e deve permitir transparência, que é princípio expresso na LGPD.

Por conseguinte, almeja-se tornar palpável e possível o abrigo desses direitos e interesses, o que é necessário à prevenção e ao confronto de lesões, não mais permitindo que os ganhos derivados do uso indevido de dados fiquem com o ofensor.

7. CONCLUSÃO

A matéria da proteção de dados pessoais engloba temas relacionados ao direito à privacidade, seu porto de origem, todavia ela acaba extrapolando este âmbito, pois liga-se ao objetivo de promover a funcionalidade de alguns valores fundamentais do ordenamento. A normatização desta área pode até parecer uma intromissão em um domínio já pacificado; mas esse é mais um caso em que a tecnologia é capaz de induzir para modificação de situações estáveis. Assim, não apenas para as pessoas naturais, mas inclusive para os Estados e entes privados, convém estabelecer um regime de proteção de dados. Além disso, em decorrência da maleabilidade e velocidade da tecnologia da informação, nosso país necessita de, com técnica legislativa, gerar legislação cujas prescrições não se esgotem rapidamente. Em especial que não sejam inapropriadas ou insuficientes, diante da necessidade de certas soluções pontuais e concretas.

Concluindo, com a inserção de um direito à proteção de dados pessoais no texto da CF, a condição de direito fundamental autônomo, apesar de ser deveras importante, precisa continuar a ser aplicada com base em interpretação implícita dos princípios constitucionais. O Brasil agora, não mais sofrerá as consequências de um "vácuo" na proteção desse direito implicitamente positivado na CF, conforme consenso doutrinário inclusive acolhido na esfera jurisprudencial.

Na forma de emenda à Constituição, é correta a ponderação de que mediante a sua incorporação ao catálogo constitucional de direitos, esse direito fundamental à proteção de

dados pessoais torna-se um marco que dará maior sustentação ao conjunto regulatório infraconstitucional, bem como, será amplamente benéfico para aplicação pelos órgãos do Poder Judiciário. Adotar-se uma práxis que dê ao direito à proteção de dados pessoais a sua máxima eficácia e efetividade, notadamente na esfera da articulação dessa proteção com outros direitos e garantias fundamentais e bens jurídicos, inclusive provocará vantagens de mercado, que não perderá seu fluxo, mas atenderá aspectos éticos que atualmente são muito valorizados (verdadeiros ativos); tudo além de, no caso de pessoa jurídica, concretizar a compliance esperada nos tempos pós-modernos.

Nos parâmetros da conformidade legal, devem ser premissas inegociáveis o respeito a fidedignidade, à ordem pública, ao interesse social, a compatibilidade moral e ética, aos valores humanos, com especial destaque para os direitos da personalidade do consumidor.

Vale notar que em tempos de crises (como no caso da pandemia causada pelo SARS-CoV-2) os bancos de dados podem ser servir para agravar a vulnerabilidade dos titulares dos dados. Pois, são capazes de amealhar e utilizarem informações que, injustamente, que possuem potencial de redundar em obstáculo para a pessoa o acesso ao crédito, aos serviços sociais e até mesmo para aquisição de produto ou serviço que necessita (inclusive os de mínimo existencial).

Atesta-se a determinação ao Estado para que se promova a defesa do consumidor, inclusive e notadamente, do titular de dados pessoais, cuja proteção também é direito fundamental autônomo. Nessa seara, o consumidor, com inerente vulnerabilidade reconhecida, possui arcabouço jurídico para enfrentar suas condições de desigualdade. Reitera-se que a vulnerabilidade é agravada no caso de a pessoa natural encontrar-se, ao mesmo tempo, nas condições de consumidor e titular de dados.

Particularmente relevante é o fato de que a condição de direito fundamental vem acompanhada de um conjunto de prerrogativas traduzidas por um regime jurídico reforçado e uma dogmática sofisticada, mas que deve ser, em especial no caso brasileiro, desenvolvida e traduzida numa práxis que dê ao direito à proteção de dados pessoais a sua máxima eficácia e efetividade, notadamente na esfera da articulação da proteção de dados com outros direitos e garantias fundamentais e bens jurídicos e interesses de estatura constitucional.

Em síntese, a LGPD surge como apoio para pretensão jurídica desta tese, posto que, como legislação infraconstitucional, direcionada às pessoas públicas e privadas, tem como objetivo a tutela de direitos fundamentais. Logo, a LGPD reforça os argumentos expostos, afinal, dentro da sua tecnicidade característica, deixa evidente que é um instrumento muito mais efetivo na tutela dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento

da pessoa humana do que a própria Constituição Lederal, que agora prevê esses direitos fundamentais enquanto direitos fundamentais.

Não obstante, conforme supracitado, um dos grandes embates quanto a medida de eficácia das normas fundamentais nas relações entre particulares reside no fato de que a titularidade e o destinatário dos direitos fundamentais se confundem.

Desse modo, a Internet deve ser considerada em seus pontos positivos e negativos, afinal, a simples disponibilidade de uma tecnologia não legitima todas as suas utilizações, que devem ser avaliadas com base em valores diferentes daqueles fornecidos pela própria tecnologia. É inegável que é por meio da Internet que se promove a conexão entre pessoas rapidamente e em lugares longíncuos, amplia-se a capacidade de difusão de informações e de conhecimentos, em todas áreas e, como se não bastasse, possibilita maior oportunidade para grupos se manifestarem com mais liberdade. Em contrapartida, o uso da tecnologia é comum aos governos autoritários, seja por meio da restrição ao acesso à Internet, como forma de manutenção de poder, seja pelo uso recorrentemente de *fake news* para manipulação dos cidadãos mais vulneráveis e leigos.

Ainda assim, os riscos do uso tecnológico no mercado estão onipresentes, desde o assédio desmesurado ao consumo, pelo uso dados pessoais como moeda de troca. Evidentemente, sob a escusa de que o digital é o ambiente de total liberdade negocial, os consumidores se tornam ainda mais vulneráveis.

Com efeito, toda a tecnologia inerente à Sociedade da Informação é criação do gênio humano, de modo que todos os defeitos, riscos e perigos aos direitos são de responsabilidade também das pessoas. Neste sentido, é preciso, mais do que nunca, garantir a autonomia privada, todavia, em diálogo com as responsabilidades, em especial quando envolve a atividade de grandes empresas no mercado de consumo, que se destacam como verdadeiros poderes privados no mundo virtual. Por isso, é preciso, nas palavras de Vittorio Frosini, a "*consciência informática",* isto é, a noção de que os novos problemas surgidos em razão da tecnologia são de responsabilidade das próprias pessoas que as desenvolvem.

É dizer que, diante da necessária tutela integral da pessoa humana, como valor central do sistema jurídico, não considerar os deveres e responsabilidades das pessoas frente aos problemas envolvendo a Sociedade da Informação significa subtrair o direito ao seu próprio tempo, afinal, a tecnologia é um vetor condicionante não só da sociedade como, por consequência, do próprio direito.

Por fim, no escopo da responsabilidade civil, apesar da Lei Geral de Proteção de Dados Pessoais referir-se a risco em variadas passagens, parte da literatura tem se posicionado no

sentido de que seria referente à responsabilidade civil subjetiva, muito pela falta de clareza do tema. Contudo, afirmamos que o retorno à subjetividade representaria um passo atrás na responsabilidade civil, haja vista que tal modalidade foi superada também com a LGPD, para a qual basta que a violação da segurança à proteção de dados (ou da legislação correlata) cause dano para que haja responsabilidade do agente. Não está expresso *"independente de culpa",* porém está o risco e isso atrai a responsabilidade civil objetiva.

Nesse contexto, nunca é demais lembrar que sem prejudicar o desenvolvimento econômico e os interesses legítimos de seus agentes, atribuir a devida relevância para a proteção de dados pessoais representa contribuir para o respeito à dignidade da pessoa humana, para o livre desenvolvimento da personalidade e para a liberdade pessoal como autodeterminação, tudo com vistas à construção de uma sociedade livre, justa e solidária no termos de nossa Constituição Federal.

REFERÊNCIAS

AGAMBEN, Giorgio. Deus não morreu. Ele tornou-se dinheiro. Entrevista com Giorgio Agamben. **Instituto Humanas Unisinos**. Porto Alegre. 30 ago. 2012. Entrevista. Disponível em http://www.ihu.unisinos.br/noticias/512966-giorgio-agamben. Acesso em 10 jul 2019.

AGAMBEN, Giorgio. **Homo Sacer**: O poder soberano e a vida nua. 1 2 ed. Belo Horizonte: UFMG, 2007.

ABRAMOVAY, Ricardo. ZANATTA, Rafael Augusto Ferreira. Dados Pessoais Abertos: Pilares dos Novos Mercados Digitais? **RDU,** Porto Alegre, Volume 16, n. 90, nov-dez, 2019.

ARENDT, Hannah. **A Condição Humana**. 10 ed. Rio de Janeiro: Forense Universitária, 2007.

ARTICLE 29. **Opinion 02/2010 on online behavioural advertising**. 22 june 2010. União Europeia. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf Acesso 04 de maio 2020.

BARBOSA, Fernanda Nunes. O dano informativo do consumidor na era digital: Uma abordagem a partir do reconhecimento do direito do consumidor como direito humano. **Revista de Direito do Consumidor,** vol. 122/2019, Mar – Abr, 2019.

BAROCAS, Solon; NISSENBAUM, Helen. **Big Data's End Run around Anonymity and Consent.** In: LANE, Julia, et al. Privacy, Big Data, and the Public Good: Frameworks for Engagement. New York: Cambridge University, 2014. cap. 2, pp. 44-75.

BAROCELLI, Sergio Sebastian**.** Towards the construction of "hyper-vulnerable consumers" category. In: MARQUES, Claudia Lima, PEARSON, Gail, RAMOS, Fabiana (Editors). **Consumer Protection: current challenges and perspectives.** Orquestra, Porto Alegre, 2017.

BARROSO, Luís Roberto. **A nova interpretação constitucional: ponderação, direitos fundamentais e relações privadas.** 2. ed. Rio de Janeiro, RJ: Renovar, 2006.

BAUMAN, Zygmunt. **Vida para consumo**: a transformação das pessoas em mercadoria. Rio de Janeiro: Zahar, 2008.

BAUMAN, Zygmunt. **Globalização:** as consequências humanas. Rio de Janeiro: Zahar, 1999.

BAUMAN, Zygmunt. LYON, David. **Vigilância Líquida**. Tradução Carlos Alberto Medeiros. Rio de Janeiro. Ed Zahar. 2013.

BIONI, Bruno Ricardo. **A proteção dos dados pessoais**: A função e os limites do consentimento. 1ª ed. São Paulo: Forense. 2018

BIONI, Bruno Ricardo. **A proteção dos dados pessoais**: A função e os limites do consentimento. 2ª ed. São Paulo: Forense, 2020.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. In: MELLO NETO, Luis Soares. TASSO, Fernando Antonio. **Cadernos Jurídicos:** Direito Digital e Proteção de dados. São Paulo, ano 21, nº 53, p. 1-202, Janeiro-Março, 2020.

BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. **Privacidade e pandemia**: recomendações para o uso legítimo de dados no combate à COVID-19. Conciliando o combate à COVID-19 com o uso legítimo de dados pessoais e o respeito aos direitos fundamentais. São Paulo: Data Privacy Brasil, 2020.

BRASIL. **Constituição: República Federativa do Brasil de 1988.** Brasília, DF: Senado Federal, 1988.

BLUM, Rita Peixoto Ferreira. **O Direito à privacidade e à Proteção dos Dados do Consumidor.** São Paulo: Almedina, 2018.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos**, São Paulo, ano 21, nº 53, p. 163-170, Janeiro-Março/2020.

CARVALHO, Ana Paula Gambogi. O consumidor e o Direito à autoderminação informacional: considerações sobre os bancos de dados eletrônicos. **Revista de Direito do Consumidor.** vol. 46, Abr – Jun, 2003. Versão digital.

CASTELLS, Manuel. **A Sociedade em Rede**: A era da informação. 3 ed. São Paulo: Paz e Terra, 2000.

CASTELLS, Manuel. **A Galáxia da Internet**: Reflexões sobre a Internet, Negócios e Sociedade. Rio de Janeiro: Zahar, 2015.

CRANOR, Lorrie Faith. MCDONALD, Aleecia M. **Beliefs and Behaviors**: Internet Users' Understanding of Behavioral Advertising. 2010. Disponível em http://ssrn.com/abstract=1989092 Acesso 30 maio 2020.

DA ROS, Luciano. **Difícil hierarquia: a avaliação do Supremo Tribunal Federal pelos**

magistrados da base do Poder Judiciário no Brasil. Revista Direito GV, v. 9, n. 1, p. 47-64, 2013. http://dx.doi.org/10.1590/S1808- 24322013000100003

DA ROS, Luciano. **O Custo da Justiça no Brasil: Uma Análise Comparativa Exploratória.** Newsletter do Observatório de Elites Políticas e Sociais do Brasil, v. 2, n. 9, p. 1-15, 2015.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** Fundamentos da Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2019.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Rev. Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

LESSIG, Lawrence. **Code: Version 2.0.** Estados Unidos: Basic Books, 2006.

FEDERAL TRADE COMMISSION. Bureau of Consumer Protection. **Online Profiling:** A Report To Congress, Washington, EUA. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-profiling-federal-trade-commission-report-congress-june-2000/onlineprofilingreportjune2000.pdf>. Acesso em: 02 maio 2020.

FERRAZ JÚNIOR, Tércio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado**. Revista da Faculdade de Direito da Universidade de São Paulo. 1993. v. 88.

FERREIRA, Jussara Suzi Assis Borges Nasser. ROSA, André Luís Cateli. Fornecimento eletrônico de dados pessoais dos consumidores: Responsabilidade Civil Objetiva e Solidária e o Dano Social. **Revista de Direito do Consumidor**, vol. 122/2019, p. 233 – 263, Mar – Abr., 2019.

FOUCAULT, Michel. **Vigiar e Punir**. O nascimento da prisão. Tradução de Raquel 20 ed. Ramalhete. Petrópolis: Vozes, 1999.

FOUCAULT, Michel. **Nascimento da biopolítica**. Tradução Eduardo Brandão. São Paulo: Martins Fontes, 2008.

FOUCAULT, Michel. **Microfísica do Poder**. Trad. Roberto Machado. 2 ed. Rio de Janeiro: Paz e Terra, 2015.

FORTES, Vinicius Borges. **Os direitos de privacidade e a proteção de dados na internet.** São Paulo: Lumen juris, 2016.

GONÇALVES, Victor Hugo Pereira. **Marco civil da internet comentado**. 1. ed. São Paulo: Atlas, 2017.

GUTWIRTH, Serge; HILDEBRANDT, Mireille. Some Caveats on Profiling. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul (ed.). **Data Protection in a Profiled World**. Dordrecht: Springer, 2010.

GRAU, Eros Roberto. **A ordem econômica na constituição de 1988**. São Paulo: Malheiros, 2006.

GRINOVER, Ada Pelegrine et al. **Código brasileiro de defesa do consumidor**. 6. ed. São Paulo: Forense Universitária, 1999.

HARARI, Yuval Noah. **Homo Deus: uma breve história do amanhã**. Trad. Paulo Geiger. São Paulo: Cia. Das Letras, 2015. Edição em versão eletrônica (epub). Não paginado.

HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Belo Horizonte: Âyné, 2018.

HOOFNAGLE, Cris Jay. URGAN, Jennifer M. LI, Su. Privacy and modern advertising: most US internet users want 'do not track' to stop collection about their online activities. In: **Amestedam Privacy Conference**, 2012. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152135 Acesso 30 maio 2020.

LACE, Susane. **The glass consumer**: life in a surveillance society. Brisol: Policy, 2005.

LEONARDI, Marcel. **Tutela da Privacidade na Internet**. São Paulo: Saraiva, 2011.

LEVY, Pierri. **As tecnologias da Inteligência**: O futuro do pensamento na era da informática. São Paulo: Editora 34, 1993.

LIPOVESTKY, Gilles. **A felicidade paradoxal:** Ensaio sobre a sociedade do hiperconsumo. Tradução Maria Lucia Machado. São Paulo: Companhia das Letras, 2007.

LOMAS, Natasha. An EU coalition of techies is backing a 'privacy-preserving' standard for COVID-19 contact tracing, **TechCrunch**, 1 de abril de 2020. Disponível em: https://techcrunch.com/2020/04/01/an-eu-coalition-of-techies-is-baprivacypreservingstandard-for covid-19-contacts-tracing/. Acesso dia 17 abril 2020.

LOVELUCK, Benjamin. **Redes, Liberdade e Controle**: Uma genealogia política da internet. Petrópolis: Ed. Vozes, 2015.

MAIMONE, Flávio Henrique Caetano de Paula. **Responsabilidade civil na LGPD: efetividade na proteção de dados pessoais** - Indaiatuba, SP: Editora Foco, 2022. e-PUB.

MANOLESCU, Dan. **Data protection as a fundamental right.** Effectius, Brussels, n. 5, jun./2010. Disponível em: <http://effectius.com/yahoo_site_admin/assets/docs/Data_protection_as_a_fundamental_right_Dan_Manolescu_Issue5.16761659.pdf>. Acesso em 20 jul. 2020.

MARCACINI, Augusto Tavares Rosa. **Direito e Informática: uma abordagem jurídica sobre a criptografia.** Rio de Janeiro: Forense, 2002.

MATTIA, Fábio Maria de. Direitos da Personalidade Aspectos Gerais. **Doutrinas Essenciais de Direito Civil**. vol. 3, Out, 2010 (versão digital).

MAYER-SCÕNBERGER. **General development of data protection in Europe**. In: AGRE, Phillip; ROTENBERG, Marc. Technology andprivacy: The new landscape. Cambridge. MIT Press, 1997.

MENDES, Laura Shertel. **A Vulnerabilidade do consumidor quanto ao tratamento de dados pessoais.** Revista de Direito do Consumidor. Vol. 102, nov – dez, 2015.

MENDES, Laura Shertel. **Privacidade, Proteção de dados e Defesa do consumidor**: Linhas gerais de um novo direito fundamental. São Paulo: saraivajur, 2019.

MENDES, Laura Shertel. **Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais: Novo direito fundamental precisará ter contornos definidos tanto pela jurisprudência, quanto pela doutrina. Jota**. 10 de maio de 2020. Disponível em https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dadospessoais-10052020 Acesso em 15 maio 2020.

MENDES, Laura Schertel. **Data protection in Brazil: New Developments and Current Challenges.** In: GUTWIRTH, Serge, et al (eds.). Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges. Dordrecht (Holanda): Springer, 2014. p. 3-20.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo.** Dissertação (Mestrado em Direito). Brasília: Universidade de Brasília, 2008.

MENDES, L. S. et al. **Tratado de proteção de dados pessoais.** 1. ed. [S.l.]: Grupo GEN, 2021.

NISSEBAUM, Helen. **Privacy in contextual: Technology, Policy, and the Integrity of Social Life**. California: Stanford Law Books, 2009.

PRUX, Oscar Ivan. **A Interação entre os Direitos da Personalidade e o Direito do Consumidor: Um Diálogo Construtivo. Revista do Instituto do Direito Brasileiro.** Ano 3, n. 1, p. 461-481, 2014. Disponível em: <http://www.idb-fdul.com/uploaded/files/2014_01_00461_00481.pdf>. Acesso em: 26 Jun. 2020, p. 474.

PRUX, Oscar Ivan. SOUSA, KEVIN. **(DES)LIBERDADE VIRAL NA PANDEMIA: UMA RELEITURA DA ESCALADA POR DADOS PESSOAIS E SEUS IMPACTOS À LUZ DOS DIREITOS DA PERSONALIDADE E A PROTEÇÃO DE DADOS.** Revista Newton Paiva. Disponível em: <https://revistas.newtonpaiva.br/redcunp/n-43-desliberdade-viral-na-pandemia-uma-releitura-da-escalada-por-dados-pessoais-e-seus-impactos-a-luz-dos-direitos-da-personalidade-e-a-protecao-de-dados/>. Acesso em: 18 nov. 2021, p. 49.

QUINTARELLI, Stefano. **A revolução digital e transformações sociais**. Tradução Rodrigo Bravo. 2019. Disponível em https://dowbor.org/2019/02/stefano-quintarelli-a-revolucao-digital-e-transformacoes-sociais-fev-2019-10p.html/ Acesso 07 maio 2020.

RASLAN, Daniela Andrade. CALAZANS, Angélica Toffano Seidel. ***Data Warehouse:*** **conceitos e aplicações.** Universitas Gestão e TI, Brasília, v. 4, n. 1, p. 25-37, jan./jun. 2014.

ROCHA, Luiz Alberto G. S. MAZIVIERO, Luiza. **Por um click: Como a Lei Geral de Proteção de Dados Pessoais possibilita o "consentimento involuntário" de fornecimento de informações de particulares a empresas.** In: VERBICARO, Dennis. VERBICARO, Loiane. VIEIRA, Janaina (Orgs). **Direito do Consumidor Digital**. São Paulo, Lumen juris, 2020.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de janeiro: Renovar, 2008.

RODOTÀ, Stefano. **Elaboratori elettronici e controllo sociale**. Bologna: II Mulino, 1973.

ROQUE, André. A tutela coletiva dos dados pessoais na Lei Geral de Proteção de Dados Pessoais (LGPD). **Revista Eletrônica de Direito Processual** – REDP. Rio de Janeiro. Ano 13. Volume 20. Número 2. Maio a Agosto de 2019.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional.** 13. ed. [S.l.]: Livraria do Advogado Editora, 2018.

MONTEIRO, António Pinto; NEUNER, Jörg; SARLET, Ingo. **Direitos fundamentais e direito privado: uma perspectiva de direito comparado.** 1. ed. [S.l.]: Almedina Brasil, 2007.

SARMENTO, Daniel. **Direitos Fundamentais e Relações Privadas**. 2a ed. Rio de Janeiro: Lumen Juris, 2010.

SIQUEIRA, D. P.; FERRARI, C. C. **O direito à informação como direito fundamental ao estado democrático.** Revista Direitos Sociais e Políticas Públicas - UNIFAFIBE, v. 4, p. 124-153, 2016.

SILVA, Adriano Correa. Homo economicus, de Foucault, e animal laboransm de Arendt: conceitos para pensar o presente. **Instituto Humanas Unisinos**. Porto Alegre, edição 468, 29 de junho de 2015. Disponível http://www.ihuonline.unisinos.br/artigo/6023-adriano-correia-1 em Acesso em 20 de maio de 2020.

SILVA, Bruno Anderson Souza. **A profanação do Improfano**: O capitalismo como religião e uma reflexão ética a partir de Agamben. Rio Grande do Sul: Editorafi. 2018.

SILVA, Joseane Suzart Lopes da. A Proteção de dados pessoais dos consumidores e a Lei 13.709/2018: em busca da efetividade dos direitos a privacidade, intimidade e autodeterminação. **Revista de Direito do Consumidor**, vol. 121/2019, Jan – Fev., 2019.

SOARES, Marcelo Negri; KAUFFMAN, M. E.; CHAO, K.; SAAD, M. O. **New Technologies and the Impact on Personality Rights in Brazil.** PENSAR - REVISTA DE CIÊNCIAS JURÍDICAS, v. 25, p. 1-12, 2020.

SOLOVE, Daniel J. **Understanding Privacy**. Harvard University Press, 2008.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco Civil da Internet: construção e aplicação.** Juiz de Fora: Editar, 2016.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. **Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet.** Pensar, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017.

WARREN, Samuel D. BRANDEIS, Louis D. The Right to Privacy**. Harvard Law Review,**

Vol. 4, No. 5, Dec., 1890, pp. 193-220.

ZANATTA, Rafael. **Proteção de dados pessoais como regulação do risco: uma nova moldura teórica?** In: I ENCONTRO DA REDE DE GOVERNANÇA DA INTERNET, 2017, Rio de Janeiro. 20 pp.

ZUBOFF, Shoshana. Big Other: Capitalismo de vigilância e perspectivas para uma civilização de informação. In. BRUNO, Fernanda. CARDOSO, Bruno. KANASHIRO, Marta. GUILHON, Luciana. MELGAÇO, Lucas (orgs.). **Tecnopolíticas de vigilância**: Perspectivas da margem. São Paulo, boitempo, 2018.