A PROTEÇÃO DE DADOS PESSOAIS ENTRE CAPITALISMO DE VIGILÂNCIA E COSMOPOLITISMO

PERSONAL DATA PROTECTION BETWEEN SURVEILLANCE CAPITALISM AND COSMOPOLITANISM

João Pedro Seefeldt Pessoa[1]
Universidade de Santa Maria

Jânia Maria Lopes Saldanha[2]
Universidade do Vale dos Sinos

Têmis Limberger[3]
Universidade do Vale dos Sinos

Resumo:
A pesquisa tem por objetivo analisar as contribuições da mirada cosmopolita na compreensão do fenômeno da mundialização da privacidade no século XXI e da necessidade de regulação do direito à proteção de dados pessoais, no contexto do capitalismo de vigilância. Percebe-se o recrudescimento das práticas de vigilância pelo Estado e pelas entidades privadas, ressignificando a privacidade e a proteção de dados pessoais nesse novo paradigma social. O marco teórico traz aportes do capitalismo de vigilância, expressão cunhada por Shoshana Zuboff, bem como do cosmopolitismo, abordado por Marta Nussbaum, Mireille Delmas-Marty, Ulrich Beck, dentre outros. Adota-se, como metodologia de abordagem, o método hermenêutico fenomenológico, o método monográfico como metodologia de procedimento, a partir da revisão bibliográfica sobre o tema. Conclui-se que o cosmopolitismo pode ser um elemento especial na discussão de um projeto global de proteção de dados pessoais, considerando a tutela do indivíduo independentemente de conformações nacionais, em razão dos desafios do capitalismo de vigilância.
Palavras-chave:
Cosmopolitismo jurídico. Privacidade. Proteção de dados pessoais. Vigilância.

Abstract:
The research aims to analyze the contributions of a cosmopolitan perspective in understanding the phenomenon of the mundialization of privacy in the 21st century and the need for regulation of the right to personal data protection within the context of surveillance capitalism. There is a perceived intensification of surveillance practices by both the State and private entities, redefining privacy and the protection of personal data in this new social paradigm. The theoretical framework incorporates insights from surveillance capitalism, a term coined by Shoshana Zuboff, as well as cosmopolitanism, discussed by Martha Nussbaum, Mireille Delmas-Marty, Ulrich Beck, among others. The research adopts a hermeneutic-phenomenological method as the approach methodology, utilizing a monographic method as the procedural, through a literature review on the subject. The study concludes

[1] Doutorando em Direito pelo Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos – UNISINOS. Mestrado em Direito pela Universidade Federal de Santa Maria – UFSM. Mestrado em Direito pela Universidad de León – UNILEON (Espanha). Graduação em Direito pela Faculdade de Direito de Santa Maria – FADISMA. Professor do Departamento de Direito da Universidade Federal de Santa Maria – UFSM e da Faculdade de Direito de Santa Maria – FADISMA..

[2] Estágio Sênior pelo Institut des Hautes Études sur la Justice (IHEJ) (França). Doutorado em Direito Público pela Universidade do Vale do Rio dos Sinos – UNISINOS. Mestrado em Integração Latino-Americana pela Universidade Federal de Santa Maria – UFSM. Graduação em Ciências Jurídicas e Sociais pela Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS. Professora do Programa de Pós-Graduação em Direito e Curso de Direito da Universidade do Vale do Rio dos Sinos – UNISINOS.

[3] Pós-Doutorado em Direito pela Universidade de Sevilha (Espanha). Doutorado em Direito pela Universidade Pompeu Fabra (Espanha). Mestrado e graduação em Direito pela Universidade Federal do Rio Grande do Sul. Professora do Programa de Pós-Graduação em Direito e Curso de Direito da Universidade do Vale do Rio dos Sinos – UNISINOS.

that cosmopolitanism can be a special element in the discussion of a global project for personal data protection, considering the safeguarding of individuals regardless of national boundaries, due to the challenges posed by surveillance capitalism.
Keywords:
Legal cosmopolitanism. Privacy. Protection of personal data. Surveillance.

1 INTRODUÇÃO

O tratamento de dados pessoais é uma realidade da sociedade em rede e desafia uma grande adaptação por parte dos titulares, agentes de tratamento e Poder Público em favor de um regime de proteção desses ativos, tendo em vista o capitalismo de vigilância, baseado num mercado digital de dados e no fluxo transfronteiriço de informações. O avanço das tecnologias de informação e comunicação pressupõe, para além de uma nova forma de relacionamento com os usuários, a adoção de leis de privacidade, normas técnicas, políticas públicas e medidas de segurança, capazes de conferir um grau maior de proteção aos titulares de dados pessoais.

Percebe-se, contudo, existir um fenômeno complexo a respeito da mundialização da privacidade e proteção de dados pessoais, num cenário de atores variados – públicos e privados -, espaços múltiplos – nacionais, regionais e internacionais -, e normas internacionais com graus variados de obrigatoriedade – *hard law e soft law* -, de modo que as correntes teóricas do cosmopolitismo jurídico podem auxiliar na criação de soluções globais. Dessa forma, a presente pesquisa questiona em que medida a mirada cosmopolita pode contribuir com a compreensão do fenômeno da mundialização da privacidade no século XXI e da necessidade de regulação do direito à proteção de dados pessoais, no contexto do capitalismo de vigilância?

O objetivo geral da presente pesquisa é, então, analisar as contribuições da mirada cosmopolita na compreensão do fenômeno da mundialização da privacidade no século XXI e da necessidade de regulação do direito à proteção de dados pessoais, no contexto do capitalismo de vigilância. Especificamente, pretende-se, a) na primeira seção, explorar o recrudescimento das práticas de vigilância pelo Estado e pelas entidades privadas, ressignificando a privacidade no século XXI no contexto do capitalismo de vigilância; e b) na segunda seção, investigar a mundialização do direito à proteção de dados pessoais e a necessidade de soluções globais, a partir das contribuições da mirada cosmopolita.

Para elaboração do presente trabalho, alerta-se o leitor que o marco teórico adotado, para fins de análise do direito à proteção de dados pessoais, é oriundo das noções de capitalismo de vigilância, expressão cunhada por Shoshana Zuboff; em relação ao cosmopolitismo, emprega-se os caminhos seguidos pelos teóricos de um cosmopolitismo contemporâneo, tais como Martha Nussbaum, Mireille Delmas-Marty, Ulrich Beck. As referências teóricas

entendem que o tratamento de dados, sem uma proteção efetiva e sem uma mudança de paradigma, pode comprometer a segurança nacional, ser utilizado para corromper a própria democracia, ameaçar a sociedade e colocar em risco os titulares, razão pela qual o tema merece aprofundamento e se justifica.

Sobre a metodologia de abordagem, adota-se o método hermenêutico-fenomenológico, uma vez que a pesquisa pretende perquirir qualitativamente sobre o fenômeno da privacidade e da proteção de dados pessoais no século XXI, como se mostra por si mesmo, levando em consideração que a compreensão humana pressupõe a interação do pesquisador com o mundo. Em relação à metodologia de procedimento, utiliza-se o método monográfico, na tentativa de analisar detalhadamente a privacidade e a proteção de dados pessoais como partes de um complexo social. Como técnica de pesquisa, usa-se a documentação indireta, em razão do levantamento de dados a partir da revisão teórica sobre o tema proposto.

O presente artigo está dividido em duas grandes seções, sendo que a primeira, por sua vez, está subdivida em duas subseções, tratando, inicialmente, sobre as rotas da vigilância e controle de corpos e, posteriormente, sobre a redefinição da privacidade no século XXI; por outro lado, a segunda seção também está subdividida em duas subseções, abordando, antes, a harmonização do direito à proteção de dados pessoais na União Europeia, e, depois, a confrontação entre o capitalismo de vigilância e o cosmopolitismo para repensar a privacidade na contemporaneidade.

2 O DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DE CAPITALISMO DE VIGILÂNCIA: AS ROTAS DA VIGILÂNCIA E A REDEFINIÇÃO DA PRIVACIDADE

Na presente seção, com o objetivo de explorar o recrudescimento das práticas de vigilância pelo Estado e pelas entidades privadas, ressignificando a privacidade no século XXI no contexto do capitalismo de vigilância, pretende-se, num primeiro momento, analisar as rotas de vigilância, que permitiram o controle dos corpos e novas formas de alienação dos sujeitos; após, perpassa-se por uma redefinição da privacidade no século XXI, especialmente considerando o avanço e desenvolvimento das tecnologias de informação e comunicação e o advento do capitalismo de vigilância.

2.1. As rotas da vigilância: do controle de corpos a novas formas de alienação

As práticas de vigilância não possuem uma história recente, mas, como dispositivo de poder, foram bem analisadas por Michel Foucault quando da teorização da sociedade disciplinar inspirada no arquétipo do panoptismo e no utilitarismo de Jeremy Bentham. No contexto das instituições totais, p. ex., – família, escola, quartel, fábrica, hospital e, principalmente, prisão - , as práticas de vigilância serviram para docilizar os sujeitos e moldar os corpos, à medida em que o indivíduo se sujeita à disciplina por entender que estava sendo permanentemente vigiado, embora não necessariamente estivesse, num funcionamento automático do poder (FOUCAULT, 2013).

Após a profusão das medidas disciplinares, ocorre uma assunção da vida pelo poder, direcionada, agora, à multiplicidade de indivíduos, ao corpo-população, merecendo atenção e controle os processos de natalidade, fecundidade, higienização, longevidade, mortalidade, dentre outros, numa nova estatística de demografia pública (FOUCAULT, 2005). Ademais, a biopolítica, agora sobre a modulação do corpo, analisa as relações da espécie humana com os demais seres vivos, as coisas e o meio ambiente, de modo que coloca a vida sob domínio público, não somente como processo biológico cotidiano, como *zoé*, vida nua, mas também como *bíos*, sinergia coletiva, afetiva e econômica (AGAMBEN, 2007).

O aperfeiçoamento das tecnologias e o desenvolvimento da cibernética, especialmente a partir da Segunda Guerra Mundial, revolucionaram as práticas de vigilância estatal, especialmente considerando a necessidade de antecipação de inimigos no contexto bélico e o aumento da espionagem militar. Surge, então, um regime de vigilância eletrônica global, fundado numa rede interplanetária de captação e inteligência de sinais, encabeçada, principalmente, pelo Tratado de Segurança UK-USA e pelos Cinco Olhos (Austrália, Canadá, Nova Zelândia, Reino Unido e Estados Unidos), capaz de interceptar e monitorar o tráfego de informações e comunicações mundiais, o que somente foi revelado no início do século XXI (GREENWALD, 2014).

Nessa linha, descobre-se a implementação de diversos outros programas de vigilância global e captação de informações (p.ex., *XKeyScore, PRISM, Lustre, Tempora* etc.), com a participação de agências de inteligência nacional, autoridades policiais, importantes universidades e centros acadêmicos, bem como empresas e organizações de diferentes setores. A Guerra ao Terror catalisou a criação de mecanismos de monitoramento eletrônico de fluxos de informações entre pessoas e grupos, banalizando e absolutizando o inimigo, já que qualquer um pode ser ou se tornar uma ameaça em potencial (GREENWALD, 2014).

Assim, o panoptismo "está vivo e bem de saúde, na verdade, armado de músculos (eletronicamente reforçados, ciborguizados) tão poderosos que Bentham, ou mesmo Foucault,

não conseguiria nem tentaria imaginá-lo" (BAUMAN, 2013, p. 22). No século XXI, o tratamento de dados pessoais pelo Poder Público e o monitoramento estatal são condição de possibilidade para um regime de biopoder baseado em um Estado de vigilância, a fim de antecipar, predizer e controlar todas as formas de vida.

Entremeio ao recrudescimento do Estado de vigilância, as técnicas de vigiar e classificar também vão ser apropriadas pelo setor privado, não somente pelas gigantes das telecomunicações, mas também por *startups* e companhias que buscam algum ponto de disrupção a partir da coleta e tratamento de dados dos usuários, que, desde então, impactam profundamente as relações sociais. A Google é um dos maiores exemplos dessa nova revolução social, porque afeta "nós", "o mundo" e "o conhecimento", daí porque se fala em "googlelização de tudo", já que "ao catalogar nossos juízos individuais e coletivos, nossas opiniões e (ainda mais importante) nossos desejos, a empresa também vai se transformando numa das mais importantes instituições globais" (VAIDHYANATHAN, 2011, p. 14).

No início da história da Google, os dados sobre o indivíduo e os respectivos comportamentos eram utilizados apenas em favor do usuário para personalizar a experiência na internet, na fase do ciclo de reinvestimento do valor comportamental (ZUBOFF, 2019). Logo, a companhia descobriu o superávit comportamental, i.e., a extração, o depósito e o tratamento de quaisquer dados produzidos pelos usuários, que, por mais irrelevantes que possam parecer, eventualmente, a partir de inteligência de máquina e combinação com diferentes fatores, podem ser traduzidos em produtos de predição e receitas de publicidade (ZUBOFF, 2019).

Trata-se de um capitalismo de vigilância, iniciado pelo "*superávit comportamental* descoberto mais ou menos já pronto no ambiente on-line, quando se percebeu que a *data exhaust* que entupia os servidores do Google podia ser combinada com as suas poderosas capacidades analíticas para gerar predições de comportamento do usuário" (ZUBOFF, 2019, p. 404). A Google, assim, "impôs a lógica da conquista, definindo a experiência humana como livre para ser apossada, disponível para ser compilada na forma de dados e reivindicada como ativos de vigilância" (ZUBOFF, 2019, p. 404).

Os usuários, então, não são o produto das companhias, como se costumava referir em razão da aparente gratuidade da plataforma, mas se tornaram os fornecedores dos ativos de vigilância, ou seja, o objeto ou o local de extração da matéria-prima para a criação de receitas de vigilância, cuja possibilidade e probabilidade de predição de comportamentos, gostos e opiniões é o grande produto dessa estrutura, vendido para os reais clientes (anunciantes), ou seja, são as empresas que pagam para atuar nos novos mercados comportamentais (ZUBOFF, 2019). Esses atores privados são, incontestavelmente, os mais verdadeiros e poderosos clientes

do capitalismo de vigilância. Ocorre que essa nova lógica de acumulação é institucionalizada e automatizada, acaba por reformular a própria economia global, agora também baseada na vigilância de dados, sendo cooptada por diferentes atores sociais.

Alguns autores, como Dominique Bourg (2019, p. 11 e 35), comparam o imenso poder das plataformas de vigilância a uma feudalização *sui generis*. Ele lembra que, após o período feudal, a Europa conheceu dois tipos de soberania: a dos Estados e a da Igreja. Esta última, na medida em que organizou a vida de milhões de indivíduos, assumiu a condição de "dona da ordem universal". Observando a ordem mundial atual, ele compara a soberania eclesiástica à do império das grandes empresas do capitalismo de vigilância que, seguramente, influenciam a organização das sociedades acima dos Estados, impondo regras contratuais e condições gerais de utilização de dados e serviços reduzindo os indivíduos à condição de vassalos

Assim, o imperativo de predição precisa ser constantemente reabastecido pelos ativos de vigilância, de modo que os dados comportamentais e dados pessoais dos usuários são minerados absoluta e exaustivamente pelas redes sociotécnicas, legitimadas pelo aceite nos "termos e condições". Trata-se de um Estado geral da vigilância, que "tende a tornar-se incorporada em diversos dispositivos, serviços e ambientes que usamos cotidianamente, mas que se exerce de modo descentralizado, não hierárquico e com uma diversidade de propósitos, funções e significações nos mais diferentes setores" (BRUNO, 2009, p. 02).

No horizonte, o Estado de vigilância e a economia de vigilância se entrecruzam, submetendo todos a essa nova lógica de biopoder institucional (PESSOA, 2020; PESSOA, 2021). Nesse caminho, os usuários pouco ou nada sabem sobre essa nova estrutura econômica, já que a velocidade, personalização e aparente gratuidade das tecnologias deixa para trás os questionamentos, evidenciando uma dependência dos usuários em relação às plataformas e uma ignorância quanto aos riscos e desafios da privacidade nessa era de vigilância.

Cabe falar, então, sobre uma "necessidade de pensar a regulação em uma sociedade marcada pela vigilância, o que não implica apenas a adoção de dispositivos legais que protejam dados e informações, mas também todo e qualquer instrumento ou técnica que apresente um efeito regulatório" (RODRIGUEZ, 2021, p. 116). Dessa forma, "a adoração de medidas dessa natureza exige, por vezes, a conivência com algumas formas positivas de vigilância virtual, norteadas por garantias e princípios que digam respeito à tutela das informações transferidas no espaço material e imaterial da sociedade" (RODRIGUEZ, 2021, p. 116).

O arranjo regulatório deve pressupor que "a) a regulação informacional não deve adotar, exclusivamente, o direito à privacidade como peça irradiante de todo seus sistema protetivo, pois nele não se esgotam os conflitos que envolvem controle e acesso de informações", bem

como que "b) a construção de um corpo legislativo deve contar com apoio técnica para tecnologias de informação e comunicação existentes, mas sem a elas se restringir, sob pena de limitar sua aplicação a determinado momento de evolução tecnológica" (RODRIGUEZ, 2021, p. 117).

Nesse contexto, caso a tutela da privacidade fique condicionada aos interesses e avanços econômicos ou ainda a uma autorregulação pelo mercado, tais circunstâncias podem comprometer a verdadeira proteção desse direito, haja vista que as redes de poder econômico tendem a eliminar os espaços próprios da privacidade em favor do lucro e da publicidade (RODOTÀ, 2008). Trata-se de reconhecer uma nova territorialidade especialmente a partir do entendimento que a internet desafia as fronteiras materiais e físicas, o que, por si só, é um dos desafios do Direito Internacional, já que "a porosidade entre lugares materiais e imateriais talvez exija muito mais do que uma autorregulação por parte do cidadão, necessitando, isso sim, de um marco regulatório claro" (RODRIGUEZ, 2021, p. 113). É até mesmo possível identificar esse espaço-mundo da vigilância digital como um sexto continente de controle quase que perfeito, cujo grande risco é a consolidação de novas formas de totalitarismo e novas e mais nocivas modalidades de alienação humana (SALDANHA, 2013).

2.2. Uma redefinição da privacidade no século XXI

Assim, é preciso atentar que essa alteração do paradigma pressupõe a ressignificação de conceitos, marcada pelo fluxo internacional e transfronteiriço de dados, numa sociedade em rede hiperconectada. Embora tenha sido falado sobre o fim da privacidade no apagar das luzes do século XX, torna-se necessário definir o direito à privacidade para além da concepção sólida e estática dos textos normativos fechados de autoconfinamento para alcançar uma perspectiva aberta, dinâmica e fluida, numa sociedade tecnológica (PEREZ LUÑO, 2012; PESSOA, 2020; RODOTÀ, 2008).

O direito à privacidade, como categoria analítica autônoma de análise, é uma construção moderna estadunidense, elaborada por Samuel Warren, motivado pela divulgação de fatos íntimos do casamento de sua filha nos jornais, e por Louis Brandeis. Os autores publicaram, em 1890, um artigo sobre o *right to privacy* (direito à privacidade), inspirado na expressão cunhada por Thomas McIntyre Cooley, *right to be let alone* (direito de ser deixado só), com base nas necessidades da burguesia estadunidense do final do século XIX (BRANDEIS, WARREN, 1890). Nesse sentido, a doutrina Warren-Brandeis distanciou a privacidade de uma concepção

da tutela da propriedade individual, como anteriormente já tinha sido aventada, e aproximou da necessidade de proteção da vida privada, no âmbito da personalidade humana.

Os autores mencionam que, diante das inovações recentes, era necessário elevar a proteção da personalidade humana e a segurança do cidadão estadunidense a um novo nível, tendo em vista que as novas câmeras e máquinas, fotografias instantâneas, revistas e programas televisivos de fofocas, dentre outras tecnologias, acabaram invadindo o espaço privado do lar e o foro íntimo das pessoas, não obstante o indivíduo possua o direito de estar só ou o direito de ser deixado só (BRANDEIS, WARREN, 1890). Desse modo, a tutela da privacidade vai além do material que contenha determinada revelação íntima, mas atinge também a própria informação veiculada, sendo que a pessoa tem o direito de ser deixada em paz e não fazer público aquilo que lhe é privado.

A doutrina Warren-Brandeis tornou-se popular e ganhou força nos ordenamentos jurídicos nacionais com o passar do tempo, porém, considerando o desenvolvimento das tecnologias de informação e comunicação e as complexidades das relações sociais no decorrer do século XX, o direito à privacidade superou os limites conceituas, desenvolvendo-se na forma de figuras afins, como, por exemplo, “vida privada”, “intimidade”, “sigilo”, “imagem”, “honra”, “proteção de dados pessoais”, dentre outras. A categorização do direito à privacidade é complexa e multifacetada, em razão da própria internalização de conceitos e necessidade de adequação dos termos aos diferentes ordenamentos jurídicos nacionais.

Sobre o tópico, a doutrina alemã da teoria das esferas serviu, por muito tempo, para representar os níveis de privacidade do sujeito na ideia de três círculos concêntricos. O primeiro e maior é a esfera da vida privada (*Privatsphäre*), onde estão as informações que o sujeito não quer que sejam de domínio público embora possam ser de conhecimento de pessoas próximas; o segundo, no interior daquele, é a esfera da intimidade (*Vertrauensphäre*), onde estão as informações que o sujeito compartilha com determinadas pessoas, de forma reservada, íntima, discreta; o terceiro, mais ainda no interior dos demais, é a esfera do segredo (*Geheimnsphäre*), onde estão as informações que o sujeito não quer que sejam do conhecimento de ninguém ou de somente algumas pessoas elegidas (COSTA JR, 1995).

A teoria das esferas ou dos círculos concêntricos de privacidade acabou sendo superada, uma vez que considerava o sujeito uma “cebola passiva” e demandava uma intensa subjetividade no entendimento do grau das esferas, de modo que a insuficiência técnica e as recentes inovações tecnológicas desafiaram os limites da doutrina (DONEDA, 2006). Para substituir a teoria das esferas, pode-se mencionar a teoria do mosaico, que dispõe que os dados relacionados a uma pessoa, num primeiro momento, podem ser irrelevantes, sob um ou outro

prisma ou ainda se considerados de forma isolada, mas, se analisados com outros dados, por si só também irrelevantes, podem gerar um conjunto pleno de significados, de modo que a privacidade deve refletir o mosaico formado com a revelação de tais informações.

Nesse sentido, ressignificar o direito à privacidade "decai em prol de definições cujo centro de gravidade é representado pela possibilidade de cada um controlar o uso das informações que lhe dizem respeito", havendo que se falar em um direito à autodeterminação informativa (RODOTÀ, 2008, p. 24). A expressão "direito à autodeterminação informativa", primeiramente utilizada pelo Tribunal Federal Constitucional Alemão, quando do julgamento de um processo relacionado com as informações pessoais coletadas de um censo no ano de 1983, representa o direito de proteção da própria pessoa, considerando o processamento tecnológico de dados e a tutela do sujeito contra o tratamento das informações, devendo a possibilidade de dispor livremente dos seus dados ser alçada ao patamar de um direito fundamental (MARTINS, 2016).

A conceituação da privacidade somente como o direito de estar só ou direito de ser deixado só, restringindo algumas informações compreendidas privadas do conhecimento público, perdeu, há alguns anos, a capacidade de ser o único fundamento de tutela, sem desconsiderar, no entanto, que essa questão ainda é um aspecto essencial a ser observado em determinados contextos. No entanto, trata-se do fim "de um longo processo evolutivo experimentado pelo conceito de privacidade: de uma definição original como o direito de ser deixado em paz, até o direito de controle sobre as informações de alguém e determinar como a esfera privada deve ser construída" (RODOTÀ, 2008, p. 17).

O direito à privacidade não pode ser entendido somente na concepção isolacionista do "ser", numa lógica excludente de "pessoa-informação-sigilo", isto é, a possibilidade de manter reservada uma informação e exigir que não haja intromissões indesejadas, mas assumir que, com o desenvolvimento das tecnologias de informação e comunicação, há uma relativização daquilo que é sigiloso, íntimo e privado. A questão da privacidade, na Era da Informação, pressupõe novos direitos e introduz-se a possibilidade de os próprios indivíduos controlarem as informações e se empoderaram diante desse contexto, em uma verdadeira metamorfose do direito à privacidade, superando-se a ideia original do direito de estar sozinho, em seu aspecto individual, pela perspectiva de estar inserido no âmbito social e coletivo (PÉREZ-LUÑO, 2012, p. 115).

Fala-se, pois, em uma nova definição da privacidade como "o direito de manter o controle sobre as próprias informações", identificada com a "tutela das escolhas de vida contra toda forma de controle público e de estigmatização social, em um quadro caracterizado

justamente pela ‘liberdade das escolhas existenciais” (RODOTÀ, 2008, p. 92). A privacidade, relacionada àquilo que é secreto e reservado, cede espaço à lógica de “pessoa-informação-circulação-controle”, não mais limitada à burguesia do século XX e às fofocas, mas destinada à multidão na sociedade informacional.

Há, pois, como indicar que “a privacidade indica uma visão negativa e estática, em larga medida pautada na concepção de impossibilitar a interferência de terceiros”, mas a proteção de dados pessoais “confere ao titular poderes positivos e dinâmicos postos à sua disposição com vistas ao controle sobre a coleta e o processamento dos dados que lhe digam respeito” (SARLET, 2020, p. 51). O direito à proteção de dados possui uma fundamentalidade material, que reside na “relevância, para a esfera individual de cada pessoa e para o interesse coletivo (da sociedade organizada e do Estado), dos valores, princípios e direitos fundamentais associados à proteção dos dados pessoais e por ela protegidos”, tais como direito à dignidade da pessoa humana, direito ao livre desenvolvimento da personalidade e direito à privacidade (SARLET, 2020, p. 47).

O Supremo Tribunal Federal, em decisão paradigmática de 2021, de relatoria da Ministra Rosa Weber, na Ação Direta de Inconstitucionalidade nº 6.393, proposta pelo Conselho Federal da Ordem dos Advogados do Brasil, contra a Medida Provisória nº 954/2021, que dispunha sobre compartilhamento de dados por empresas de telecomunicações com o Instituto Brasileiro de Geografia e Estatística – IBGE para fins produção estatística, assentou a constitucionalidade do direito à proteção de dados pessoais. Na decisão que concedeu a medida cautelar para suspensão do ato normativo, a relatora considerou que os dados pessoais “integram, nessa medida, o 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)”, de modo que “sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional” (BRASIL, 2020).

Na verdade, trata-se de um longo processo normativo-regulatório, que pode ser classificado, conforme a doutrina especializada, em quatro gerações de leis (MAYER-SCÖNBERGER, 1997). A primeira geração de leis sobre proteção de dados pessoais, preocupada com o estado da técnica, estabeleceu um conjunto de normas que exigiam a autorização dos usuários para criação de bancos de dados estruturados e regulavam as atribuições do poder público para processamento das informações coletadas (DONEDA, 2011). Por sua vez, a segunda geração de leis sobre a temática, pensando na difusão da utilização de bancos de dados estruturados, previa normas que regulamentavam a privacidade como uma

liberdade negativa, ou seja, que o cidadão pudesse restringir o acesso aos dados pelo poder público (DONEDA, 2011).

Contudo, em razão da necessidade do fornecimento de dados pessoais diante dos fluxos de informação na globalização, a terceira geração de leis sobre proteção de dados, na década de 80, entendeu que, em se tratando de um processo complexo, a tutela da privacidade devia ir além da permissão ou não para utilização das informações, mas deveria levar em apreço a inclusão e informação ao usuário sobre as fases do tratamento de dados, numa autodeterminação informativa (DONEDA, 2011). Por fim, a quarta geração de leis sobre proteção de dados pessoais, momento normativo atual, percebe que a tutela da privacidade não pode ser limitada a uma escolha individual, porém deve exigir a elaboração de instrumentos coletivos de garantias e fortalecer o sujeito, em razão do evidente desequilíbrio na relação entre agentes e usuários, bem como a criação de autoridades independentes para supervisão pública do tratamento de dados na sociedade (DONEDA, 2011).

A democratização do acesso às tecnologias de informação e comunicação e a utilização indiscriminada das informações pessoais diante das inovações cibernéticas trouxe novos desafios à tutela da privacidade. Na rede informática, toda operação ou conjunto de operações, realizadas pelo próprio usuário ou por meio de processos automatizados, permite a coleta, produção, classificação, utilização, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, transferência, difusão, dentre outros tratamentos, de dados comportamentais e pessoais, de modo ser necessária a tutela de um grande número de informações, às vezes produzidas sem o conhecimento do sujeito, não estando mais a privacidade somente limitada àquelas informações privadas, íntimas ou secretas.

O direito à proteção de dados pessoais supera, dessa forma, o conteúdo essencial do direito à vida privada, à intimidade ou ao segredo, uma vez que não se fundamenta apenas na tutela do conteúdo de natureza privada dos dados eventualmente coletados, mas perpassa, também, pela posição de o sujeito saber sobre o tratamento de dados. Na sociedade em rede da Era da Informação (CASTELLS, 2002), com a relevância da grandeza *big data*, a partir da geração de dados independentemente de tempo, espaço e dispositivo, o direito à proteção de dados é um direito autônomo, traduzindo-se em uma tutela para garantia da dignidade humana e livre desenvolvimento da personalidade, frente ao uso perverso das tecnologias de informação e comunicação.

Em outras palavras, é preciso destacar que as normativas quanto à regulação de dados não servem para coibir ou proibir o tratamento, tendo em vista que a livre circulação de dados pessoais é uma realidade não somente de um mercado comum interno, mas também da

sociedade em rede. Assim, trata-se de um superpanóptico, formado por panópticos, banópticos e sinópticos (BAUMAN, 2013), que invertem a lógica de vigilância, fazendo com que o indivíduo forneça os próprios dados informacionais e de outros com quem interage para sustentar essa nova arquitetura de vigilância.

A regulação do direito à proteção de dados precisa considerar que o horizonte é marcado pelos fluxos globais de dados comportamentais e de dados pessoais como ativos econômicos e receitas de publicidade, especialmente diante do capitalismo de vigilância (PESSOA, 2020). Nessa perspectiva de "pessoa-informação-circulação-controle", cabe salientar que, se antes as informações estavam sob domínio do sujeito, que podia controlar se compartilhava ou divulgada com outras pessoas, na sociedade em rede, os dados – e, especificamente, os dados pessoais – estão espalhados pela malha digital, divididos em uma pluralidade de grandezas, obtidos de uma multidão.

O abuso ou uso indevido dos dados, no contexto da sociedade em rede, pode afetar desde a liberdade dos titulares até a própria democracia, como, por exemplo, por meio de mecanismos de manipulação da opinião pública, da criação de filtros invisíveis no debate político, da proliferação do fenômeno da desinformação, do desenvolvimento de consumos insustentáveis de bens e serviços, do vazamento ou comercialização de informações pessoais para agentes maliciosos e da vigilância massiva e constante dos cidadãos por parte de governos e empresas, além da utilização de tais ativos para prática de condutas criminosas. Trata-se, em verdade, de um grande mercado no qual as predições da evolução do comportamento humano são compradas e revendidas de maneira especulativa (MBEMBE, 2023).

O caso da Cambridge Analytica evidencia como a perda de privacidade pode ser usada, por exemplo, para manipular a própria democracia. Em violação à proteção de dados das pessoas, essa agência conseguiu criar perfis psicológicos detalhados, que foram utilizados para direcionar anúncios políticos específicos para eleitores e indecisos com base em suas inclinações, a favor de um determinado candidato às eleições, como ocorreu nos Estados Unidos da América, ou em direção a uma específica posição política, como aconteceu no Reino Unido nas discussões sobre o Brexit, cuja revelação do escândalo levou a empresa à falência e escárnio público (PRIVACIDADE, 2019).

Porém, não é só, já que o potencial impacto negativo do tratamento de dados pode trazer consequências preocupantes. O processamento de dados pode comprometer a segurança nacional, incluindo informações sobre cidadãos, funcionários do governo, membros de forças armadas e outras questões confidenciais; pode corromper a democracia, manipulando eleições e influenciando a opinião pública, especialmente por meio de campanhas de desinformação ou

de propagandas direcionadas; pode ameaçar a sociedade ao promover uma cultura de exposição e vigilantismo; pode colocar em risco a própria segurança dos indivíduos, em razão da exposição indevida de informações pessoais, que pode levar a roubos de identidade, fraudes financeiras, bem como problemas relacionados à segurança pessoal.

Chega-se a dizer que "os dados pessoais são perigosos, porque são sensíveis, altamente suscetíveis ao mau uso, difíceis de manter em segurança e cobiçados por muitos – desde criminosos a seguradoras e agências de inteligência", concluindo-se que "os dados são vulneráveis, o que acaba por tornar os seus titulares e qualquer pessoa que os armazene igualmente vulneráveis" (VÉLIZ, 2021, p. 128). Por essa razão, o direito à privacidade ultrapassa os limites de uma tutela individual e também desafia estratégias de proteção coletiva, especialmente a partir da proliferação de regulações extraterritoriais de proteção de dados, tornando-se elemento importante na construção da cidadania global.

3 O DIREITO À PROTEÇÃO DE DADOS PESSOAIS DIANTE DA MIRADA COSMOPOLITA: OS ESFORÇOS EUROPEUS E A VIA DO COSMOPOLITISMO

Na presente seção, com o objetivo de investigar a mundialização do direito à proteção de dados pessoais e a necessidade de soluções globais, a partir das contribuições da mirada cosmopolita, procura-se analisar o desenho e a experiência de harmonização sobre a temática da proteção de dados pessoais na União Europeia, com a confrontação do capitalismo de vigilância ao cosmopolitismo jurídico.

3.1. Proteção de dados pessoais no desenho de harmonização na União Europeia

Se no panorama anterior, a violação da privacidade podia ser essencialmente a fofoca ou a revelação do segredo, atualmente, a violação ocorre por métodos abstratos e desconhecidos, a partir da manipulação e vigilância dos dados comportamentais e dados pessoais nas diferentes formas de tratamentos do capitalismo de vigilância. Nesse cenário, "raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados", sendo possível que não reflita sobre a periculosidade do uso de tais informações por parte de diferentes agentes estatais ou organizações (RODOTÀ, 2008, p. 37).

Como referido anteriormente, a Europa já vinha discutindo o caráter normativo da proteção de dados pessoais, pelo menos, desde a década de 70/80, em países como Alemanha,

Espanha e França. A Convenção nº 108, do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981, foi um dos primeiros instrumentos internacionais adotados no âmbito da proteção de dados, com especial relevância à coleta e processamento de dados sensíveis sobre raça, política, saúde, religião, vida sexual, registro criminal, dentre outros (CONSELHO DA EUROPA, 1981).

Sobre a nova concepção da privacidade, no direito comunitário europeu, justamente em razão da livre circulação de pessoas, bens e dados, o direito à proteção de dados pessoais foi previsto, de forma autônoma, na Carta de Direitos Fundamentais da União Europeia de 2000, que, no art. 8º, estabelece que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito", de modo que "esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei", sendo que "todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação" (UNIÃO EUROPEIA, 2000).

No âmbito, algumas diretivas já direcionavam a tutela dessa nova acepção do direito à privacidade, como no caso da Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (UNIÃO EUROPEIA, 1995); da Diretiva 97/66/CE, do Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997 relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações (UNIÃO EUROPEIA, 1997); e da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas (UNIÃO EUROPEIA, 2002).

Conquanto as diretivas não possuem obrigatoriedade de aplicação direta, representam, na verdade, um caminho que precisa ser adotado ou adaptado pelos ordenamentos jurídicos nacionais. Considerando o recrudescimento do tratamento de dados e a necessidade de um marco comum, a União Europeia estabelece, então, o Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE, também conhecido como Regulamento Geral de Proteção de Dados, ou pela sigla RGPD, sendo este um marco normativo obrigatório e diretamente aplicável nos países signatários (UNIÃO EUROPEIA, 2016).

O Regulamento Geral de Proteção de Dados Pessoais (RGPD) exige uma mudança de postura, visto que, além de uma proteção repressiva – a exemplo da possibilidade de aplicação de multas milionárias pelo tratamento de dados pessoais em desconformidade com a lei -, é necessária uma atuação proativa, baseada na avaliação e mitigação do risco (ao contrário da norma anterior que considerava o tipo de dado ou o tipo de tratamento), bem como na responsabilidade ativa, consciente e diligente dos agentes de tratamento, requerendo a adoção de medidas de segurança administrativas e técnicas, boas-práticas e políticas de privacidade.

No entanto, o Regulamento Geral de Proteção de Dados Pessoais (RGPD) acaba por avançar as fronteiras físicas nacionais, superando os limites da territorialidade da União Europeia, já que a tutela é aplicável ao tratamento de dados por uma empresa estabelecida na União Europeia, independentemente do local de tratamento desses dados ou da nacionalidade do titular deles; e, ainda, ao tratamento de dados por uma empresa que, embora não estabelecida na União Europeia, ofereça bens e serviços ou monitoramento para usuários que ali se encontrem, além de servir como fonte de inspiração para normativas sobre proteção de dados pessoas em países de outros continentes (UNIÃO EUROPEIA, 2016).

A comunidade europeia, a fim de concretizar os princípios e o próprio direito fundamental à proteção de dados, buscou tomar medidas ativas no cenário internacional, por meio da regulação de mercado, afastando qualquer tentativa de autorregulação. Evidentemente, tal ato ocorreu por ser a União Europeia detentora do maior mercado comum interno do mundo, sendo promovido por fortes instituições regulatórias e permitindo a imposição de suas normas aos mercados de consumo, além de uma propensão à regulação de direitos fundamentais (ao contrário da tradição norte-americana, por exemplo) (BRADFORD, 2012).

Na tentativa de manutenção das práticas comerciais com a União Europeia e a possibilidade de fluxos transfronteiriços de dados, países fora do bloco se viram diante da necessidade de adequação das normativas aos padrões europeus de exigência, dando origem ao fenômeno denominado “Europeização” ou “Efeito Bruxelas” (BRADFORD, 2012). Nesse viés, o Regulamento Geral de Proteção de Dados (RGPD) gerou grande impacto internacional, com previsão de medidas de cooperação internacional em tema de proteção de dados e restrições à transferência internacional de dados, especialmente considerando a concessão de decisão de adequação ou conformidade, isto é, uma chancela, por parte da União Europeia, de que os demais países possuem nível adequado de proteção de dados pessoais.

O “Efeito Bruxelas” foi precipuamente estudado e conceituado por Anu Bradford, na obra *The Brussels Effect*. De acordo com a autora, existem cinco requisitos que precisam estar presentes para ocorrer tal fenômeno, quais sejam: i) a jurisdição deve conter um grande poder

de mercado – na medida em que não há opção para o negociante em renunciar à venda, mas sim visualizar que os benefícios de acessar o mercado superam os custos de ajustes necessários; ii) capacidade regulatória para impor suas regras, com a devida *expertise*; iii) existência de órgãos regulatórios que visem criar normas rígidas, que repasse às companhias a ideia de que haverá um alto custo associado com o descumprimento de tais regras; iv) objetivo do Regulamento inelástico, com meta fixada em termos de localização, como os consumidores que compram um produto, assim o produtor não poderá escapar da jurisdição pela qual está regulado; e v) o sistema produtivo deve ser indivisível, o que significa que produzir diferentes versões do mesmo bem ou serviço terá um custo elevado (BRADFORD, 2012).

A título exemplificativo, as áreas afetadas no contexto mundial por esse fenômeno foram: i) a saúde e a segurança dos consumidores; ii) a proteção ao meio ambiente, por meio da restrição à produção e comercialização de produtos, bem como à utilização de determinados insumos e métodos produtivos; e iii) a economia digital, que engloba as restrições ao tratamento de dados pessoais (BRADFORD, 2012). Não por acaso, sinala-se que a possibilidade de transferência internacional de dados pessoais, inclusive sem o consentimento do titular, está condicionada à concessão de decisão de adequação por parte da União Europeia; quer dizer, a União Europeia avocou para si a iniciativa de determinar qual país possui um nível de proteção de dados pessoais adequado a permitir o fluxo de dados transnacionais com países do bloco, o que evidencia o fenômeno da europeização (GNOATTON, 2021).

A influência europeia, ante o pioneirismo de legislação própria tratando sobre proteção dos dados pessoais e posição importante no mercado internacional, fez com que a União Europeia tivesse a habilidade quase que unilateral de regular o mercado global com normas protetivas de tratamento de dados pessoais. Diante deste cenário, atores privados, grupos empresariais e países terceiros tiveram que se reorganizar interna e regionalmente, editando leis protetivas acerca da matéria, tudo isto visando atender o *standard* de proteção previsto no Regulamento.

Percebe-se um duplo matiz, uma vez que a regulação da privacidade em termos de proteção de dados pessoais "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", sendo necessário recordar "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" (DONEDA, 2011, p. 102).

Com a promulgação de diretrizes sobre o tema nos últimos anos, é possível abordar, pelo menos, alguns modelos ou estratégias de regulação de proteção de dados: o modelo normativo-estatal, o modelo liberal e o modelo misto ou eclético. Nesse sentido, o modelo normativo-estatal possui como característica principal a existência de um sistema normativo centralizador, mais procedimental, cuja competência regulatória e fiscalizatória fica a cargo do próprio Estado; o modelo liberal pressupõe a existência de uma autorregulação regulada, na medida em que o Estado somente normatiza em áreas sensíveis, como saúde, finanças e crianças e adolescentes; o modelo misto ou eclético resulta de um conjunto de estratégias de regulação, tais como normas estatais, códigos mercadológicos, mecanismos alternativos de resolução de conflitos, soluções tecnológicas e posturas proativas no cumprimento e fiscalização da legislação sobre a temática (GUIDI, 2018, p. 85-110).

A elaboração de marcos jurídicos de proteção de dados pessoais, inclusive internacionais, não se reduz a questionar "se" e "por que" regular, mas questiona "por quem" e "como" tutelar o direito à proteção de dados pessoais, justamente porque a legitimação do tratamento de dados é fundamental para proteger a privacidade e o livre desenvolvimento da personalidade dos titulares, ou, pelo menos, oferecer garantias e salvaguardas aos usuários diante da economia de dados pautada no capitalismo de vigilância. Em caso contrário, i.e., relegando a proteção de dados à autorregulação ou a nenhuma regulação, pode-se correr o risco de chancelar a privacidade como simples *commodity* no mercado globalizado, como meto ativo de vigilância.

A discussão sobre marcos jurídicos de proteção de dados pessoais, considerando que os fenômenos jurídicos, políticos, sociais, culturais, econômicos e naturais estão interligados, traz a transversalidade própria da mundialização, ressignificando os processos e valores na sociedade em rede. Nessa linha de pensamento, é possível debater sobre a proteção de dados pessoais global, em razão dos desafios que já se avizinham, mormente pelo advento do Regulamento Geral de Proteção de Dados Pessoais e outras iniciativas regulatórias da União Europeia, que, mais do que normas de conexão, influenciam os atores internacionais a repensar as próprias agendas regulatórias comuns.

Entremeio a isso, encontram-se as normas técnicas ou de gestão, bem como os *frameworks* ou *standards* que influenciam nas discussões sobre a temática. Nesse sentido, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), grupo dos países mais ricos do mundo, cujo ingresso pressupõe a adoção de normas técnicas, políticas diplomáticas e legislações estatais específicas, editou, em 1980, as Diretivas sobre Proteção da Privacidade e Fluxo de Dados Fronteiriços da OCDE (tradução livre para *OECD's Guidelines*

on the Protection of Privacy and Transborder Flows of Personal Data), determinando que os membros adotassem legislação doméstica apropriada, encorajassem a autorregulamentação, fornecessem aos indivíduos meios razoáveis para exercerem seus direitos, trouxessem sanções e soluções apropriadas em caso de inobservância das medidas, garantissem não haver injusta discriminação contra os sujeitos dos dados e cooperassem internacionalmente (OCDE, 1980).

A ISO 27001:2013, por sua vez, criou o Sistema de Gestão de Segurança da Informação (SGSI), baseando nos requisitos de segurança da informação, quais sejam, confiança, integridade e acesso ou disponibilidade, com a certificação de adequação e conformidade das organizações que adotarem os padrões estabelecidos na norma técnica (ISO, 2013). Ainda, dentro da família ISO 27000, estabeleceu-se a ISO 27701:2019, que trouxe o Sistema de Gestão da Privacidade da Informação (SGPI), com particularidades relativas à proteção de dados pessoais (ISO, 2019).

Esse quadro traz uma importante mudança de postura, posto que "as normas técnicas e de gestão investem e colonizam o conjunto dos campos sociais em todos os níveis, inclusive nacionais, locais e setoriais, e invadem progressivamente todos os aspectos da vida pública até, e inclusive, a intimidade" (FRYDMAN, 2018, p. 81). Assim, pensando que a sociedade global é uma sociedade fragmentada em setores, regulados por instâncias e normas específicas, de modo que o Direito assume uma função de tradução e mediação, torna-se "necessário e urgente que o jurista se emancipe de uma concepção muito estreita, formal e rígida, a fim de voltar seu olhar, seu interesse e seus estudos para o campo mais vasto da normatividade, em toda a diversidade de suas formas e de suas técnicas" (FRYDMAN, 2018, p. 94).

3.2. O capitalismo de vigilância confrontado ao cosmopolitismo: como repensar a proteção de dados pessoais

O mercado digital global e os fluxos transfronteiriços de dados atravessam a inexperiência e a barreira territorial dos países, exigindo coordenação e cooperação internacional. Caberia, então, questionar sobre a possibilidade de caminhos regulatórios sobre proteção de dados pessoais, apesar dos desafios e limites advindos da corregulação, já que reflete sobre a privacidade não somente por um viés individual, do ponto de vista do usuário, mas desde uma tutela coletiva, direcionada a uma multidão, considerando a economia de dados pautada no capitalismo de vigilância.

Percebe-se um contexto de intensa desterritorialização, que impacta os conceitos clássicos de soberania e territorialidade, mormente porque as atividades transnacionais e os

fluxos informacionais ocorrem além das fronteiras físicas dos Estado-nação, apesar dos entes políticos tradicionais. O ambiente digital globalizado permite que indivíduos, grupos, empresas e governos acessem informações e realizem transações em diferentes jurisdições, o que reacende o debate sobre qual conjunto de leis e regulamentos deve ser aplicado em casos de conflito, justaposição ou emaranhado de normas jurídicas e técnicas.

Nesse sentido, convém tratar sobre uma mirada cosmopolita, que pode ajudar na compreensão desse fenômeno por diferentes ângulos, com base em princípios plurais e objetivos comuns, que desafiam as noções jurídico-políticas dos Estados nacionais. Isso porque "a multiplicação das fontes de criação do Direito, a fragilização da soberania e a erosão da representação unitária da vontade dos Estados são expressões do mundo contemporâneo", provocando, entre outros efeitos, "a interrelação entre vários sistemas normativos, o acentuado aumento da complexidade das razões jurídicas, a diversificação dos critérios de validade e a hibridação dos saberes jurídicos" (SALDANHA, 2018, p. 78).

No entanto, não se está a falar unicamente de um cosmopolitismo moral dos antigos, que, inspirado no cinismo ou no estoicismo greco-romano, em apertada síntese, pregava a fraternidade universal, baseada no respeito recíproco, uma vez que, controlando as ações e pensamentos, concentrando-se naquilo que pode mudar e agindo de forma racional para com o outro, seria possível maximizar o bem-estar de todos, responsabilizando pelo futuro (NUSSBAUM, 2020). Ademais, conforme a moral cosmopolita, o local de nascimento de um ser humano é mero acidente ou fruto do azar, de modo que todos os seres humanos são merecedores de igual respeito e interesse em um sentido profundo, desapegando-se dos bens materiais desnecessários para partirem em busca de uma comunidade cosmopolita.

Tampouco se está a referir somente de um cosmopolitismo filosófico dos modernos, principalmente guiado pelo pensamento kantiano, que, de forma resumida, convidava as Nações a constituírem uma aliança dos povos em favor de um projeto de paz segundo o direito das gentes. Conforme o cosmopolitismo kantiano, a paz perpétua poderia ser alcançada a partir de três caminhos: um interno, com a existência de uma Constituição para desenvolvimento nacional; um internacional, com a formação de uma Federação de Estados livres que poria fim ao estado de guerra e de natureza global; e cosmopolítico, com base na hospitalidade universal e nas relações pacíficas para além da ordem internacional (KANT, 2020; KANT, 2010; SALDANHA, 2018).

Mas, sim, abordar um cosmopolitismo contemporâneo, surgido, notadamente, a partir do novo pacto humanitário firmado após a experiência totalitarista do século XX e do fenômeno da mundialização do Direito, com especial ênfase nas acelerações e complexidades das relações

sociais em razão do desenvolvimento das tecnologias de informação e comunicação. Ainda, quem sabe, explorar um cosmopolitismo jurídico em virtude do duplo fenômeno da internacionalização do direito constitucional e da constitucionalização do direito internacional, considerando instituições cosmopolitas, espaços públicos cosmopolitas, normas e atores também cosmopolitas (SALDANHA, 2018).

Desde o término da Segunda Guerra Mundial, testemunha-se uma ampliação e um aprimoramento de documentos e tratados internacionais que protegem os direitos humanos, tais como a Declaração Universal dos Direitos Humanos e textos específicos, que têm buscado proteger os direitos de grupos particulares, como migrantes, refugiados, mulheres e crianças. No entanto, essa evolução normativa enfrenta desafios e oscilações, como é o caso da interação entre os interesses nacionais e as reivindicações de caráter cosmopolita que ultrapassam as fronteiras dos Estados nacionais (BENHABIB, 2006).

De um lado, identifica-se a tensão entre a busca por autonomia e autodeterminação em nível nacional, e, por outro lado, as demandas pelo reconhecimento de direitos universais e universalizáveis. A abordagem das iterações democráticas é vista como a forma necessária de convergência entre as aspirações e normas cosmopolitas e os processos de deliberação em contextos nacionais, que serão os destinatários dos resultados de processos globais (BENHABIB, 2006). A cooperação e a solidariedade transnacional tornam-se valores fundamentais para legitimar o cosmopolitismo contemporâneo.

Na perspectiva cosmopolita, as iterações democráticas representam uma profunda modificação na comunidade global, refletindo a emergência de novos códigos comunicativos e novos atores que transcendem as fronteiras nacionais e locais. O fenômeno da mundialização e os processos de cooperação transnacionais apresentam um desafio significativo no que concerne à necessidade premente de conciliar os princípios universalistas dos direitos humanos com as necessidades particulares e concretas de indivíduos e grupos que se conectam através de laços religiosos, linguísticos, étnicos e culturais (SALDANHA, 2018).

Necessário, pois, modificar o modo de compreender o mundo contemporâneo, conectado de diferentes modos, reestruturando, ainda que conceitualmente, tradicionais noções sobre o Estado e Direito. Nesse contexto, a “primeira modernidade”, relativa às sociedades individuais nacionais ordenadas, deve ser superada pela “segunda modernidade”, caracterizada pelas formas de vida transnacionais, já que a proteção e a blindagem dos nacionalismos individuais contra o global não é mais suficiente e pode acabar violando direitos e garantias individuais e coletivas (BECK, 2004, p. 10-15).

Trata-se de uma "empatia cosmopolita ou compaixão cosmopolita" (BECK, 2004, p. 15), a fim de que fazer com que a humanidade queira agir contra as mais variadas injustiças e violências contra os direitos humanos, inclusive surgidos ou desenvolvidos nesse novo paradigma social, alicerçado pelas tecnologias de informação e comunicação. Assim, "os movimentos das organizações internacionais humanitárias, somados aos das redes sociais que colorem o espaço virtual deste início de século, representam essa empatia global que se choca com o nacionalismo metodológico e excludente" (SALDANHA, 2018, p. 80).

A mirada cosmopolita, que não substitui a empatia nacional, mas complementa a visão mundial, pode ser fundamentada em cinco expressões: experiência de crises globais da sociedade mundial (vide pandemia de COVID-19), reconhecimento das diferenças da sociedade mundial e preocupação com a alteridade, empatia cosmopolita e mudança de perspectiva, (im)possibilidade de viver em uma sociedade mundial sem fronteiras e mistura entre culturas e tradições locais, nacionais, étnicas, religiosas e cosmopolitas (BECK, 2004, p. 17; SALDANHA, 2018, p. 80).

O marco teórico do cosmopolitismo não desconsidera a interconexão entre o local e o global. Em vez disso, defende a importância da imaginação dialógica, reconhecendo que o global está intrinsecamente vinculado ao local e vice-versa, já que ambos formam um conjunto de propriedades que não se excluem, mas coexistem em uma interdependência significativa. Beck argumenta que, diante do "cosmopolitismo subalterno", reconhece-se a interconexão entre o local e o global, entendendo que o Direito não pode ser limitado por fronteiras nacionais e há uma necessidade de ações e responsabilidades compartilhadas em relação aos problemas globais (BECK, 1999; BECK, 2004).

O cosmopolitismo jurídico requer o estabelecimento de instituições e ferramentas legais que possam interagir com questões globais, como direitos humanos, proteção ambiental e justiça social. Assim, o cosmopolitismo não busca eliminar as diferenças culturais e identidades locais, mas reconhecer a interdependência e buscar uma coexistência pacífica e justa entre diferentes perspectivas, sendo, portanto, uma abordagem necessária para enfrentar os desafios globais.

Por sua vez, Nussbaum fundamenta uma perspectiva de desenvolvimento humano cosmopolita, baseado na promoção das capacidades humanas básicas, inclusive em escala global (NUSSBAUM, 2020). Dessa forma, deve-se garantir o desenvolvimento das capacidades humanas básicas, tais como vida saudável, educação, participação política, liberdade de expressão, entre outras, que devem ser asseguradas a todos os seres humanos, independentemente de suas origens ou conformações nacionais, inspirada no pensamento

estoico que a nacionalidade é fruto do acaso, em reconhecimento de verdadeiros cidadãos do mundo.

Atentando-se para o objeto do presente trabalho, percebe-se que a temática da privacidade e da proteção de dados pessoais é uma questão global, que, de igual modo, precisa de soluções globais – ou cosmopolitas. Ora, os dados comportamentais e os dados pessoais dos usuários se tornam ativos de vigilância e geram receitas de toda sorte para os agentes de tratamento; os fluxos transfronteiriços de dados são pressupostos necessários no mercado de consumo globalizado e na economia digital; a internet e, em especial, as redes sociais, principais espaços para mineração de dados, são compartilhados globalmente, de modo que a informação e a comunicação é global; a *googlelização*, *facebookzação* e a *tiktokzação* de tudo homogeneíza e pasteuriza as relações sociais em diferentes lugares, coletando cada vez mais e mais dados; as *big techs* superam os limites territoriais nacionais e se volvem atores globais, inclusive mais ricos que muitos países, aplicando termos e condições – no horizonte, contratos de adesão – a bilhões de pessoas, alterando profundamente a compreensão e a significação dos fenômenos, dentre outros.

Além disso, as normas jurídicas e técnicas sobre privacidade vão se encaixando numa rede complexa de instrumentos regulatórios. A União Europeia publica, em 2016, um Regulamento Geral de Proteção de Dados Pessoais diretamente aplicável nos Estados-membros, sem necessidade de transposição por norma nacional; ademais, o RGPD estabelece, dentre os requisitos para ocorrer o fluxo transfronteiriço de dados pessoais, a necessidade de decisão de nível adequado de proteção de dados, que compete à Comissão Europeia, fazendo com que diversos países se inspirem no modelo europeu para criação ou atualização de normas de privacidade, tais como o Brasil, Argentina, Uruguai, Nova Zelândia, Japão e, inclusive China.

Para conceder o nível de adequação, a Comissão Europeia analisa, dentre outros elementos, o primado do Estado de Direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor e sua aplicação, as medidas de segurança, a jurisprudência, bem como os direitos e recursos para o titulares dos dados; ainda, verifica a existência e o efetivo funcionamento de uma ou mais autoridades de controle independentes, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados; e, também, os compromissos internacionais assumidos pelo país ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, assim como a participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais (UNIÃO EUROPEIA, 2016).

Nessa linha, diferentes países buscam, na União Europeia, um modelo regulatório de privacidade e acabam importando regramentos similares sobre a proteção de dados pessoais, sendo que, um em especial, gera um efeito interessante: a possibilidade de aplicação extraterritorial da legislação sobre o tema, por muitas considerarem, no âmbito de aplicação, o local da operação de tratamento, independentemente de nacionalidade ou residência do titular, da sede ou domicílio do agente de tratamento ou de localização dos dados. Desse modo, cria-se um emaranhado de leis no espaço com significados comuns a respeito da privacidade e proteção de dados pessoais.

É possível dizer, então, que, "da análise do mosaico global das relações econômicas, jurídicas e políticas, antevê-se ter o cosmopolitismo deixado de ser uma simples ideia da razão e do mundo filosófico, para constituir-se numa pura e inexorável realidade", modificando o modo de compreender e se compreender no mundo (SALDANHA, 2018, p. 79). Para tanto, fala-se em uma mirada cosmopolita, i.e., "mínima exigência para que se entenda a realidade jurídico-social e política do século em curso a partir da 'reestruturação' conceitual das tradicionais percepções sobre o Estado e sobre as formas de produção e de aplicação do Direito" (SALDANHA, 2018, p. 79).

De fato, como advertiu Mireille Delmas-Marty (2020, p.16), o mundo é cada vez mais invadido por normas sensoriais que se impõem diretamente e impedem toda a desobediência. Ela faz a pergunta lancinante: como responderemos a essas práticas aparentemente inofensivas na forma de um "conta-gotas normativo" cotidiano que nos submete a todos? A resposta que a autora nos confere é a de que necessitamos de um novo humanismo jurídico neste tempo em que estamos "desbussolados" e no qual a inovação se opõe à conservação. Mais preocupante, ainda, é que as democracias, ao permitirem o armazenamento e o cruzamento de milhões de dados, em verdade, sucumbem ao "totalitarismo doce" da sociedade de vigilância (DELMAS-MARTY, 2020, p. 17).

No contexto do Estado de vigilância e do capitalismo de vigilância, a preocupação com a proteção de dados dos usuários das redes sociotécnicas assume especial relevância, especialmente no que se refere à concretização de direitos e assunção de responsabilidades, uma vez que o tratamento de dados comportamentais e de dados pessoais afeta o livre desenvolvimento da personalidade humana e o exercício da cidadania (vide efeitos nos processos eleitorais, por exemplo). Porém, levando em conta o totalitarismo digital global, não há respostas jurídicas unicamente na dimensão nacional, devendo-se considerar que "o reconhecimento da dimensão cosmopolita a determinadas normas é pressuposto para a proteção

os direitos na esfera global, independentemente da vinculação dos indivíduos ao território ou a qualquer conformação nacional" (SALDANHA, 2018, p. 119).

O direito à hospitalidade universal, sem ignorar sua importância nos fluxos migratórios e nos conflitos bélicos, tampouco tentar revolucionar ou superar o conceito inspirado no pensamento kantiano, pode ser revisitado no contexto da proteção de dados. Quer dizer, se o tratamento de dados pessoais é condição de possibilidade para o exercício da cidadania, para o livre desenvolvimento da personalidade humana e para mover a nova ordem econômica global, sem desconsiderar as severas críticas ao vigilantismo, o direito à proteção de dados (não somente pessoais) caminha em sentido cosmopolita, tutelando-se, de um lado, o titular, independentemente de nacionalidade ou localização, e, do outro lado, os dados pessoais, onde quer que tenham sido coletados, para onde transferidos, com quem compartilhados ou onde se localize o titular.

Reconhece-se o avanço de algumas legislações sobre a temática da proteção de dados pessoais em um sentido mundializado. O Regulamento Geral de Proteção de Dados Pessoais da União Europeia se aplica ao tratamento de dados pessoais efetuado no contexto das atividades de um agente de tratamento situado no território comunitário, independentemente de a operação ocorrer dentro ou fora, bem como ao processamento de dados pessoais de titulares residente da União Europeia, ainda que o controlador ou operador não esteja estabelecido naquele contexto (UNIÃO EUROPEIA, 2016). A Lei Geral de Proteção de Dados Pessoais do Brasil, por sua vez, também se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que o tratamento seja realizado no território nacional, ou tenha por objetivo ofertar bens ou serviços a indivíduos aqui localizados ou que os dados pessoais sejam coletados no espaço brasileiro (BRASIL, 2018).

O direito à proteção dos dados pessoais, em uma perspectiva global e atual, revela o fenômeno da fragmentação constitucional e o surgimento de normas transconstitucionais (TEUBNER, 2020). Isso ocorre porque o tratamento de dados pessoais não se limita a fronteiras físicas, graças às tecnologias de informação e comunicação, especialmente a internet. Portanto, diversas normas de proteção são estabelecidas por diferentes atores sociais em vários processos constitucionais, em diferentes comunidades políticas, com influências variadas de outros sistemas sociais. Essa complexidade vai além das fronteiras nacionais e desafia a concepção de um constitucionalismo digital e uma abordagem cosmopolita.

Há, portanto, um caráter transnacional e humanista, visto que as legislações nacionais têm aplicação além das fronteiras territoriais e precisam se adequar a padrões comunitários,

internacionais e técnicos para permitir o fluxo internacional de dados. Além disso, os agentes que tratam esses dados se conformam às normas técnicas de atores privados internacionais, e os titulares estão vinculados a termos e condições globais, inclusive de instituições privadas. Como resultado, existe uma complexa rede de normas constitucionais fragmentadas relacionadas à privacidade e proteção de dados pessoais, todas com o objetivo de garantir a segurança do titular dos dados, independentemente da conformidade nacional.

Desde o projeto jurídico de Kant, que remonta ao passado distante, até os marcos normativos internacionais que surgiram ao longo do século XX, o século atual requer mais do que apenas regulamentações nacionais ou as tradicionais do direito internacional, frente aos desafios da sociedade mundializada, inclusive mediada pelas tecnologias de informação e comunicação. Nesse caminho, para além da construção comum da esfera pública, "o cosmopolitismo jurídico se caracteriza por trazer como elemento primordial a necessidade de proteção dos indivíduos, dos grupos, dos animais não humanos e da natureza em suas relações com os estados no plano mundializado" (SALDANHA, 2018, p. 137).

Não se desconhece os desafios e conflitos de implementação de cosmopolíticas, mas esse novo paradigma social pode ser entendido como uma visão holística do mundo, que "concebe o mundo como um todo integrado e não como uma coleção de partes dissociadas, e reconhece a interdependência fundamental de todos os fenômenos e o fato de que, enquanto indivíduos e sociedades, estamos todos encaixados nos processos cíclicos da natureza" (CAPRA, 1996, p. 16). O cosmopolitismo jurídico pressupõe uma solidariedade planetária, como expressão maior de um humanismo de interdependência, diante do horizonte da mundialização e do inevitável destino comum (SALDANHA, 2018).

4 CONCLUSÃO

A presente pesquisa se insere dentro de um cenário desafiante de buscar caminhos ou criar soluções para problemas globais e complexos, especialmente a partir do desenvolvimento das tecnologias de informação e comunicação e do fenômeno da mundialização. Dessa forma, o problema da presente pesquisa questionava em que medida a mirada cosmopolita pode contribuir com a compreensão do fenômeno da mundialização da privacidade no século XXI e da necessidade de regulação do direito à proteção de dados pessoais, no contexto do capitalismo de vigilância.

Percebe-se, então, o recrudescimento das práticas de vigilância pelo Estado e pelas entidades privadas, de modo que a descoberta do superávit comportamental, da exaustão de

dados e do imperativo de predição forjaram uma nova lógica econômica de produção – o capitalismo de vigilância. Nesse contexto, a privacidade acabou ressignificada em favor de um direito à proteção de dados pessoais, que fez eclodir um emaranhado complexo de normas jurídicas e técnicas de regulação do tema, desafiando, ainda, proteções coletivas em favor dos titulares de dados.

Por sua vez, a mundialização do direito à proteção de dados pessoais e a eminente necessidade de soluções globais, considerando que o capitalismo de vigilância, em razão da perversa lógica de tratamento de dados dos titulares, desafia tutelas coletivas sobre o tema. Isso porque a proteção dos dados dos usuários está intimamente ligada ao livre desenvolvimento da personalidade humana e ao exercício da cidadania, que, contudo, diante das práticas de vigilância, não encontra resposta única na dimensão nacional.

Nesse sentido, o cosmopolitismo jurídico, na defesa dos direitos e interesses dos indivíduos independentemente da vinculação a território ou conformação nacional, pode auxiliar na pavimentação de caminhos para a tutela global dos titulares de dados. O cosmopolitismo jurídico pode ser um elemento especial na discussão de um projeto global de proteção de dados pessoais, ou pelo menos, sobre a necessidade de cooperação e coordenação regulatória internacional, a fim de tutelar o direito à privacidade, independentemente do lugar da coleta ou do tratamento, da nacionalidade do titular ou do agente de tratamento, porquanto a tutela do direito à proteção de dados pessoais está intrinsecamente conectada ao livre desenvolvimento da personalidade humana.

Assim, a mirada cosmopolita pode contribuir para a compreensão e para a refundação da privacidade no século XXI, a partir de uma ética cosmopolita, de uma solidariedade planetária e de um humanismo de interdependência, em razão dos nefastos perigos do capitalismo de vigilância. Por oportuno, não se olvida que tais questões assumem cada vez maior relevância considerando o horizonte de tratamento de dados pela inteligência artificial e a crise do antropoceno diante do advento do pós-humano.

REFERÊNCIAS

AGAMBEN, Giorgio. *Homo sacer***:** o poder soberano e a vida nua. Belo Horizonte: UFMG, 2007.

BAUMAN, Zygmunt. *Vigilância líquida*: diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013.

BECK, Ulrich. *La mirada cosmopolita o la guerra es la paz.* Barcelona: Paidós, 2004.

BECK, Ulrich. *O que é a globalização?* Equívocos do globalismo, respostas à globalização. São Paulo: Paz e Terra, 1999.

BENHABIB, Seyla. *Another cosmopolitanism.* Oxford: Oxford Press, 2006.

BOURG, Dominique. *Le marché contre l'humanité*. Paris: PUF, 2019.

BRADFORD, Anu. The Brussels Effect. In: *NorthWestern University Law Review*, v. 107, n. 1, p. 1-68, 2012. Disponível em: https://scholarship.law.columbia.edu/faculty_scholarship/271. Acesso em: 10 abr. 2023.

BRANDEIS, Louis. WARREN, Samuel. The right to privacy. In: *Harvard Law Review*, v. IV, n. 5, dez., 1890. Disponível em: http://faculty.uml.edu/sgallagher/brandeisprivacy.htm. Acesso em: 10 abr. 2023.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 13 abr. 2023.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6.393, Decisão em Medida Cautelar *ad referendum*. Relatora: Minª. Rosa Weber. Brasília, DF, 24 de abril de 2020. *Diário de Justiça Eletrônica*. Brasília, 27 abr. 2020. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5896399. Acesso em: 20 jul. 2023.

BRUNO, Fernanda. Mapas de crime: vigilância distribuída e participação na cibercultura. In: *Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação*, Brasília, v.12, n. 2, p. 1/-16, maio/ago. 2009. Disponível em: http://www.e-compos.org.br/e-compos/article/viewFile/409/352. Acesso em: 10 abr. 2023.

CAPRA, Fritjof. *A Teia da vida:* uma nova compreensão científica dos sistemas vivos. São Paulo: Cultrix, 1996.

CASTELLS, Manuel. *A Era da Informação*: economia, sociedade e cultura, vol. 3. 3. ed. São Paulo: Paz e Terra, 2002.

CONSELHO DA EUROPA. *Convenção nº 108, do Conselho da Europa, para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais*. Estrasburgo: Conselho da Europa, 1981. Disponível em: https://rm.coe.int/1680078b37. Acesso em: 10 abr. 2023.

COSTA JR. Paulo José da. *O direito de estar só:* tutela penal da intimidade. 2. ed. São Paulo: RT, 1995.

DELMAS-MARTY, Mireille. *Une boussole des possibles: g*ouvernance mondiale et humanismes juridiques. Paris: Collège de France, 2020.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. In: *Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-110, jul./dez. 2011. Disponível em:

https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 10 abr. 2023.

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

FOUCAULT, Michel. *Em defesa da sociedade***:** curso no Collège de France (1975-1976). 4. ed. São Paulo: Martins Fontes, 2005.

FOUCAULT, Michel. *Vigiar e punir:* história da violência nas prisões. 41. ed. Petrópolis: Vozes, 2013.

FRYDMAN, Benoit. *O fim do Estado de Direito*: governar por standards e indicadores. 2. ed. Porto Alegre: Livraria do Advogado, 2018.

GNOATTON, Letícia Mulinari. *A conformidade da Autoridade Nacional de Proteção de Dados aos critérios exigidos pela União Europeia para a concessão de decisão de adequação ao Brasil nos termos do Regulamento Geral de Proteção de Dados.* 2021. 183 f. Dissertação (Mestrado) - Curso de Direito, Universidade Federal de Santa Catarina, Florianópolis, 2021. Disponível em: https://tede.ufsc.br/teses/PDPC1536-D.pdf. Acesso em: 10 abr. 2023.

GREENWALD, Gleen. *Sem lugar para se esconder*: Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. In: BRANCO, Sérgio; TEFFÉ, Chiara de (Org.). *Privacidade em perspectivas*. Rio de Janeiro: Lumen Juris, 2018, p. 85-110.

ISO. *ISO/IEC 27001:2013*. Information technology — Security techniques — Information security management systems — Requirements. Genebra: International Organization for Standardization, 2013.

ISO. *ISO/IEC 27701:2019*. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Genebra: International Organization for Standardization, 2019.

KANT, Immanuel. *A Paz Perpétua*: um projeto filosófico. Petrópolis: Vozes, 2020.

KANT, Immanuel. *Ideia de uma história universal de um ponto de vista cosmopolita*. São Paulo: Martins Fontes, 2010.

MARTINS, Leonardo. *Tribunal Constitucional Federal Alemão:* decisões anotadas sobre direitos fundamentais. Volume 1: Dignidade humana, livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física, igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS, 2016, p. 55-63. Disponível em: https://www.kas.de/c/document_library/get_file?uuid=4f4eb811-9fa5-baeb-c4ce-996458b70230&groupId=268877. Acesso em: 10 abr. 2023.

MAYER-SCÖNBERGER. General development of data protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). *Technology and privacy*: The new landscape. Cambridge: MIT Press, 1997.

MBEMBE, Achille. *La communauté terrestre.* Paris: La Découverte, 2023.

NUSSBAUM, Martha. *La tradición cosmopolita:* un noble e imperfecto ideal. Barcelona: Editorial Planeta S.A., 2020

OCDE. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Paris: OCDE, 1980. Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 10 abr. 2023.

PÉREZ LUÑO, Antonio Enrique. *Los derechos en la sociedad tecnológica***.** Madrid: Editorial Universitas, S.A., 2012.

PESSOA, João Pedro Seefeldt. "*Verás que um filho teu não foge à luta":* a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. Porto Alegre: Fi, 2021. Disponível em: https://www.editorafi.org/102luta. Acesso em: 10 abr. 2023.

PESSOA, João Pedro Seefeldt. *O Efeito Orwell na sociedade em rede*: cibersegurança, regime global de vigilância social e direito à privacidade no século XXI. Porto Alegre: Fi, 2020. Disponível em: https://www.editorafi.org/073orwell. Acesso em: 10 abr. 2023.

PRIVACIDADE hackeada. Direção de Karim Amer; Jehane Noujaim. [S.L]: The Othrs; Netflix, 2019. (113 min.), son., color. Legendado.

RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODRIGUEZ, Daniel Piñero. *O direito fundamental à proteção de dados:* vigilância, privacidade e regulação. Rio de Janeiro: Renovar, 2021.

SALDANHA, Jânia Maria Lopes Saldanha. *Cosmopolitismo jurídico:* teorias e práticas de um direito emergente entre a globalização e a mundialização. Porto Alegre: Livraria do Advogado, 2018.

SALDANHA, Jânia Maria Lopes. Os desafios do "Império Cibernético" na era da aceleração e da informação: Um "sexto" continente de liberdade perfeita ou de controle perfeito. In: TYBUSH, Jerônimo Siqueira; ARAUJO, Luiz Ernani Bonesso de; SILVA, Rosane Leal da. (Org.). *Direitos emergentes na sociedade global:* anuário do Programa de Pós-Graduação em Direito da UFSM. Ijuí: Unijuí, 2013, pp. 173-220.

SARLET, Ingo. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo (coord.). *Tratado de Proteção de Dados Pessoais.* Rio de Janeiro: Forense, 2020.

TEUBNER, Gunther. *Fragmentos constitucionais*: constitucionalismo social na globalização. 2 ed. São Paulo: Saraiva Jur, 2020.

UNIÃO EUROPEIA. *Carta dos Direitos Fundamentais da União Europeia de 2000*. Niza: Jornal Oficial das Comunidades Europeias, 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 10 abr. 2023.

UNIÃO EUROPEIA. Parlamento Europeu. *Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas (Diretiva relativa à privacidade e às comunicações eletrônicas).* Bruxelas: Jornal Oficial da União Europeia, 2002. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32002L0058. Acesso em: 10 abr. 2023.

UNIÃO EUROPEIA. Parlamento Europeu. *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.* Luxemburgo: Jornal Oficial da União Europeia, 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046. Acesso em: 10 abr. 2023.

UNIÃO EUROPEIA. Parlamento Europeu. *Diretiva 97/66/CE do Parlamento Europeu e do Conselho de 15 de dezembro de 1997 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações.* Bruxelas: Jornal Oficial da União Europeia, 1997. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31997L0066. Acesso em: 10 abr. 2023.

UNIÃO EUROPEIA. Parlamento Europeu. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Bruxelas: Jornal Oficial da União Europeia, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679. Acesso em: 10 abr. 2023.

VAIDHYANATHAN, Siva. *A googlelização de tudo (e por que devemos nos preocupar):* a ameaça do controle total da informação por meio da maior e mais bem-sucedida empresa do mundo virtual. São Paulo: Cultrix, 2011.

VÉLIZ, Carissa. *Privacidade é poder:* por que e como você deveria retomar o controle de seus dados. São Paulo: Contracorrente, 2021.

ZUBOFF, Shoshana. *A era do capitalismo de vigilância.* Rio de Janeiro: Intrínseca, 2018.

ZUBOFF, Shoshana. Un capitalisme de surveillance. Disponível em: https://www.monde-diplomatique.fr/2019/01/ZUBOFF/59443. Acesso em: 18 abr. 2023.

Submissão: 14/06/2023. Aprovação: 08/08/2023.