XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

DANIELLE JACON AYRES PINTO

MARCOS VINÍCIUS VIANA DA SILVA

Copyright © 2022 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Diretora Executiva - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - UNIVEM/FMU – São Paulo
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
Vice-presidente Nordeste - Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR – Ceará

Representante Discente: Prof. Dra. Sinara Lacerda Andrade – UNIMAR/FEPODI – São Paulo

Conselho Fiscal:
Prof. Dr. Caio Augusto Souza Lara – ESDHC – Minas Gerais
Prof. Dr. João Marcelo de Lima Assafim - UCAM – Rio de Janeiro
Prof. Dr. José Filomeno de Moraes Filho – Ceará
Prof. Dr. Lucas Gonçalves da Silva – UFS – Sergipe
Prof. Dr. Valter Moura do Carmo – UNIMAR – São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Daniela Marques De Moraes – UNB – Distrito Federal
Prof. Dr. Horácio Wanderlei Rodrigues - UNIVEM – São Paulo
Prof. Dr. Yuri Nathan da Costa Lannes - Mackenzie – São Paulo
Comunicação:
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali – Rio Grande do Sul
Profa. Dra. Maria Creusa De Araújo Borges - UFPB – Paraíba
Prof. Dr. Matheus Felipe de Castro - UNOESC – Santa Catarina
Relações Internacionais para o Continente Americano:
Prof. Dr. Heron José de Santana Gordilho - UFBA – Bahia
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM – Rio Grande do Sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA – Maranhão
Relações Internacionais para os demais Continentes:
Prof. Dr. José Barroso Filho – ENAJUM
Prof. Dr. Rubens Beçak - USP – São Paulo
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba – Paraná
Eventos:
Prof. Dr. Antônio Carlos Diniz Murta - Fumec – Minas Gerais
Profa. Dra. Cinthia Obladen de Almendra Freitas - PUC – Paraná
Profa. Dra. Livia Gaigher Bosio Campello - UFMS – Mato Grosso do Sul

Membro Nato – Presidência anterior Prof. Dr. Raymundo Juliano Feitosa – UMICAP – Pernambuco

D597

Direito, governança e novas tecnologias III [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto; Marcos Vinícius Viana da Silva.

– Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-625-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias.

XXIX Congresso Nacional do CONPEDI Balneário Camboriu - SC (3: 2022: Florianópolis, Brasil).

CDU: 34



Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

Apresentação

O XXIX Congresso Nacional do CONPEDI – Balneário Camboriú, em seu Grupo de trabalho Direito, Governança e Novas Tecnologias, apresentou temas relacionados às novas tecnologias, seus impactos na vida em sociedade, o papel do Estado nas demandas internacionais e o papel central ocupado pela governança nestes cenários.

Assim, a presente apresentação introduz os artigos apresentados no GT, informando desde já, que os temas se completam e permitem o devido aprofundamento teórico prático.

O primeiro trabalho apresentado, de autoria de Sílvia Helena Schimidt e Romulo Rhemo Palitot Braga, e denominada "SEGURANÇA HUMANA E PROTEÇÃO DE DADOS: DOS RISCOS DA DISCRIMINAÇÃO ALGORÍTMICA EM TEMPOS DE COVID-19" enfrenta os riscos da discriminação algorítmica durante a pandemia da COVID-19 e os direitos da personalidade. A pesquisa analisou os contornos do capitalismo de vigilância à proteção de dados do usuário, a problemática do reconhecimento facial e seu eventual viés preconceituoso e discriminatório.

Na sequencia o artigo intitulado "VÍDEOS VEICULADOS NO YOUTUBE: ARTE OU INCITAÇÃO AO SUICÍDIO?", de Manoella Miranda Keller Bayer e Eduardo Biavatti Lazarini, discorre sobre a dificuldade de compatibilizar o rápido desenvolvimento da tecnologia frente ao ritmo mais lento de atualização do direito, tratando em especial dos vídeos veiculados no youtube e a responsabilidade civil atrelada.

O artigo das autoras Agatha Gonçalves Santana, Raíza Barreiros e Andreza Maria Nascimento De Mattos, intitulado "OS IMPACTOS TECNOLÓGICOS NOS SERVIÇOS PÚBLICOS NO BRASIL: A FORMAÇÃO DE UMA ADMINISTRAÇÃO PÚBLICA DIGITAL", traz a questão da Administração Pública no contexto tecnológico e seus serviços prestados. Questiona-se se o Brasil está vivenciando uma transformação de sua Administração Pública, a ponto de se poder afirmar haver de fato a observância de uma Administração Pública Digital no âmbito dos serviços públicos.

Na sequência os autores Gustavo Ferraro Miranda e Raphael da Rocha Rodrigues Ferreira, apresentaram o artigo "PROCESSO DE DEMOCRATIZAÇÃO DA PROTEÇÃO DOS

DADOS PESSOAIS E PRIVACIDADE: UM ESTUDO COMPARADO E HISTÓRICO PARA A REFLEXÃO DO CASO BRASILEIRO", tal trabalho trata da democratização da proteção de dados pessoais e privacidade no caso brasileiro à luz do cenário internacional, realizando uma análise do desenvolvimento histórico da autodeterminação informativa e de sua vinculação aos direitos da personalidade,

"O DEVIDO PROCESSO LEGAL NA ERA DOS ALGORITMOS: UMA PROPOSTA DE RELEITURA DOS PRINCÍPÍOS CONSTITUCIONAIS DE PROCESSO CIVIL" é obra da autoria de José Antonio de Faria Martos, Oniye Nashara Siqueira e José Sérgio Saraiva, discorre sobre a elevação do patamar tecnológico experimentada pela sociedade desde o advento da internet proporcionou ao Poder Judiciário a modificação expressiva da gestão processual.

"CONSIDERAÇÕES ACERCA DA REGULAÇÃO TRANSNACIONAL PARA O DESENVOLVIMENTO ÉTICO DA INTELIGÊNCIA ARTIFICIAL", de Hernani Ferreira e Jose Everton da Silva, demonstra como a discussão inovadora relativa a IA poderá facilitar a criação de uma legislação transnacional, baseada em uma ética global.

"O DIREITO FUNDAMENTAL À INFORMAÇÃO FRENTE AO ACESSO DESIGUAL ÀS TECNOLOGIAS DE COMUNICAÇÃO NO BRASIL" da autoria de Mariana Mostagi Aranda e Zulmar Antonio Fachin, apresenta uma reflexão sobre o direito fundamental à informação e a internet frente ao acesso desigual às tecnologias de comunicação, em especial o direito fundamental de informação e comunicação, a partir das limitações de acesso aos meios de comunicação digital e da internet no Brasil.

"A UTILIZAÇÃO DA INTELIGÊNCIA ARTIFICIAL PARA APRECIAÇÃO DE PEDIDOS DE TUTELA PROVISÓRIA DA EVIDÊNCIA EM CARÁTER LIMINAR" da lavra de Bruno Berzagui e Jose Everton da Silva, enfrenta a possibilidade de utilização da inteligência artificial (IA) para apreciação de pedidos de tutela provisória de evidência em caráter liminar, de forma mais específica nestes casos, uma vez que dependem de prova já constituída em decisão que cabe reversão.

"RESPONSABILIDADE CIVIL DO MÉDICO PELO USO DA INTELIGÊNCIA ARTIFICIAL NOS PROCEDIMENTOS ESTÉTICOS", escrito por Divaneide Ferreira Dos Santos e José Carlos Francisco dos Santos, aborda a responsabilidade do médico em procedimentos estéticos utilizando a Inteligência Artificial (IA) e examinar quais direitos e

obrigações são devidos à relação de consumo entre médico e paciente, identificando também as formas pelas quais o erro médico é reparado, especialmente sob a tutela do Código de Defesa do Consumidor.

A obra dos autores Eduardo Lincoln Domingues Caldi e Zulmar Antonio Fachin é intitulada: "A COLONIZAÇÃO DIGITAL DA ESFERA PESSOAL DO INDIVÍDUO E VIOLAÇÕES AO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS", e aborda a colonização digital da esfera pessoal do indivíduo e seu impacto no direito fundamental à proteção de dados pessoais, discutindo como o movimento de extração dos dados pessoais ocorre frente ao posicionamento do Direito contemporâneo.

O artigo intitulado "ARTICULAÇÕES EPISTEMOLÓGICAS E A CONVERGÊNCIA INTERDISCIPLINAR DA CIÊNCIA DA INFORMAÇÃO COM A CIÊNCIA JURÍDICA NO CONTEXTO DIGITAL" da autoria de Marcos Alexandre Biondi e José Carlos Francisco dos Santos enfrenta as articulações da epistemologia tradicional e suas limitações perante a epistemologia complexa. Evidenciando a interdisciplinaridade entre a Ciência da Informação e a Ciência Jurídica no contexto contemporâneo digital.

O artigo intitulado "A ALGORITMIZAÇÃO DO PROCESSO: NUANCES SOBRE OS PROJETOS DE INTELIGÊNCIA ARTIFICIAL NO PODER JUDICIÁRIO", redigido por Oniye Nashara Siqueira, José Antonio de Faria Martos e José Sérgio Saraiva debruça sobre a desatualização do sistema de justiça brasileiro, que digitalizou o sistema processual, porém não otimizou sua utilização, em claro atraso na aplicação de diferentes possibilidades tecnológicas.

Os autores Andrey Luciano Bieger, Reginaldo Pereira e Idir Canzi apresentam o trabalho intitulado "PREVALECE NO SUPREMO TRIBUNAL FEDERAL O CARÁTER FRACO DA PRECAUÇÃO? PROBLEMATIZAÇÕES A PARTIR DO JULGAMENTO DO RECURSO EXTRAORDINÁRIO 627.189/SP", o qual aborda a interpretação do princípio da precaução a partir do julgamento do Recurso Extraordinário 627.189/SP, informa que a compreensão deferida por cada julgador pode representar resultados completamente distintos em um mesmo caso.

Os autores Marcelo Markus Teixeira, Reginaldo Pereira e Idir Canzi apresentam o trabalho intitulado "TRANSNORMATIVIDADE E GOVERNANÇA DE RISCOS SOCIOAMBIENTAIS DE NOVAS TECNOLOGIAS", discutindo, entre outros, como as novas tecnologias (ainda que apresentam riscos socioambientais), possibilitam a superação de distintas adversidades, conferindo base material para a economia informacional.

Os autores Frederico Thaddeu Pedroso, Gabriel Lima Mendes e Isabel Christine Silva De Gregori apresentam a obra “O USO DO SISTEMA DE GEOLOCALIZAÇÃO DE APLICATIVOS DE STARTUPS EM TEMPOS DE PANDEMIA COVID-19: UMA RELAÇÃO DE BIOPOLÍTICA E SURVEILLANCE A PARTIR DE FOUCAULT”, narrando as relações da biopolítica como sistema de poder e controle dos indivíduos com o uso do sistema de geolocalização de aplicativos de Startups que visam a localização de seus usuários em tempos de pandemia COVID-19.

A obra intitulada “A IMPORTÂNCIA DA REGULAMENTAÇÃO LEGAL DAS STARTUPS POR MEIO DA UTILIZAÇÃO DA PROPRIEDADE INTELECTUAL COMO PROPRULSORA DA SEGURANÇA JURÍDICA E DO SEU CRESCIMENTO EXPONENCIAL”, de Frederico Thaddeu Pedroso e Gabriel Lima Mendes, aborda a importância das inovações tecnológicas promovidas por empresa startups, bem como a respeito da possibilidade de implantação jurídica desse modelo no âmbito da propriedade intelectual.

O texto de Ana Paula Bustamante, Eduardo Dos Santos Pereira e Ruan Silva Gomes, intitulado “DIREITO E TECNOLOGIA: INTELIGÊNCIA ARTIFICIAL E FERRAMENTAS TECNOLÓGICAS COMO CATALISADORES PROCEDIMENTAIS NO PODER JUDICIÁRIO”, expõe como o Poder Judiciário brasileiro padece de uma crise procedimental em razão da quantidade exorbitante de processos distribuídos, e que somente a aplicação tecnológica permitirá a redução desta quantidade que apenas aumenta.

Por fim, o trabalho “ESTRATÉGIA JURÍDICA: ONLINE DISPUTE RESOLUTION - ODR COMO INSTRUMENTO A RESOLUÇÃO EXTRAJUDICIAL DE CONFLITOS”, de autoria de Gustavo Silva Macedo e Frederico de Andrade Gabrich, analisa a viabilidade da plataforma Online Dispute Resolution (ODR) como estratégia jurídica viável para acesso do cidadão à justiça, preferencialmente sem a judicialização dos conflitos relativos aos direitos patrimoniais disponíveis.

Por todo este conteúdo, os trabalhos do GT do Conselho Nacional de Pesquisa em Direito, renderam uma tarde profícua de produção intelectual aplicada ao bom serviço do Sistema Nacional de Pós-Graduação na área do Direito.

Tenham uma excelente leitura.

Dra. Danielle Jacon Ayres Pinto.

Dr. Marcos Vinícius Viana da Silva.

PROCESSO DE DEMOCRATIZAÇÃO DA PROTEÇÃO DOS DADOS PESSOAIS E PRIVACIDADE: UM ESTUDO COMPARADO E HISTÓRICO PARA A REFLEXÃO DO CASO BRASILEIRO

DEMOCRATIZATION PROCESS OF THE PROTECTION OF PERSONAL DATA AND PRIVACY: A COMPARATIVE AND HISTORICAL STUDY TO REFLECT ON THE BRAZILIAN CASE

Gustavo Ferraro Miranda [1]
Raphael da Rocha Rodrigues Ferreira [2]

Resumo

Este artigo busca compreender o avanço do processo de democratização da proteção de dados pessoais e privacidade no caso brasileiro à luz do cenário internacional, realizando uma análise do desenvolvimento histórico da autodeterminação informativa e de sua vinculação aos direitos da personalidade, até uma transição ao momento presente, em que a tutela individual dos dados supostamente foi substituída pelas várias formas de tutela coletiva, em razão da tendência à constitucionalização desse direito, que o coloca em paridade com outros direitos fundamentais no ordenamento jurídico nacional e estrangeiro. A partir desse debate, cabe uma reflexão quanto à eficácia da autodeterminação informativa atualmente em cumprir com a finalidade a que foi originada: a integração do titular à gestão de suas informações particulares, de modo que fosse possível dispor adequadamente dos dados conforme se construía uma compreensão efetiva do tratamento de dados. Uma das missões deste trabalho é apresentar uma nova perspectiva da tutela individual que desvirtue a antiga compreensão individualista da privacidade, entendendo a autodeterminação informativa como um instrumento político de defesa à subjetividade humana e ao livre desenvolvimento da personalidade. Este é o processo de democratização que o artigo se propõe a discutir, e que será investigado em relação ao Brasil, entendendo a postura do Estado quanto às maneiras de aproximar o cidadão comum ao tratamento de seus dados pessoais, tornando-o capaz de proteger a sua privacidade e com isso tornando a sociedade apta a consentir.

Palavras-chave: Direito comparado e histórico, Democratização, Direitos fundamentais, Proteção de dados

Abstract/Resumen/Résumé

This article aims to understand the progress of the democratization process of the protection of personal data and privacy in the Brazilian case in the light of the international scenario, performing an analysis of the historical development of the right to informational self-determination and its link to the personality rights, making a transition to the present

[1] Pesquisador do Observatório Data Protection & Business Brasil.

[2] Professor da Faculdade de Direito da Universidade Presbiteriana Mackenzie (UPM). Pesquisador do Observatório Data Protection & Business Brasil.

moment, in which the individual guardianship of data has been supposedly replaced by the various forms of collective guardianship due to the tendency to constitutionalize data protection, which pairs this right to the fundamental ones in the national and foreign legal systems. From this debate, it's fair to reflect on the current effectiveness of the informational self-determination in fulfilling the purpose that originated this right: the integration of the subjects to the management of their private information, so that it's possible to properly dispose of the data, having an effective understanding about the data processing. One of the missions of this work is to present a new perspective of the individual guardianship that disvirtues the old individualistic concepct of privacy, understanding that the informational self-determination is actually a political instrument to defend the human subjectivity and the free development of the personality. This is the democratization process that the article proposes, which will be investigated in the Brazilian case, noting the actions of the government regarding the ways to approach the common citizens to the processing of their personal data, capacitating them to protect their privacy and thus making the society able to consent.

Keywords/Palabras-claves/Mots-clés: Comparative and historical law, Democratization, Fundamental rights, Data protection

PROBLEMA – Diante de todos os avanços jurídicos e institucionais a favor de uma tutela coletiva dos dados pessoais, a autodeterminação informativa se tornou obsoleta em sua função como um instrumento de proteção ao titular?

TEMA CENTRAL – A democratização da proteção de dados a partir da compreensão e integração do titular ao tratamento de seus dados pessoais.

OBJETIVOS – É um objetivo deste trabalho o desenvolvimento do conceito de processo de democratização de proteção de dados a partir de uma nova perspectiva da autodeterminação informativa como um instrumento político de zelo à subjetividade humana e ao livre desenvolvimento da personalidade. Além disso, o artigo possui como um segundo objetivo o estudo dos dispositivos de tutela individual de dados pelo titular na LGPD, a fim de apurar como o legislador brasileiro se posiciona frente à importância da autodeterminação informativa.

JUSTIFICATIVAS – Existe um crescente movimento no sentido da tutela coletiva dos dados pessoais no Brasil, isso se dá em razão de fatores que derivam: (i) da complexidade técnica e contratual do tratamento automatizado de dados, que dificulta o entendimento do cidadão comum desses procedimentos; (ii) da consideração da proteção de dados como um direito fundamental, que se reflete tanto nacional quanto internacionalmente; (iii) da consolidação de normas que contribuíram para ampliar o poder da tutela coletiva, como a Lei de Ações Civis Públicas e o Código de Defesa do Consumidor. Por conta de todos estes elementos, questiona-se a efetividade da autodeterminação informativa e como ela deve ser vista, entendendo principalmente o vínculo da proteção de dados aos interesses da sociedade.

METODOLOGIAS – Será realizado um estudo comparado e histórico por meio da investigação de documentos legais sobre a origem e a aplicação atual da autodeterminação informativa; a tutela coletiva será investigada com base nas leis que possibilitam o seu exercício; e será avaliada a postura jurídica assumida no país quanto à importância da autodeterminação informativa, entendendo as funções da ANPD (Autoridade Nacional de Proteção de Dados) e de autoridades estrangeiras; e identificando discussões relevantes sobre o papel do titular no tratamento de dados. Durante toda a estruturação teórica deste trabalho, serão referenciadas pesquisas científicas de acadêmicos com expertise nas respectivas matérias.

INTRODUÇÃO

O Brasil se vê em um momento histórico da proteção à privacidade, considerando a vigência de sua primeira Lei Geral de Proteção de Dados (LGPD) e da classificação da proteção de dados como um direito fundamental na Constituição Federal, a partir da Emenda Constitucional n° 115 de 2022. Verifica-se que carregamos um histórico de proteção a direitos difusos e coletivos por meio do aprimoramento contínuo de documentos legais e instituições responsáveis por zelar pelos interesses da sociedade, o que pode significar uma compatibilidade à proposta de co-regulação trazida pela LGPD, com inspiração no Regulamento Geral de Proteção de Dados europeu (GDPR).

No entanto, existe um direito cuja aplicação se viu dificultada ao longo dos anos, em razão do forte desenvolvimento das tecnologias de predição de comportamento e a sua disseminação do mercado. A autodeterminação informativa deu origem à proteção de dados e hoje possui uma efetividade desafiadora, como argumentam estudiosos da relação entre a tecnologia e o direito, mas é apresentada na LGPD como um fundamento central para a proteção de dados, implicando a persistência de sua relevância na atualidade.

Dito isso, cabe uma análise acerca da trajetória da autodeterminação informativa desde a sua origem até a sua presença na privacidade do século XXI, visando demonstrar que a tutela individual não deve ser enxergada atualmente apenas como um interesse liberal, pois há mais interesses em jogo, e a autodeterminação informativa pode representar uma peça-chave para zelar pelo livre desenvolvimento da personalidade, pela subjetividade humana e pela democracia, atuando como um instrumento de conscientização das pessoas, a fim de evitar que a inserção do tratamento automatizado de dados no Brasil crie uma realidade distópica em que o livre arbítrio se perdeu.

1. DESENVOLVIMENTO

1.1 A CONSTRUÇÃO DA AUTODETERMINAÇÃO INFORMATIVA

A autodeterminação informativa é um fundamento da proteção de dados pessoais no Brasil, previsto no art. 2º, inciso II, da LGPD. O surgimento deste valor no ordenamento jurídico nacional é certamente recente, mas assim como a proteção de dados, a sua origem remete a discussões que ocorrem há mais de quarenta anos na Europa, num cenário em que se iniciava o tratamento automatizado de dados pelo poder público.

Em verdade, os precedentes da autodeterminação informativa são ainda mais antigos, pois este conceito é fruto de debates jurisprudenciais na Alemanha desde a década de 60 e 70

acerca dos direitos da personalidade, que se formaram, de acordo com a doutora em direito Laura Schertel Ferreira Mendes, a partir de três elementos basilares: a proteção abrangente, a autodeterminação e a abstração. Essencialmente, o conceito de autodeterminação seria um poder de decisão acerca de como cada indivíduo desejava se apresentar à sociedade, e em que medida terceiros poderiam dispor de sua personalidade, sendo função do Estado garantir uma proteção abrangente de qualquer informação pessoal, independentemente do grau de intimidade, compreendendo ainda, que este direito seria dotado de abstração, o que permitiria uma interpretação extensiva dos direitos da personalidade, estabelecendo que a ameaça ao indivíduo deveria ser analisada no caso concreto.[1]

Esta perspectiva foi essencial para o desenvolvimento da autodeterminação informativa, pois naquela época pouco se sabia sobre os impactos que a tecnologia viria a ter no futuro das pessoas quanto aos seus direitos fundamentais à intimidade, vida privada, honra e imagem,[2] e especialmente ao direito humano de livre desenvolvimento da personalidade.[3]

Observa-se o amadurecimento da discussão sobre os direitos da personalidade ao realizar um paralelo com o contexto legislativo de proteção de dados na Alemanha entre 1970 e 1977. Na primeira data, entrou em vigor uma legislação visando regulamentar o tratamento automatizado de dados por hospitais públicos no Estado de Hesse (*Hessisches Datenschutzgesetz*): o documento previa uma lista de três direitos concedidos aos titulares, como a possibilidade de acesso e retificação dos dados pessoais no caso de equívoco em seu tratamento, porém, consistia em um rol restrito que ainda não contemplava, por exemplo, os direitos de consentir ou rejeitar o tratamento de dados de acordo com a vontade do titular.[4]

Em contrapartida, em 1977, a BDSG ou lei federal alemã entrou em vigor (*Bundesdatenschutzgesetz*) pioneiramente regulamentando o tratamento de dados em todo o território nacional. Mesmo não apresentando uma distinção clara entre dados pessoais e dados pessoais sensíveis, a legislação aprofundou a participação do titular ao condicionar o tratamento de dados ao seu consentimento escrito e inequívoco, salvo se dada permissão expressa pelas autoridades competentes,[5] como o Comissário Federal para Proteção de Dados e Liberdade de Informação, instituído por meio deste ato.

Além disso, a BDSG passou a dividir os direitos dos titulares em relação aos setores público e privado, abordando novas possibilidades, como o bloqueio de acesso aos dados

[1] MENDES, 2020
[2] Inciso X, Art. 5º, Constituição Federal
[3] Ver nesse sentido o inciso o art. 22, Carta de Declaração de Direitos Humanos
[4] §4 - Lei Hessiana de Proteção de Dados (HDSG) - 1970
[5] Ver nesse sentido, o artigo científico de J. Lee Riccardi em 1983, que discorre sobre o contexto histórico e conteúdo da BDSG.

pessoais na unidade de armazenamento quando não houvesse precisão adequada sobre as informações e quando elas cumprissem a finalidade às quais foram originalmente coletadas,[6] uma aplicação do atual princípio da finalidade previsto no inciso I, art. 6º da LGPD.

Após este período, a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais foi sediada em 1981, um tratado que vinculava os seus signatários a obrigações legais aplicáveis a ambos os setores público e privado, pretendendo a proteção aos titulares e a regulação das transferências internacionais de dados. Começava a ser desenvolvida a ideia de que os dados pessoais não possuíam nacionalidade,[7] e da mesma forma que os direitos da personalidade eram universais, construiu-se a noção de que a proteção de dados pessoais também deveria ser, e em função disso, dois anos depois, o Tribunal Constitucional Alemão estabeleceu que a autodeterminação informativa havia se tornado um direito fundamental protegido pela Constituição Federal, uma tendência de constitucionalismo que seria observada nos anos seguintes em países como Espanha e Portugal.[8]

Verifica-se que as discussões alemãs sobre os direitos da personalidade acarretaram num debate maior de escala internacional sobre a autodeterminação informativa, o que se comprova ao fazer a leitura da Convenção 108 de 1981, com destaque ao seguinte artigo:

> Art. 8 - Salvaguardas adicionais para o titular dos dados. Qualquer pessoa deve ter o direito a: (a) tomar ciência da existência de um arquivo automatizado de dado pessoal, as suas principais finalidades, bem como a identidade e residência habitual ou local principal de negócios do controlador de o arquivo; (b) obter, a intervalos razoáveis e sem atraso indevido ou cobrança, a confirmação de se os dados pessoais que lhe são relativos estão sendo armazenados no arquivo de dados automatizados, também tendo direito ao esclarecimento sobre estes dados de forma facilitada; (c) obter, se for o caso, a retificação ou eliminação dos dados se foram processados de forma contrária às determinações legais, aplicando os efeitos dos princípios básicos previstos nos artigos 5 e 6 desta Convenção; (d) dispor de um recurso se um pedido de confirmação ou, conforme o caso, de esclarecimentos, retificação ou eliminação, como referidos nos parágrafos b e c deste artigo, não forem atendidos. (Tradução nossa)

Reitera-se que este documento internacional diz respeito ao tratamento automatizado de dados, logo, ao constatar a nítida intenção de dar garantias ao titular – inclusive legitimando o emprego de meios judiciais, como se infere a partir do item "d" –, fica evidente que os dados pessoais passariam a assumir uma definição legal intrinsicamente vinculada à liberdade de seus

[6] RICCARDI, p. 259, 1983

[7] Esta afirmação deriva do entendimento jurídico de que não é relevante a nacionalidade do titular para a proteção de seus dados pessoais. Isso se dá em razão do art. 3º, que dispõe em seus incisos que a LGPD se aplica desde que: (i) a operação de tratamento de dados seja realizada em território nacional, (ii) os dados pessoas tenham sido coletados no Brasil ou (iii) que se vise a oferta de bens ou serviços a indivíduos localizados no país. Nota-se que em momento algum a lei cita como requisito o titular ser brasileiro, pois a economia digital dificilmente se restringe às fronteiras geopolíticas, e nesse sentido, torna-se o dever de cada um dos Estados proteger a privacidade das pessoas naturais em seu país, mesmo que transitoriamente.

[8] DONEDA, p. 97, 2011

titulares, o que comprova a reciprocidade entre o tratamento de dados e a autodeterminação informativa, como se, para que esta tecnologia fosse aplicável no presente e no futuro, os cidadãos necessitassem de direitos e garantias que permitissem a compreensão do fenômeno tecnológico centrado nas suas informações pessoais, de modo que fosse possível exercer a autodeterminação ativamente como titulares de dados e de direitos inerentes ao ser humano.

Atualmente, no cenário nacional, existe um esforço da ANPD para que o cidadão compreenda os riscos do tratamento impróprio ou ilegal de seus dados pessoais, com efeitos que variam desde prejuízos econômicos a restrição de liberdades fundamentais. A autarquia vem incentivando a precaução por meio de medidas que transitam desde o âmbito doméstico, como a criação de *backups* e ativação de criptografia em discos e mídias externas; até o externo, com as tentativas de contato direto com as lojas e empresas que coletam os dados pessoais, ou ainda, no caso de identificação de atividade ilícita, a petição ao Poder Judiciário ou à autoridade nacional.[9]

No entanto, qual é a efetividade de incentivar essas medidas atualmente, compreendendo os avanços na tecnologia do tratamento automatizado de dados e o consequente aumento de sua complexidade?

1.2 O PROBLEMA ATUAL DA AUTODETERMINAÇÃO INFORMATIVA

De acordo com a narrativa histórica, o poder público perdeu a exclusividade da tecnologia de tratamento de dados, pois o fim do século XX trouxe os computadores pessoais e outros equipamentos que permitiram a exploração do tratamento de dados pelo âmbito privado com a finalidade econômica.[10] Em vista disso, para estudiosos do vínculo entre tecnologia e direito, o que está em pauta nas discussões jurídicas não é mais a privacidade no âmbito individual, como originalmente se intentava com a autodeterminação informativa, mas o poderio econômico e a capacidade de influência das empresas sobre as massas a partir da coleta dos dados pessoais de um contingente enorme de pessoas, informações dos mais variados tipos que são adquiridas a partir de contratos de adesão cuja aceitação é muitas vezes inevitável.

Shoshana Zuboff discute esse tema em sua obra "A Era do Capitalismo de Vigilância", que reflete uma faceta infeliz da tecnologia de tratamento automatizado de dados. Ela dá o exemplo de um projeto denominado "*Aware Home*", que surgiu na Georgia Tech no ano de 2000. O trabalho visava entender o vínculo existente entre o indivíduo e o seu lar, usufruindo

[9] Todos esses exemplos fazem alusão direta ao conteúdo gratuito disponibilizado pela ANPD. Para mais detalhes, acessar o Guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor em parceria com a ANPD e a SENACON, disponibilizado nas referências bibliográficas.
[10] MANTELERO, p. 336, 2022

de equipamentos e sensores, a fim de produzir um novo conhecimento empírico voltado ao lado psíquico e emocional das pessoas, iniciando um novo sistema de conhecimento, cujos dados obtidos seriam de propriedade total dos moradores, que poderiam dispor de parte dessas análises íntimas para uma melhoria no serviço e consequentemente na qualidade vida.

No entanto, alguns anos depois, a tecnologia do "*smart home*" começou a ser explorada pelo Google em associação com outras empresas, que apresentaram um produto superior em funções e rentabilidade em relação ao antigo Lar Consciente. Todavia, este novo projeto já não partilhava dos mesmos princípios que seu antecessor. Nesse sentido, Zuboff explana:

> Com um Wi-Fi habilitado e conectado, os intricados e personalizados arquivos de dados do termostato são enviados aos servidores do Google. Cada termostato vem com uma "política de privacidade", um "contrato de termos de serviço" e um "contrato de licença para o usuário final". Esses documentos revelam consequências opressivas para a privacidade e a segurança, nas quais informações sensíveis do indivíduo e da casa são compartilhadas com outros dispositivos inteligentes, departamentos não identificados de empresas e terceiros, para propósitos de análise preditiva e vendas a outras partes não especificadas. A empresa proprietária do Nest assume pouca responsabilidade pela segurança da informação que coleta e nenhuma pela maneira como as demais companhias no seu ecossistema farão uso desses dados. [...] **Caso o cliente se recuse a concordar com as estipulações da Nest Labs, os termos de serviço indicam que a funcionalidade e a segurança do termostato ficarão profundamente comprometidas**, não mais respaldadas pelas necessárias atualizações destinadas a garantir sua confiabilidade e segurança. As consequências podem variar desde canos congelados e falhas nos alarmes de fumaça a um sistema doméstico interno muito suscetível de ser hackeado. (ZUBOFF, 2019, p.21-22)

Este caso reflete um problema contemporâneo no tratamento automatizado de dados. É a manifestação de um poder coercitivo advindo do sacrifício da privacidade em troca da manutenção de outros direitos fundamentais, como à segurança,[11] de modo que é impossível exercer a autodeterminação informativa realisticamente em circunstâncias nas quais a negativa do consentimento pode resultar na privação de necessidades básicas para a residência, como no caso citado pela autora, ou no impedimento de acesso à informação, como ocorre mais comumente em sites e serviços de internet que exigem o consentimento para que funcionem.

Portanto, Zuboff estabelece que a permissão do titular é sempre uma faca de dois gumes. Isso se dá em razão da própria natureza dessa tecnologia, que trabalha a partir do compartilhamento e coleta de uma quantidade imensurável de dados pessoais para aprimorar os produtos e serviços, mas que busca primordialmente aprimorar a "inteligência da máquina". Nesse sentido, as informações pessoais destinadas a esse processo são classificadas como *superávit comportamental*, a matéria-prima para criar tecnologias cada vez mais aptas a antecipar os comportamentos, pensamentos e desejos dos indivíduos, as quais são comercializadas no que Zuboff chama de "mercados de comportamentos futuros".

[11] Art. 5º, *caput*, Constituição da República Federativa do Brasil de 1988

Pode-se interpretar que a autodeterminação informativa deixou de ser uma opção viável ao indivíduo em razão da inevitabilidade do consentimento. Em paralelo, outro problema que dificulta o exercício desse direito deriva de dois fatores de complexidade: contratual e técnica.

Está claro que na maioria dos casos não há uma relação bilateral entre o controlador e o titular de dados, e sim uma rede de intermediações com um conjunto de controladores que realizam o tratamento de dados a partir de mecanismos que acessam as informações dos dispositivos utilizados, como I.P. e GPS; ou que inferem padrões de movimentação, emoção e de outras naturezas que o indivíduo nem sequer tem a compreensão.[12]

O Instagram é um dos casos em que esta multilateralidade contratual entra em pauta, pois, entendendo que é um aplicativo de uso gratuito para o acesso a informações e promoção de conteúdo, uma de suas principais atividades lucrativas parte do compartilhamento de dados a terceiros para aproximar o potencial consumidor de vendedores desconhecidos. Todos esses dados são adquiridos a partir de um monitoramento contínuo da atividade do usuário e dos conteúdos que mais visualiza, com o intuito de construir um perfil para o mercado.[13]

Com os anúncios personalizados, a experiência do consumidor é mais conectada aos assuntos e produtos que lhe interessam, porém, o problema maior em relação a essa prática é novamente a inafastabilidade, pois a princípio o aplicativo não deixa essa relação de compartilhamento de dados suficientemente clara aos seus usuários, que se evidencia apenas com a aparição de anúncios e postagens de interesse dentro e fora da plataforma. E mesmo buscando gerenciar os limites do tratamento de dados, o Instagram expõe que o usuário pode afastar os anúncios de determinados vendedores, mas não possui ferramentas que facultam o cessamento parcial ou completo do compartilhamento dos dados advindos da vigilância.[14]

Portanto, esta é uma circunstância em que, além de não ser nítido ao consumidor quem está realizando o tratamento de seus dados, mesmo que se tome ciência disso, é um contrato de adesão inevitável, pois a única possibilidade de evitar o compartilhamento é por meio do abandono à rede social.

Como dito antes, a coleta de dados na economia digital não ocorre unicamente via consentimento, uma vez que os dados pessoais podem ser inferidos a partir do monitoramento nos dispositivos eletrônicos por meio de uma tecnologia de predição comportamental, como ocorre com o Instagram. Porém, foi aludida apenas a dimensão contratual deste problema, que

[12] ZANATTA, p. 202, 2019
[13] pCLOUD. *The most invasive apps: which apps are sharing your personal data?* 2021
[14] Todas estas informações estão disponíveis na Política de Privacidade do aplicativo, sendo possível inclusive requisitar a portabilidade dos dados pessoais do usuário, que comprovam o tratamento de dados relacionados ao histórico de atividades em detalhe; usuários que mantém contato e a sua possível origem no próprio dispositivo móvel; conteúdos que pesquisa; fotos, vídeos e áudios encaminhados etc.

reflete o questionamento de “quem são as figuras responsáveis pelo tratamento”, enquanto prevalece também uma dimensão técnica que dificulta a autodeterminação informativa, pois obscurece as respostas às seguintes perguntas: “Quais informações pessoais estão sendo coletadas? Como estão sendo coletadas?”

Elaborando, entre as décadas de 80 e 90, a complexidade do tratamento de dados ainda era relativamente limitada, então os titulares tinham a possibilidade de consentir e entender a coleta de dados e as suas finalidades, como a criação de perfis e o oferecimento de serviços e produtos customizados.[15] Porém, isso mudou com a chegada das análises com *Big Data*, porque volumes enormes de dados de todas as variedades possibilitaram correlacionar informações de predição, a fim de adquirir mais conhecimento sobre indivíduos, as suas características e gostos, inserindo-os em um público-alvo específico. Nenhum desses pontos era compatível com o consentimento inicialmente obtido do titular.

De certa forma, o enquadramento em perfis não é uma novidade, porém, o *Big Data* permitiu que essa técnica se tornasse quase imperceptível: o consentimento se desvinculou da autodeterminação informativa, e dados pessoais de origens e variedades distintas passaram a ser tratados por meio dessa rede complexa.

Além disso, Shoshana Zuboff encontra na ausência de precedentes das tecnologias de tratamento automatizado de dados, uma maneira infelizmente ideal para explorar a privacidade humana, uma vez que a inovação tecnológica já é de entendimento restrito até que se torne senso comum, porém, somado a este fator, a própria natureza do atual tratamento de dados evidencia que o cidadão comum não é o cliente direto, mas a fonte de matéria-prima para o desenvolvimento de um produto que proporciona a manipulação das pessoas. Portanto, é plausível economicamente a falta de interesse desse mercado no entendimento e integração dos titulares ao tratamento de seus dados, pois não é uma estratégia de negócios voltada a eles, e sim a terceiros. Nesse sentido, argumenta a autora:

> As perguntas dignas de nota aqui dizem respeito aos fatos de que nossa vida é, em primeiro lugar, reduzida a dados comportamentais; de que a ignorância é uma condição dessa ubíqua redução; de que os direitos de escolha desaparecem antes que o indivíduo nem sequer tenha ciência de que existe uma decisão a tomar; de que há consequências para a diminuição de direitos que ainda não conseguimos ver tampouco prever; que não há nenhuma saída, nenhuma voz e nenhuma lealdade, apenas impotência, resignação e insensibilidade psicológica; e que a encriptação é a única ação positiva que resta para discutir quando nos sentamos em torno da mesa de jantar e casualmente refletimos sobre como nos esconder das forças que se escondem de nós (ZUBOFF, p. 122, 2019)

[15] MANTELERO, p. 337, 2022

1.3 A TUTELA COLETIVA DA PROTEÇÃO DE DADOS

Frente à ascensão de obstáculos à autodeterminação informativa, cumulada com o reconhecimento da proteção de dados como um direito fundamental, a sua tutela coletiva nasceu como uma forma de zelar pelo interesse público, que se fortaleceu por meio da atuação de entidades públicas e privadas.

Para melhor entender quais características da tutela coletiva estão em aplicação, é essencial notar primeiramente a existência de dois modelos de regulação do tratamento de dados ao qual o Brasil pode ter feito alguma alusão: (i) o modelo estadunidense, que vincula elementos de autorregulação no âmbito privado à fiscalização de autoridades, mas com pouco fulcro em normas concretas, um método similarmente empregado na Alemanha;[16] e (ii) o modelo dominante na Europa, centrado na constitucionalização de proteção de dados e em seu reconhecimento como um direito fundamental, visando a rígida adequação do tratamento de dados à lei através da intensa fiscalização de autoridades delegadas a esta competência.

Esta divisão foi trabalhada pela doutora em direito Mónica Arenas Ramiro, que investigou a proteção de dados na América Latina e notou que os países Ibero-Americanos mantêm um vínculo intenso com a Europa: (i) discutindo a privacidade em fóruns internacionais, como na Rede Ibero-americana de Proteção de Dados;[17] (ii) integrando a Convenção de Estrasburgo de 1981 como signatários, no caso do Uruguai e da Argentina, em 2013 e 2019; e (iii) assumindo características do modelo europeu, como a constitucionalização da proteção de dados, no caso do Brasil, Chile, Colômbia, Equador, México e República Dominicana.

Salientados estes indicadores, é possível olhar para a LGPD sob outra ótica ao compará-la ao GDPR, pois a legislação brasileira instituiu uma autoridade nacional; fez a sua fundação sobre princípios abstratos; e aplicou regras e mecanismos de aplicação no caso concreto, como o Relatório de Impacto à Privacidade (art. 36, § 2º)[18].

O doutor em direito Maximilian Von Grafenstein explica que a forma como o regulamento europeu foi estruturado visa a efetivação de um modelo de co-regulação da proteção de dados, uma alternativa que considerou a constante inovação neste meio, o qual rapidamente inutilizaria regras muito concretas. Nesse sentido, o autor conclui que o GDPR: (i) dá um enfoque evidente aos direitos gerais no artigo 5, aplicáveis a todas as operações de tratamento de dados, o que se aproxima à interpretação extensiva dos direitos da personalidade

[16] BAMBERGUER; MULLIGAN, p. 89, 2015
[17] Em 04 de outubro de 2021, a ANPD ingressou como membro da Rede Ibero-Americana de Proteção de Dados
[18] Originalmente conhecido como *Privacy Impact Assessment*, no art. 35, GDPR

no histórico alemão; (ii) e ainda, integra os agentes de tratamento e as entidades competentes à gestão dos riscos dos tratamentos de dados, por meio de uma dinâmica de responsabilização e fiscalização.

Nesse sentido, entendendo a estrutura do GDPR à qual o legislador brasileiro se espelhou, pode-se inferir que existe a intenção de assumir uma tutela coletiva da proteção de dados pessoais no país por meio da convergência entre a atuação dos setores público e privado. No entanto, apesar de aparentar uma mera reprodução, essa forma de defender direitos difusos e coletivos é imensamente favorecida pelas estruturas jurídicas já existentes no Brasil, que foram empregadas para a proteção de dados antes mesmo da vigência da LGPD, graças a um processo conhecido pelo doutor Rafael Zanatta como "revolução dos direitos difusos".

Decorrentes de vitórias ao longo dos anos, como a promulgação da Lei de Ações Civis Públicas e do Código de Defesa do Consumidor, nos anos de 1985 e 1990, uma série de transformações ocorreram no direito brasileiro visando a ampliação do acesso à justiça. Durante esse processo, segundo Zanatta, a definição dos interesses coletivos e difusos foi essencial para dar um fundamento adequado à aplicação das ações civis públicas:

> Com as reformas jurídicas iniciadas em 1981 e concluídas em 1990, firmou-se a teoria de que os **interesses coletivos** são os interesses comuns a uma coletividade de pessoas (e apenas a elas), "a partir de um vínculo jurídico definido que as congrega". Já por **interesses difusos** temos os interesses que não encontram relação-base bem definida, reduzindo-se o vínculo entre as pessoas a fatores conjunturais, como o consumo de um mesmo produto, a vivência sob determinadas condições socioeconômicas ou a sujeição a determinados empreendimentos. (ZANATTA, p. 9, 2020)

Além disso, através da legitimação para que o Ministério Público e outras entidades figurassem no polo ativo de litígios envolvendo direitos difusos (art. 5º, Lei nº 7.347/85), somada à garantia de que a defesa dos interesses e direitos dos consumidores e das vítimas poderiam ser exercidos em juízo coletivamente (art. 81, CDC), a tutela coletiva foi incentivada e começaram a ser fundadas entidades de defesa do consumidor especializadas em litígio, como o caso do IDEC (Instituto Brasileiro de Defesa do Consumidor),[19] que recebeu destaque no processo polêmico das Portas Interativas Digitais em 2018, ajuizando uma ação civil pública contra a ViaQuatro por:

> (i) violar o direito básico do usuário de serviços públicos de proteção de suas informações pessoais, (ii) descumprir parâmetros de tratamento de dados biométricos definidos na Lei Geral de Proteção de Dados Pessoais, (iii) descumprir o direito básico do consumidor de proteção contra práticas abusivas nos termos do Código de Defesa do Consumidor, (iv) configurar prática abusiva, exigindo do consumidor vantagem manifestamente excessiva, (v) violar a proibição de obrigações onerosas ("pesquisa de opinião forçada"), (vi) descumprir o direito constitucional de proteção da imagem. (ZANATTA, p. 4, 2020)

[19] ZANATTA, p. 7, 2020

Nota-se que não foram utilizados apenas fundamentos previstos na LGPD para que a ação fosse iniciada, o que reforça a ideia de que mesmo anteriormente à vigência da lei, a tutela coletiva da proteção de dados já ocorria por meio de outras garantias. Por conta disso, Zanatta entende que a cultura de proteção de dados já vem sendo desenvolvida através da proatividade dessas entidades, o que significa que os novos mecanismos da LGPD poderão auxiliar ainda mais a proteção aos direitos dos titulares no Brasil:

> Considerando (i) o quão avançado é o sistema de tutela coletiva no Brasil, (ii) a força dos Ministérios Públicos e o predomínio do uso de ACPs, (iii) a existência crescente de entidades de direitos digitais com alguma colaboração com o sistema de justiça (não somente Idec, mas também CodingRights, Artigo 19, Intervozes, InternetLab, IRIS, entre outros) e (iv) crescente percepção de que os problemas de proteção de dados pessoais são problemas de ordem coletiva, envolvendo interesses difusos, fica evidente que a tutela coletiva desempenhará um papel importante na constituição de um regime jurídico brasileiro de proteção de dados pessoais. (ZANATTA; p. 12, 2020)

1.4 UMA NOVA LEITURA DA AUTODETERMINAÇÃO INFORMATIVA

Além de todos os fatores citados que levaram a autodeterminação informativa a um campo secundário na proteção aos dados pessoais, o fato de que ela diz respeito apenas ao âmbito da administração individual do titular de dados gerou um contraste intenso com o movimento de constitucionalização e de uma proteção de dados voltada ao interesse público, pois se tornava cada vez mais evidente que o tratamento de dados traria impactos à sociedade como um todo, como frequentemente se intentavam práticas comerciais potencialmente perigosas à autonomia dos consumidores e ao poder de decisão por conta do alto teor de personalização dos serviços e produtos.[20]

Nesse sentido, argumenta-se que a autodeterminação informativa era dotada de uma perspectiva liberal, uma vez que a sua aplicação se restringiria à esfera da liberdade negativa e individual, o que não seria mais adequado de discutir no tratamento de dados, pois o tratamento de dados nem sempre decorre do consentimento do titular,[21] o que representa o fator de principal diferença entre os campos práticos da "privacidade" e da "proteção de dados", pois enquanto a primeira é um conceito que engloba a proteção de dados, mas também zela pelo direito de "ser deixado só" e de preservação da intimidade; o segundo traz um enfoque maior à proteção da vida privada enquanto há a circulação de informações pessoais, de modo a administrá-las para que a privacidade seja preservada.[22]

[20] CLIFFORD, p. 234, 2022
[21] Ver nesse sentido, o extenso rol de requisitos para o tratamento de dados no art. 7º, da LGPD
[22] LIMA, p. 60, 2019

A divisão entre a tutela individual e coletiva da proteção de dados existe em razão dos desafios à autodeterminação informativa decorrentes da inevitabilidade atual do tratamento de dados, sendo impossível viver sob as normas de um Estado, por exemplo, sem que haja a coleta de informações pessoais para o usufruto de serviços públicos.

Portanto, existe um espaço para autodeterminação informativa nos dias de hoje? É certo que a privacidade desempenha um papel essencial na sociedade, pois não se trata de uma mera preferência pessoal, e sim de um pressuposto de operação da estrutura social, como alega Robert Merton em sua obra *Social Theory and Social Structure*. Deste modo, entendendo a autodeterminação informativa como uma ferramenta de gestão da privacidade, é possível utilizá-la para zelar por um interesse maior?

Este trabalho se posiciona a favor de uma resposta positiva, pois argumenta-se que qualquer ato em defesa à privacidade é também um ato em defesa à democracia. Vejamos um caso polêmico que impactou a vida das pessoas em escala global ao influenciar as eleições estadunidenses de 2016, entre Donald Trump e Hillary Clinton. Através do aplicativo *This is Your Digital Life*, que calculou as predileções de personalidade de seus usuários e, sem o consentimento deles, compartilhou tais dados com a instituição inglesa de análise de dados Cambridge Analytica, esta última empresa recebeu o apoio e usufruiu do Facebook como canal para direcionar postagens de cunho ideológico a usuários que preenchiam requisitos de personalidade específicos, visando a conversão de milhões de eleitores ao candidato que posteriormente foi vitorioso.[23]

A casuística foi destrinchada em inúmeros debates, mas um ponto de reflexão importante é a origem da investigação que levou à descoberta do escândalo: a preocupação de David Carroll, um cidadão comum, pelo tratamento de seus dados pessoais na posse de Cambridge Analytica.[24] Uma atitude por parte de um titular de dados trouxe mudanças favoráveis ao interesse público, provocando inclusive a elevação do *compliance* dos termos de serviço e política de privacidade do Facebook em relação ao GDPR, e consequentemente fortalecendo o princípio da transparência nas práticas comerciais.[25]

É evidente que a autodeterminação informativa não deixa de ser uma pretensão individualista e fortemente liberal, considerando o interesse pela administração da privacidade para que o tratamento de dados produza efeitos compatíveis ao desenvolvimento pessoal de acordo com as influências sociais desejadas, fazendo com que a individualidade e a liberdade

[23] SCHROEPFER, 2018
[24] Privacidade Hackeada, Netflix, 2019
[25] LIMA, p. 62, 2019

de expressão efetivamente floresçam.[26] Porém, mesmo sendo um pressuposto egoísta, é certo que o tratamento de dados atualmente influencia a sociedade como um todo. Portanto, de forma similar ao ocorrido com Carroll, às vezes a pretensão de solucionar um problema individual referente à privacidade pode auxiliar outros titulares que se encontram em posições similares, um cenário que se verificaria no caso brasileiro em razão: (i) do princípio de publicidade das decisões judiciais;[27] e (ii) do poder incumbido à autoridade nacional de tornar públicas as infrações cometidas por agentes de tratamento após a devida apuração.[28]

Nesse sentido, a autodeterminação informativa nunca irá sobrepor a tutela coletiva dos dados pessoais, uma vez que o titular possui menos recursos investigativos, mas ainda sim dispõe da legitimidade para reivindicar os seus dados pessoais e perseguir o direito ao livre desenvolvimento da personalidade, no que tange à subjetividade humana.

Logo, pode-se pensar em uma complementariedade da autodeterminação informativa na proteção aos direitos coletivos. A União Europeia constituiu as primeiras legislações e tratados sobre proteção de dados da história; apresenta um sistema regulatório visto como referência global, e mesmo assim não preveniu o escândalo de compartilhamento ilícito de dados em 2016.

O que se conclui desses indícios é a baixa probabilidade de que as entidades públicas e privadas – mesmo com um desenvolvimento institucional avançado da tutela coletiva de direitos no Brasil – consigam neutralizar todas as atividades ilícitas de tratamento de dados, principalmente ao considerar que o Brasil não condiciona a abertura de bancos de dados ao registro público, diferentemente de como ocorre em seus vizinhos que apresentam graus de proteção de dados equiparáveis à União Europeia, a Argentina e o Uruguai.[29]

Além disso, existe uma linha tênue entre ilicitude e imoralidade no tratamento de dados, já que a própria tecnologia de predição de comportamentos pode influenciar o livre desenvolvimento da personalidade e a liberdade de pensamento e expressão aos quais todo cidadão deve ter direito, sendo plausível enxergar a autodeterminação informativa como um instrumento subsidiário quando nenhuma norma de tratamento de dados é expressamente infringida, já que o uso de informações pessoais na veiculação de mensagens políticas, por exemplo, pode representar um atentado à integridade da democracia e do processo eleitoral, porque essas mensagens não apenas polarizam a população, mas também, como um resultado

[26] COHEN, 2000
[27] Ver nesse sentido o art. 11, caput, Novo Código de Processo Civil.
[28] Ver nesse sentido o inciso IV, art. 52, LGPD
[29] A Argentina foi reconhecida pela União Europeia em 2003, mediante a decisão nº 2003/490/EC; e o Uruguai em 2012, mediante a decisão nº 2012/484/EU

do tratamento, discriminam eleitores ao direcionar ideologias com alto teor de aceitação a pessoas que se encaixam em critérios ligados a características da personalidade.[30]

É um cenário que se agrava nas eleições de 2022, com a utilização de marketing digital por candidatos políticos em campanhas milionárias para encontrar as pessoas certas e falar aquilo que a predição de comportamentos sabe que há o interesse em ouvir, como a peça publicitária de Jair Bolsonaro às "tias do Zap" no Google, direcionada somente a mulheres com idade igual ou superior a 35 anos. As campanhas de Bolsonaro e de Lula têm tido peças removidas por infringir as políticas da plataforma ou a pedido do TSE (Tribunal Superior Eleitoral),[31] o que significa que há uma preocupação quanto aos impactos dessas condutas à democracia brasileira, entretanto, não é possível neutralizar todos os atentados à privacidade por meio da tutela coletiva, pois não há certeza quanto à ilegalidade dos mesmos.

1.5 A DEMOCRATIZAÇÃO DA PROTEÇÃO DE DADOS NO BRASIL

A construção do direito à privacidade e à proteção de dados em uma cultura jurídica é um processo *sui generis*, pois existe um contexto histórico e social específico que salienta a necessidade de proteger a vida privada, como foi o caso da lei federal de proteção de dados francesa (*Informatique et Libertées*) em 1978, que surgiu em resposta a um programa governamental de coleta de dados que causou um levante popular, pois o "SAFARI" atuaria como um banco de dados estatal e centralizado que permitiria às agências públicas identificar cada um dos cidadãos individualmente.[32]

Não obstante, é possível identificar um padrão entre os países que legislam sobre proteção de dados e hoje são reconhecidos pelo elevado grau de segurança jurídica: as legislações inicialmente protegiam o cidadão das tecnologias de coleta e tratamento, e atualmente buscam maneiras mais eficientes para integrá-los, mesmo com a hegemonia da tutela coletiva na proteção aos dados pessoais.

Em outras palavras, a participação do titular no tratamento de seus dados foi incrementada ao longo dos anos numa tentativa de conscientizar os cidadãos sobre a importância da privacidade, que aliás, representa uma função de autoridades nacionais e internacionais delegadas à fiscalização do tratamento de dados, como dispõe: (i) a LGPD em seu inciso VI, art. 55-J, quanto às funções da autoridade brasileira; (ii) o BDSG na Seção 14, parágrafo 1, item 2, quanto às tarefas adicionais da autoridade federal alemã; (iii) a lei de

[30] REGAN, p. 165, 2019
[31] CNN Brasil, 2022
[32] BAMBERGUER, p. 54, 2015

proteção de dados uruguaia na alínea "a", art. 34, quanto às funções e atribuições da autoridade uruguaia, entre outras.

Deste modo, somando o papel da ANPD à posição da autodeterminação informativa como um fundamento da proteção de dados no Brasil, é prudente verificar como a legislação brasileira busca sanar as dificuldades atuais da tutela individual já trabalhadas nesse artigo, a fim de fornecer instrumentos verdadeiramente capazes de serem utilizados pelos titulares para a proteção contra as constantes ameaças à subjetividade humana.

Inicialmente, destaca-se que a LGPD visa sanar a barreira da complexidade técnica ao promover a gestão e acesso facilitados dos titulares aos seus dados pessoais. O princípio de livre acesso, da qualidade dos dados e da transparência são regras abstratas às quais os controladores devem se atentar ao coordenar o tratamento de dados, para que, quando exercido o direito de informação previsto em uma série de dispositivos da lei, seja possível fornecer os esclarecimentos de forma clara, adequada, ostensiva e dentro de um prazo de 15 dias[33] sobre questões como a finalidade específica do tratamento; a forma e duração; os direitos do titular, etc.[34]

A LGPD empodera o titular além do mero acesso à informação, tornando-o uma figura de intervenção no tratamento, capaz de retificar dados incompletos, inexatos ou desatualizados;[35] pedir a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei;[36] revogar, alterar e se informar sobre as consequências da negativa do consentimento na prestação do serviço;[37] solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, como as decisões destinadas à definição de perfis pessoais, profissionais, de consumo e de créditos ou aspectos da personalidade;[38] requisitar a portabilidade dos dados, uma inovação que promete ampliar a força do titular ao viabilizar a manipulação e direcionamento de seus dados no mercado;[39] entre outros.

A questão principal que efetivamente democratiza a integração do titular é o fato de que todos esses direitos devem ser concedidos de forma gratuita,[40] podendo qualquer obscuridade ser indagada diretamente aos agentes de tratamento e, se não for sanada, é igualmente possível

[33] Ver nesse sentido o inciso II, Art. 19, LGPD
[34] Ver nesse sentido o art. 9º, LGPD
[35] Ver nesse sentido o inciso III, art. 18, LGPD
[36] Ver nesse sentido o inciso IV, art. 18, LGPD
[37] Ver nesse sentido o inciso VI, art. 18, LGPD
[38] Ver nesse sentido o art. 20, LGPD
[39] Este tema é melhor desenvolvido no trabalho de "Direitos básicos dos titulares de dados pessoais" da doutora em direito Ana Frazão
[40] Ver nesse sentido o § 5º, art. 18, LGPD

recorrer à ANPD,[41] aos organismos de defesa de consumidor[42] e ao Poder Judiciário[43] por meio de petições. Aliás, tendo ingressado em juízo, cabe imediatamente ao controlador comprovar a obtenção do consentimento de acordo com a lei;[44] e no processo civil, pode ser determinada a inversão do ônus da prova a favor do titular de dados quando as suas alegações forem verossímeis e quando houver hipossuficiência para fins de produção de prova ou quando ela for excessivamente onerosa.[45]

O que se extrai de tantos direitos distintos e circunstanciais é uma proteção formal e elevada ao titular, pois, de forma idêntica às relações consumeristas, são abordadas várias maneiras de exercer a tutela individual, de modo a sanar o desequilíbrio de recursos entre as partes. Por conseguinte, a LGPD busca assegurar primeiramente a conciliação, apresentando uma poderosa base de direitos que força os agentes de tratamento a se adequarem à lei e a repensarem os seus contratos e condutas, de modo que se mostra necessário atender às requisições dos consumidores independentemente da complexidade técnica do tratamento em pauta.

Então, verificada a abstenção dos controladores nas medidas e esclarecimentos obrigatórios, as entidades públicas nacionais e os tribunais assumem um papel de repressão, forçando a adoção de procedimentos adequados[46] e submetendo os responsáveis a sanções administrativas previstas na LGPD, podendo inclusive haver desdobramentos nas esferas criminal e civil, de acordo com a falta.,[47] o que representa o suporte institucional fornecido ao titular, constituindo um arranjo de direitos interdependentes ao qual os controladores devem respeitar.

Além disso, a LGPD também se preocupa em sanar a complexidade contratual ao definir em seu inciso VII, art. 18, o direito à "informação adequada das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados". Através desta norma, em tese, não seria mais possível o livre compartilhamento por uma rede complexa sem que o titular estivesse à par de quem são os seus membros, principalmente entendendo que o fornecimento de dados pessoais a terceiros sem o consentimento livre, expresso e informado foi vedado desde a vigência do Marco Civil da Internet, em 2014.[48]

[41] Ver nesse sentido o § 1º, art. 18, LGPD
[42] Ver nesse sentido o § 8º, art. 18, LGPD
[43] Ver nesse sentido o art. 22, LGPD
[44] Ver nesse sentido o § 2º, Art. 8º, LGPD
[45] Ver nesse sentido o § 2º, Art. 42, LGPD
[46] Ver nesse sentido o § 1º, art. 46, LGPD
[47] Ver nesse sentido o inciso I, § 1º, art. 42, LGPD
[48] Ver nesse sentido o inciso VII, Art. 7º, MCI

A partir desses direitos, o último sendo reiterado pelo art. 7º da LGPD, a estrutura jurídica brasileira fixa um entendimento de que o compartilhamento de dados deve ser feito com atenção aos meios necessários e adequados para atingir a finalidade do tratamento,[49] reforçando a importância de que o titular tenha pleno conhecimento não apenas de todos os controladores envolvidos no tratamento de seus dados, como também da extensão do referido compartilhamento e dos dados envolvidos, a fim de assegurar que nenhuma etapa do processamento de suas informações fuja da finalidade à qual o titular originalmente consentiu.[50]

Por fim, outro fator legal que contribui com a autodeterminação informativa no caso concreto advém especialmente do modelo de co-regulação herdado da estrutura do regulamento europeu, ao qual se promove uma maior eficácia na fiscalização ao submeter os agentes de tratamento a um sistema de riscos e responsabilidades, impondo aos fornecedores grande parte das condutas de prevenção de danos com base nas suas próprias atividades, devendo comprovar por meio do Relatório de Impacto à Proteção de Dados, que há a noção dos riscos do tratamento e que existe um planejamento sobre os procedimentos adotados no caso de concretização de cenários indesejados.[51]

Logo, se comprovada que a negligência dos riscos resultou em incidentes de segurança, violações ao sigilo ou à finalidade do tratamento, ocorre a responsabilização de todos os envolvidos no tratamento de acordo com a culpa, o que certamente se mostra como um fator coercitivo para que o compartilhamento de dados seja realizado apenas quando necessário, resultando possivelmente em uma simplificação ao problema da multilateralidade contratual, pois quanto mais controladores envolvidos, maior é o risco assumido.

CONSIDERAÇÕES FINAIS

A despeito de todas as dificuldades criadas à autodeterminação informativa com o desenvolvimento do mercado de circulação de dados pessoais, é evidente a sua relevância atual tanto para a tutela individual, como para um instrumento subsidiário e complementar à tutela coletiva. A origem desse direito foi o primeiro passo para a criação e desenvolvimento das normas sobre proteção de dados ao longo dos anos, pois todas tiveram como objeto central a proteção à privacidade, entendendo sempre a conscientização e o fornecimento de instrumentos de proteção como elementos essenciais para que a economia digital progredisse, pois eram

[49] Ver nesse sentido os incisos II e III, art. 6º, LGPD
[50] FRAZÃO, p, 45, 2019
[51] Ver nesse sentido o inciso XVII, art. 5º, LGPD

aprimoradas tecnologias cada vez mais aptas a antecipar comportamentos e pensamentos através da dedução de informações pessoais.

Em razão dos riscos aos direitos da personalidade, tanto sob a ótica individual quanto social, ficou claro que a proteção de dados havia se tornado uma matéria de interesse público, pois populações inteiras seriam afetadas com as novas possibilidades do tratamento de dados, como se deu nas eleições estadunidenses do ano de 2016. A tutela coletiva assume relevância crescente, mas a tutela individual reflete os mesmos interesses ao gerar consequências que conscientizam as demais pessoas sobre uma situação problemática.

Com a LGPD, o Brasil investiu significativamente nos instrumentos de tutela individual, demonstrando que há uma nítida intenção democratizar a proteção de dados por meio das relações de tratamento de dados e das soluções a questões que dificultam o exercício da autodeterminação informativa. A resposta parece estar sempre na conscientização do titular, pois o zelo à privacidade é uma das principais formas de administrar corretamente a inserção de uma tecnologia de predição de comportamentos na sociedade, sem que se concretize um cenário distópico de alienação total dos cidadãos.

Nos próximos anos, será avaliado como o Estado brasileiro irá aplicar essas normas sem causar um estranhamento ao mercado diante de tantas exigências legais surgindo simultaneamente. A LGPD apresenta normas sólidas e compatíveis ao sistema jurídico brasileiro, como a tutela coletiva da privacidade, e o próximo passo deverá ser um processo de familiarização dos titulares e dos agentes de tratamento aos seus deveres e direitos, a fim de consolidar uma economia digital aliada à segurança jurídica.

REFERÊNCIAS BIBLIOGRÁFICAS

ALEMANHA, Hessets Datenshutzgesets. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit. 1970.

ALEMANHA, Bundesdatenschutzgesets. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit. 1977.

BAMBERGER K. A., MULLIGAN, Deirdre K. Privacy on the ground: driving corporate behavior in the United States and Europe. 2015. MIT PRESS. E-book.

BRASIL. Código de Processo Civil. Lei nº 13.105, de 16 de março de 2015. Brasília, DF: Presidência da República [2015]. República Federativa do Brasil. 2015. Brasília: Planalto.

BRASIL. Constituição da República Federativa do Brasil. 1988. Brasília: Planalto.

BRASIL. Guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor. Brasília, DF: Presidência da República, 2021.

BRASIL. Emenda Constitucional nº 115. 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. 10 de fevereiro de 2022. Brasília, Planalto.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Lei nº 13.709, de 14 de agosto de 2018. Brasília, DF: Presidência da República [2018]. República Federativa do Brasil.

BRASIL. Marco Civil da Internet (MCI). Lei nº 12.965, de 23 de abril de 2014. Brasília, DF: Presidência da República [2014]. República Federativa do Brasil. Disponível em:

COHEN J. E. Examined Lives: Informational Privacy and the Subject as Object. Stanford Law Review 52(5)1377. 2000. E-book.

CLIFFORD, D. Data protection and consumer protection: The empowerment of the citizen-consumer. Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the "state of the art" of data protection-by-design. In FUSTER, G. G.; BRAKEL, V. R.; HERT, P. d. Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing, 1st Ed. Cheltenham: Edward Elgar Publishing. 2019. E-book.

CONSELHO DA EUROPA. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg: 1981. Disponível em: https://www.coe.int/en/web/conventions/fulllist/-/conventions/treaty/108/signatures.

DIMITROV, I. The most invasive apps: which apps are sharing your personal data? pCloud. 05 de março de 2021. Disponível em: https://www.pcloud.com/pt/invasive-apps

FRAZÃO, A. Direitos básicos dos titulares de dados pessoais. Revista do Advogado. AASP. nº 144. p. 33-46. 2019. Disponível em: https://www.aasp.org.br/revistas/revista-no-144/

DONEDA, D. C. M. A Proteção dos Dados Pessoais como um Direito Fundamental. Espaço Jurídico. nº 2. p. 91-108. 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315

GRAFENSTEIN, M. v. Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the "state of the art" of data protection-by-design. In FUSTER, G. G.; BRAKEL, V. R.; HERT, P. d. Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing, 1st Ed. Cheltenham: Edward Elgar Publishing. 2019. E-book.

INSTAGRAM. Política de Privacidade. 2022.

INTERSOFT CONSULTING. General Data Protection Regulation. União Europeia. 2016. Disponível em: https://gdpr-info.eu/

LIMA, C. R. P. Consentimento inequívoco versus expresso: o que muda com a LGPD? Revista do Advogado. AASP. nº 144. p. 60-66. 2019. Disponível em: https://www.aasp.org.br/revistas/revista-no-144/

MANTELERO, A. Big Data and data protection. In FUSTER, G. G.; BRAKEL, V. R.; HERT, P. d. Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing, 1st Ed. Cheltenham: Edward Elgar Publishing. 2019. E-book.

MENDES, Laura S. F. Autodeterminação informativa: a história de um conceito. Rev. de Ciências Jurídicas Pensar, v. 25, n. 4, 2020. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828/pdf>. Acesso em 22 abr 2021.

NAKAGAWA, F. Bolsonaro triplica verba e ultrapassa Lula em gasto com publicidade no Google. CNN Brasil. 21 de outubro de 2022. Disponível em: https://www.cnnbrasil.com.br/business/bolsonaro-triplica-verba-e-ultrapassa-lula-em-gasto-com-publicidade-no-google/

NETFLIX. Privacidade Hackeada. Direção de Karim Amer e Jehane Noujaim. Black Rock City: Netflix, 2019. 110 min

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos, 1948.

RAMIRO, M. A. Data Protection in Latin America. In FUSTER, G. G.; BRAKEL, V. R.; HERT, P. d. Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing, 1st Ed. Cheltenham: Edward Elgar Publishing. 2019. E-book.

REGAN, P. M. Social values and privacy law and policy. In FUSTER, G. G.; BRAKEL, V. R.; HERT, P. d. Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing, 1st Ed. Cheltenham: Edward Elgar Publishing. 2019. E-book.

RICCARDI, J. L. The German Federal Data Protection Act of 1977: Protecting the Right to Privacy? Int'l & Comp. L. Rev. Boston. v. 6. p. 243-271. 1983. Disponível em: http://lawdigitalcommons.bc.edu/iclr/vol6/iss1/8

SCHROEPFER, Mike. An update on our plans to restrict data access on Facebook. Facebook Newsroom, 4 abr. 2018. Disponível em: https://newsroom.fb.com/ news/2018/04/restricting-data-access/. Acesso em: 26 set. 2018.

ZANATTA, R. A. F. Tutela coletiva e coletivização da proteção de dados pessoais. Temas Atuais da Proteção de Dados Pessoais. 2020. p. 345-374. Editora: Revista dos Tribunais. Disponível em: https://www.researchgate.net/publication/350852661_Tutela_coletiva_e_coletivizacao_da_protecao_de_dados_pessoais

ZANATTA, R. A. F. A tutela coletiva na proteção de dados pessoais. Revista do Advogado. AASP. nº 144. p. 201-208. 2019. Disponível em: https://www.aasp.org.br/revistas/revista-no-144/

ZUBOFF, Shoshana. A Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira do poder. 1ª edição. Editora Instrínseca, 2021. E-book.