Privacidade no século 21: proteção de dados, democracia e modelos regulatórios

Adriana Veloso Meireles[1]

DOI: 10.1590/0103-3352.2023.41.265909

Introdução

A proteção de dados pessoais reflete um dos principais aspectos da privacidade, um conceito do século 19, que parece impossível de se realizar no século 21, diante da expansão das tecnologias da informação e comunicação. A metáfora espacial da distinção entre o que é público ou privado não é mais aplicável. A interação e o exercício da cidadania deslocam-se da esfera pública para as telas individuais. Sendo assim, a esfera privada, que historicamente foi compreendida como espaço de não intervenção política (liberdade negativa), ganha relevância no debate contemporâneo das ciências sociais.

Os algoritmos que operam as tecnologias digitais permeiam os mais diversos aspectos da vida em sociedade. A teoria do capitalismo de vigilância (ZUBOFF, 2019) aponta como o uso dos dados pessoais desafia as democracias liberais não apenas por influenciar em seus processos políticos e eleitorais, mas principalmente por tornar as experiências privadas em fonte de lucro e vantagem mercadológica de grandes empresas de tecnologia. Diversas vivências cotidianas como as sugestões de conteúdo, a mídia direcionada, dentre outras, são mediadas por estes códigos que analisam, comparam e tratam informações dos mais variados formatos a todo momento de forma automatizada.

1 Doutora em Ciência Política pela na Universidade de Brasília (UnB), Brasília, DF, Brasil. E-mail: dricaveloso@gmail.com

O ponto central é a transformação pela qual passam esses sistemas cibernéticos. Originalmente os códigos computacionais eram simples, escritos para resolver questões específicas, como as calculadoras, por exemplo. Já os algoritmos inteligentes – sejam eles chamados de inteligência artificial ou *machine learning* – são programados para solucionar problemas, interagindo com humanos, assimilando resultados e instruindo-se a partir dos desdobramentos. Entretanto, como "eles não aprendem ou raciocinam como os humanos, isso pode fazer com que seus resultados sejam difíceis de prever e explicar" (TUTT, 2017, p. 87). Como a interação dos algoritmos com humanos varia de acordo com as respostas (*inputs*), não ocorre um treinamento linear, ou seja, cria-se um labirinto de possibilidades. É preciso ter em mente ainda a interação que ocorre entre os próprios algoritmos. As consequências podem ser simples ou complexas: uma sugestão de rota que direciona a uma área da cidade dominada pelo tráfico de drogas, ou um problema (*bug*) no sistema que cause efeitos indesejados, como um simples fechamento de programa sem o trabalho salvo. Não se trata mais de uma exposição aos dispositivos eletrônicos, mas de máquinas "aprendendo o que podem sobre as pessoas, seus atributos e ações passadas, em um esforço para entender suas predisposições e prever ações futuras" (NISSENBAUM, 2009, p. 42). Cada vez mais as pessoas estão submetidas às decisões automáticas dos algoritmos, sem que saibam de que forma foi feita a escolha, seleção ou decisão.

A partir de um modelo de negócios em que as informações pessoais são cedidas de forma "voluntária" por meio da adesão a serviços "gratuitos", o setor de tecnologia consolidou-se. Zuboff descreve este processo como capitalismo de vigilância, "uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais ocultas de extração, previsão e vendas" (ZUBOFF, 2019, p. 1). Neste contexto é preciso considerar que, frequentemente, estas informações são utilizadas para categorizar e discriminar pessoas a partir de critérios muito pouco transparentes. A opacidade do funcionamento desses sistemas torna-se cada vez mais problemática. Para O'Neil (2017) estes algoritmos segregam determinadas informações, privilegiando outras, reproduzindo padrões de preconceito e discriminação de gênero, de raça e de renda, dentre outras, reforçando assim o aprofundamento das desigualdades da sociedade.

Diante disso, as normas jurídicas e instituições não podem mais negligenciar o que ocorre na esfera privada, que se torna cada vez mais política (PATEMAN, 2013). A proteção de dados pessoais deixa de ser uma questão individual e ganha uma dimensão coletiva já que ocorre uma "mudança na natureza da coleta de dados, realizada de forma automatizada e indiscriminada" (NISSENBAUM, 2009, p. 21). É neste contexto em que se discute qual o papel dos Estados em regular o setor de tecnologia e garantir direitos e liberdades individuais, em especial com relação à privacidade e a proteção de dados pessoais. Antes de prosseguir, é importante distinguir estes direitos: enquanto a privacidade está relacionada à intimidade, a proteção de dados está associada às informações pessoais, que podem ser públicas ou privadas (DONEDA, 2019).

Ao longo do texto, argumenta-se que os modelos regulatórios adotados por diferentes regiões refletem valores sociais e éticos intrínsecos ao próprio sistema democrático. Visões sobre liberalismo, direitos humanos, o exercício da liberdade de expressão, da cidadania, e a própria democracia manifestam-se nas diversas abordagens normativas (MIGUEL, 2014). É preciso enfatizar que regular não quer dizer restringir, ou dificultar o surgimento de inovações tecnológicas. Significa traçar diretrizes e parâmetros para que determinado setor atue com transparência para com a sociedade e de forma compatível com a democracia e o Estado de direito. Todos os setores da economia estão sujeitos a algum nível de regulação e o mercado de tecnologia não pode ser exceção.

Realizadas essas breves considerações, sublinha-se que o artigo está dividido em quatro partes, além desta introdução que contextualiza as questões centrais debatidas nas próximas páginas. Inicia-se resgatando o histórico do debate sobre proteção de dados a partir da perspectiva da União Europeia, para analisar, em seguida, o Regulamento Geral sobre a Proteção de Dados (RGPD), em vigor desde 2018. Ao avaliar aspectos normativos da proteção de dados pessoais, busca-se identificar questões que impactam as democracias contemporâneas, como o uso de informações pelos Estados, a tomada de decisões automatizadas pelos algoritmos, polêmicas como a remoção de conteúdo online, dentre outras controvérsias que refletem valores e visões sobre cidadania e exercício de direitos e liberdades.

Na segunda parte do artigo, o foco desloca-se para os marcos normativos dos Estados Unidos, onde se encontram as grandes corporações de tecnologia,

conhecidas pelo acrônimo GAFAM (Google, Apple, Facebook, Amazon e Microsoft). Marcada por uma diversidade de leis, que variam de acordo com regiões do país, trata-se de uma legislação com ênfase nos direitos dos consumidores e da livre concorrência. Além disso, a mesma foi fortemente influenciada pelos ataques de 11 de setembro de 2001, em Nova Iorque. Este acontecimento levou à suspensão de regulamentos sobre proteção de dados pessoais e privacidade em nome do combate ao terrorismo.

Na terceira parte, explora-se a lei brasileira de proteção de dados (LGPD) aprovada em 2018. Destaca-se seu histórico a partir do debate em torno do Marco Civil da Internet e a tramitação dos projetos de lei sobre proteção de dados pessoais no Congresso Nacional. Em seguida, são enfatizadas as alterações realizadas na lei, com destaque para o amplo poder de uso e compartilhamento de dados pessoais pelo Estado.

A metodologia adotada é uma análise comparada entre os principais aspectos e controvérsias destas normas com relação a três categorias de atores: o Estado, o setor privado e os cidadãos (KING; KEOHANE; VERBA, 1994; LATOUR, 2012). Como resultado sintetiza-se em um quadro comparativo as principais correlações identificadas, sublinhando como cada uma das três abordagens trata de temas contemporâneos relacionados aos direitos de proteção de dados pessoais, tais como: não estar sujeito a automatização de decisões realizadas por máquinas, não ter dados compartilhados entre autoridades, ser informado sobre o uso de seus dados, delimitar a finalidade do uso dos dados e o direito de ser removido de bancos de perfis (*profiling*). A partir deste diagnóstico, pode-se concluir que as principais divergências são em relação à responsabilidade das plataformas intermediárias (setor privado), o acesso aos dados pelo poder público e os direitos dos titulares de dados.

O Regulamento Geral Sobre a Proteção de Dados

O debate sobre proteção de dados pessoais na União Europeia tem como marco histórico a Convenção de Estrasburgo, ocorrida em 1981. O documento que resultou do encontro demonstra a preocupação com o tratamento de dados pessoais de forma automatizada e as consequências de decisões tomadas por máquinas para a sociedade, além de diferenciar o tratamento de dados

pessoais realizado pelo setor privado e o realizado pelos Estados, incluindo autoridades policiais e judiciárias.

Neste contexto, outro importante documento é "relativo à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matérias criminais" (UNIÃO EUROPEIA, 2008). Essa diretiva tem como um de seus objetivos proteger os direitos e liberdades fundamentais, em particular o direito à privacidade, "quando para efeitos de prevenção, investigação, detenção ou repressão de infrações penais, ou execução de sanções penais, os dados pessoais são transmitidos entre as autoridades dos Estados membros do bloco" (UNIÃO EUROPEIA, 2008). Observa-se a presença de uma preocupação distinta, com foco na prevenção do vazamento de informações entre fronteiras e uma regulação da atuação policial e judicial.

Em 2009, a partir do Tratado de Lisboa, o direito à proteção de dados pessoais tornou-se um direito fundamental no âmbito da União Europeia. Mas é em 2012 que o Comitê Europeu de Proteção de Dados propõe a reforma de todas essas regras com o objetivo de aumentar o controle das pessoas sobre os próprios dados e diminuir a burocracia envolvida em seu tratamento. O resultado desta reforma, que inclui também uma revisão da diretiva de dados pessoais no âmbito das investigações policiais e judiciais, é o Regulamento Geral sobre a Proteção de Dados (RGPD) (UNIÃO EUROPEIA, 2016).

Dentre as principais mudanças, destaca-se uma ênfase à necessidade do consentimento explícito para o uso e tratamento de dados pessoais. A regulação garante ainda uma série de direitos para os titulares dos dados, explorados adiante. Além disso, cria mecanismos de conformidade e responsabilização para empresas e governos e prevê sanções e multas administrativas.

Importante pontuar que enquanto os primeiros documentos possuíam um caráter sugestivo, o RGPD obriga todos os Estados da União Europeia a cumprirem suas regras. O texto define dado pessoal como "toda informação relativa a uma pessoa singular identificada, ou identificável" (UNIÃO EUROPEIA, 2016). Diferencia tipos de dados pessoais, tais como: dados genéticos, dados biométricos e dados relativos à saúde. Dentre as categorias de dados há aqueles considerados especiais, ou sensíveis, que englobam informações pessoais que revelam a origem racial ou étnica, as opiniões políticas, as convicções religiosas e políticas, dados relativos à saúde, ou dados relativos à orientação sexual

de uma pessoa. O tratamento destes dados é proibido a não ser que a pessoa forneça o consentimento explícito (com exceções previstas como em outros artigos que tratam de interesse público e segurança, em sua maioria). A relevância é justamente a existência de uma categoria diferenciada de dados sensíveis, que busca conter o fenômeno da discriminação algorítmica.

Por sua vez, a definição de consentimento do titular dos dados refere-se à "manifestação de vontade, livre, específica, informada e explícita, pela qual o titular aceita, mediante declaração, ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam tratados" (UNIÃO EUROPEIA, 2016). O consentimento explícito é um dos grandes avanços da regulação, pois impacta diretamente no formato dos termos de uso dos programas e aplicativos digitais. O efeito direto dessa nova orientação é observado nas atuais "retratações de responsabilidade (*disclaimers*)" contidas em sites e aplicativos (BIONI, 2019). Importante notar ainda que surge uma margem de negociação, já que as pessoas podem optar em geral por compartilhar apenas os dados necessários para o uso do serviço e renunciar às opções de publicidade e personalização. Trata-se da aplicação de preferências de permissão do uso de dados (*opt in e opt out*).

Ressalta-se ainda que o regulamento já parte da premissa de que os dados são coletados e busca atuar na etapa seguinte que é justamente o que é conhecido no jargão do setor como mineração de dados. No âmbito do tratamento de dados, o regulamento define uma importante prática do setor: a construção de perfis (*profiling*).

Essa atividade é um dos aspectos que geram mais controvérsias sobre os possíveis impactos na sociedade quando o tema é a proteção de dados pessoais. O conjunto de técnicas para a criação de perfis – com dados biométricos e reconhecimento facial – já é amplamente utilizado em diversos setores, que vão de instituições financeiras a planos de saúde, passando pelo varejo, entretenimento e até mesmo pelos órgãos policiais e jurídicos. Portanto, esta prática é uma das que mais influenciam o exercício da cidadania e dos direitos, já que as pessoas são agrupadas de acordo com determinadas características. A construção de perfis tende a reproduzir padrões de discriminação e categorias que aprofundam as desigualdades, ao privilegiar pessoas que apresentam determinados dados em detrimento de outras (O'NEIL, 2017). Somado a todos

estes fatores não há transparência sobre como esses algoritmos operam, sendo ainda mais problemático quando tomam decisões, de forma automatizada, que influenciam a vida das pessoas.

Há uma pluralidade de atores que trabalham com o tratamento de dados pessoais e cada um deles possui obrigações e responsabilidades específicas. Os controladores, ou responsáveis pelo tratamento, são aqueles que determinam os propósitos e meios de processar dados pessoais. Já os operadores, ou subcontratantes, são aqueles envolvidos no processamento de dados pessoais em nome dos controladores, assim como os receptores e terceiros.

Para diferenciar operadores e controladores, é necessário identificar as finalidades e meios de processar os dados, ou seja, quais dados são coletados e por qual motivo. O que será feito com eles? O ator que define isso é o responsável pelo tratamento, ou controlador, e os que o auxiliam neste exercício são os operadores, recipientes ou terceiros. Portanto, os responsáveis pelo tratamento, ou controladores, possuem mais responsabilidades e obrigações.

Todos estes atores que tratam dados pessoais precisam contar com um encarregado da proteção de dados, um *Data Protection Officers (DPO)*. Estes agentes são responsáveis por informar e orientar sobre as práticas necessárias para cumprir o regulamento.

Por fim, é importante destacar o papel da autoridade de dados. A regulação determina que cada país tenha uma autoridade de controle independente do governo, responsável pela fiscalização, aplicação das regras e pela defesa dos direitos dos titulares de dados, com poderes de investigação. O regulamento é assertivo em destacar a independência da autoridade, incluindo a financeira. A autoridade pode ser uma única agência, ou autarquia, ou um conjunto de instituições, como funcionam a rede de proteção aos consumidores no Brasil (Procons), e cada Estado membro tem autonomia para definir seu arranjo nacional.

Dentre os oito princípios de proteção de dados, são relevantes para o debate aqueles referentes ao consentimento e a privacidade por padrão (*privacy by design*). Ao determinar que o consentimento deve ser específico, informado e não ambíguo, a regulação enfatiza a necessidade da alteração dos termos de uso para modelos mais diretos e objetivos, tornando indispensável que o consentimento seja dado por meio de uma declaração, ou ação afirmativa.

Outra transformação fundamental proposta pela regulação é a privacidade por padrão (CAVOUKIAN, 2011). Este conceito destaca que o direito à privacidade e a proteção de dados pessoais não deve se limitar às medidas regulatórias e normas jurídicas. É necessário que os sistemas sejam voltados para a necessidade das pessoas e seus direitos.

A norma estabelece uma série de direitos dos titulares de dados. Dentre eles o de solicitar e adquirir acesso aos seus dados pessoais a qualquer momento. A legislação garante ainda que as pessoas possam contestar e/ou restringir a coleta e tratamento de seus dados. Este direito é exercido quando o titular de dados não quer que suas informações componham bancos de dados de perfis (*profiling*), ou de marketing direcionado. Além disso, os titulares de dados podem solicitar a retirada de informações quando os propósitos da coleta já não mais se justificam, ou são irrelevantes, com exceção para informações de interesse público.

Já o direito a oposição permite que qualquer pessoa solicite aos controladores que seus dados deixem de ser tratados. A principal diferença entre o direito de restrição e o de oposição é que, no primeiro caso, os controladores continuam coletando alguns dados, mas no segundo, a cessão deve ser imediata. A regulação também prevê o exercício do direito de reparação, que ocorre quando o titular dos dados requer que suas informações sejam retificadas, em caso de inconsistências.

Um dos direitos mais controversos garantidos pelo RGPD é o de solicitar a remoção, ou apagamento de determinado conteúdo, implícito no direito ao controle dos próprios dados. A questão ganhou destaque nos debates sobre o "direito ao esquecimento". A disputa encerrou-se em 2014, quando o Tribunal de Justiça da União Europeia decidiu que mecanismos de busca na internet são responsáveis pelo processamento de informações pessoais que aparecem em páginas de terceiros. A decisão determinou que as plataformas intermediárias têm responsabilidade na propagação de informações na rede e abriu precedentes para a remoção de conteúdo em casos específicos, como, por exemplo, fatos irrelevantes, ocorridos há muito tempo, ou considerados inadequados. O caso ficou conhecido como o direito ao esquecimento, entretanto considera-se que o termo não é o mais adequado para descrevê-lo. Diz respeito muito mais à desindexação dos mecanismos de busca do que seu

apagamento, ou remoção de determinado conteúdo da internet. Novamente existem exceções: as solicitações devem considerar o exercício do direito à liberdade de expressão e de informação, do interesse público, ou para fins estatísticos. Portanto, não se trata de um direito ao esquecimento, mas o direito de solicitar a remoção de um dado pessoal específico e de forma justificada.

A regulação estabelece ainda o direito de cada pessoa não estar sujeita à uma decisão tomada por processos automáticos, permitindo tal prática apenas diante de consentimento explícito, ou contrato específico para esta finalidade. Sendo assim, os controladores são obrigados a informar sobre o prazo que os dados serão armazenados, os motivos pelos quais precisam daquelas informações e se os dados serão submetidos a decisões automatizadas.

O titular de dados que considerar ter sofrido dano pode acionar a Autoridade e solicitar indenização do controlador, ou operador que violou seus direitos. Estas agências podem estabelecer multas de até 20 milhões de euros, ou até 4% do total do faturamento anual mundial da empresa, o que for maior. O valor das multas deve ser proporcional, variando de acordo com a natureza, gravidade e duração da infração.

Desde que entrou em vigência, o RGPD foi utilizado em diversos casos, dentre os quais o mais conhecido é o do *Cambridge Analytica*, que obteve dados de milhões de pessoas do Facebook, utilizando as informações em campanhas políticas como a do presidente norte-americano Donald Trump, e a da saída do Reino Unido da União Europeia, conhecido como *Brexit*.

Somente neste caso, a Autoridade de proteção de dados da Inglaterra, o *Information Commissioner's Office* (ICO), multou o Facebook em 500 mil libras, apenas pelo vazamento de dados dos britânicos. Já a Itália, no mesmo caso, multou a empresa em 10 milhões de euros. Mas foi na sede da companhia, nos Estados Unidos, o valor mais significativo: 5 bilhões de dólares em multa aplicada pela Comissão Federal de Comércio (*Federal Trade Comission*).

Devido a todos estes fatores, é possível concluir que a abordagem da União Europeia com relação à proteção de dados pessoais é focada nos direitos dos cidadãos, na conformidade do setor privado e dos governos locais com o regulamento. Ao determinar Autoridades Nacionais com poderes punitivos e investigativos, a regulação acaba por desonerar o poder judiciário de decidir sobre questões já determinadas e acordadas. Resultado de ao menos trinta

e cinco anos de reflexão, trata-se do marco regulatório mais relevante quando o tema é a privacidade e a proteção de dados pessoais. Sendo assim, o RGPD reflete uma compreensão do Estado enquanto mediador dos conflitos e interesses presentes na sociedade, regulando a atuação do setor privado para garantir direitos de seus cidadãos.

Marcos normativos dos Estados Unidos

Primeiramente, é preciso salientar que, nos Estados Unidos, o debate sobre a proteção de dados pessoais tem uma abordagem bastante distinta da União Europeia, a começar pelos próprios termos utilizados. O tema é tratado como privacidade de dados (*data privacy*) não como proteção de dados. Em segundo lugar, observa-se uma atuação da perspectiva dos direitos do consumidor e do conjunto de leis concorrenciais (*antitruste*).

A terceira premissa importante para tratar do tema da privacidade e proteção de dados nos Estados Unidos são os ataques de 11 de setembro de 2001, que influenciaram diretamente na suspensão de legislações sobre estes temas, em nome da vigilância para combater a guerra contra o terrorismo. Justamente por isso, boa parte do marco regulatório do país data da década de 1990, anterior a interatividade da web.

Nos Estados Unidos, não há uma lei geral de proteção de dados, mas uma série de regulações distintas, até mesmo algumas cuja finalidade original não é a proteção de dados, mas questões envolvendo menores de idade, saúde e crédito, por exemplo. Outras leis remetem à privacidade diretamente, mas, em sua maioria, buscam regular setores econômicos específicos como o sistema financeiro, a comunicação eletrônica e o sistema de saúde. O caminho legislativo não é preventivo, mas reativo, ou seja, as leis surgem após a solução de casos jurídicos específicos (MOVIUS; KRUP, 2009). O conjunto de normas do sistema judiciário privilegia o comércio e a segurança do Estado em primeiro lugar, caracterizando-se como um modelo extremamente neoliberal, em que o Estado intervém muito pouco, atuando de forma discreta na proteção dos direitos individuais (COBB, 2016). De fato, quando busca proteger os cidadãos, faz isso tratando-os como consumidores.

Não existe uma agência ou autoridade nacional responsável pela proteção da privacidade ou proteção de dados. Estes temas são tratados, ou pela

justiça, ou pela Comissão Federal de Comércio (*Federal Trade Commission)*. A agência é responsável pela execução de políticas de privacidade e segurança no país, por produzir uma série de diretrizes sobre políticas de privacidade e por multar empresas que ferem a legislação.

As principais normas que versam sobre a defesa da concorrência nos Estados Unidos são o *Sherman Act,* de 1890 e o *Clayton Act* de 1914. O primeiro tornou ilegal contratos que restringiam o comércio com o intuito de formar monopólios. Já o segundo, regulou a fixação de preços, negociações casadas e a aquisição de empresas concorrentes. Estas leis tinham como foco a regulação do mercado, não necessariamente os consumidores, mas foram responsáveis pela criação da Comissão Federal de Comércio.

Os direitos do consumidor levariam ainda alguns anos para se conformarem, representando um segundo aspecto da regulação do livre mercado. Trata-se de um conjunto de normas que buscam garantir o direito em ter um comércio justo, informações precisas e opções de mercado. Nos Estados Unidos, o marco histórico dos direitos do consumidor é o discurso do presidente John Kennedy, em 1962, no qual ele apresenta quatro direitos básicos: à segurança, à informação, à livre escolha e a ser ouvido. Estes direitos consolidam-se a partir de uma série de legislações como, por exemplo, a *Fair Debt Collection Practices Act*, de 1977, que busca reduzir o abuso na coleta de dívidas.

Além destas legislações comerciais, existem leis que tratam diretamente de proteção de dados e privacidade. Uma delas é o *Fair Credit Reporting Act* (FCRA), de 1970, editada para promover a justiça, a exatidão e privacidade da informação do consumidor. De forma semelhante, há o *Financial Services Modernization Act,* de 1999. Esta e outras normas são voltadas para o cadastro positivo ou negativo – relativos ao recebimento ou negação de crédito das instituições financeiras. Estes marcos regulatórios tratam da privacidade de forma tangencial, buscando regular o mercado.

O tema é encaminhado de forma mais direta pelo *Federal Privacy Act*, de 1974, que normatiza as bases de dados do governo e que garante que a privacidade é um direito. De forma semelhante, destaca-se a *Electronic Communications Privacy Act*, de 1986, que estendeu às tecnologias digitais as mesmas restrições aplicadas à interceptação de comunicações telefônicas.

A fragmentação da legislação faz com que o sistema judiciário seja acionado com frequência (COBB, 2016). No âmbito da Suprema Corte dos Estados Unidos foram julgadas várias ações sobre privacidade. O entendimento recorre à quarta emenda da constituição, que garante "o direito do povo à inviolabilidade de sua pessoa, casas, papéis e haveres", defendendo em mais de uma ocasião que ela se aplica ao direito à privacidade. Entretanto a privacidade, ao ser abordada por várias legislações específicas, é garantida em uma série de situações, mas a despeito do entendimento da Suprema Corte, não é um direito universal, nem é um direito como na abordagem europeia, em que a privacidade é um direito por padrão.

Na década de 1990, quando a internet se comercializava, foram editadas uma série de leis com o objetivo de regulá-la. Dentre elas, destaca-se a *Communications Decency Act*, de 1996, feita com o propósito de combater a pornografia *online*. Esta legislação abre precedentes para a controvérsia sobre a responsabilização das plataformas intermediárias e a remoção de conteúdo da internet, especialmente a partir de sua seção 230, que determina que os provedores não podem ser responsabilizados pela publicação de terceiros. Ocorre que essa é uma lei anterior à indexação de conteúdo por buscadores.

Esta legislação é resultado justamente de uma controvérsia criada em torno de duas decisões judiciais contrárias à remoção de conteúdo difamatório na internet (ZUBOFF, 2019, p. 109). Na prática, ao eximir os intermediários de responsabilidade, ela possibilitou o surgimento de práticas como a criação de contas falsas em redes sociais, a disseminação de conteúdo de ódio, o uso de robôs e outros fenômenos contemporâneos, que não existiam em 1996. Este tema está relacionado à proteção de dados pessoais justamente porque este marco regulatório estabelece a jurisprudência adotada em boa parte das normatizações, protegendo as grandes empresas intermediárias e não os direitos (como a privacidade e até mesmo a liberdade de expressão). A defasagem da legislação tornou-se tão discrepante que, em junho de 2023, estão marcados três julgamentos na Suprema Corte dos Estados Unidos com o objetivo de revisar a norma (CAPOZZI, 2023).

Ainda na década de 1990, foi aprovado o *Children's Online Privacy Protection Act* (COPPA), que passou a vigorar a partir dos anos 2000. Criada para salvaguardar a privacidade de menores de 13 anos, a lei estabelece uma

série de requerimentos que sites e aplicativos precisam adotar para a proteção dos dados desse público específico. Além de definir termos técnicos tais como informação pessoal, coleta e tratamento de dados, operadores e controladores, a lei introduz o conceito de "conhecimento real". A COPPA define não apenas a necessidade do consentimento dos responsáveis devido à ausência de conhecimento real por parte de menores de idade, como determina a adoção de algumas práticas importantes. A primeira delas é a necessidade de criação de políticas de privacidade descrevendo quais informações são coletadas, com qual objetivo, se os dados são compartilhados com terceiros, e quais são os direitos dos responsáveis. Em nível federal, a COPPA é o que há de mais avançado em termos de proteção de dados e privacidade nos Estados Unidos.

Justamente por isso, um grupo de trabalho da Comissão Federal de Comércio enviou um relatório ao Congresso, em 1998, sugerindo que alguns dos procedimentos e direitos previstos na COPPA fossem estendidos a todas as pessoas. Além disso, o texto sugeria estabelecer padrões para a coleta e tratamento de dados e a ampliação da capacidade da agência para atuar nas violações (ZUBOFF, 2019, p. 112). Em suas conclusões, os comissários destacaram que apesar da maioria das empresas estarem cientes da necessidade de proteger a privacidade de seus consumidores, muitos não haviam implementado as medidas de conformidade, ou seja, atuavam sem considerar as recomendações da agência.

A proposta chegou a ser discutida no Congresso, entretanto "meses de debate sobre privacidade simplesmente desapareceram da noite para o dia" (ZUBOFF, 2019, p. 112), após os ataques de 11 de setembro de 2001. O incidente foi responsável por colocar a questão da segurança em primeiro plano, levando à edição do controverso *Patrioct Act,* cerca de um mês e meio após os ataques. Esta legislação aumentou a capacidade de vigilância do Estado, seja por meio da ampliação de buscas e apreensões, ou grampos judicialmente autorizados (MOVIUS; KRUP, 2009). Além disso, o *Patrioct Act* tinha como objetivo interceptar comunicações terroristas, o que levou às agências de segurança do país a focarem em um campo ainda pouco explorado: a internet. Os resultados dessa legislação só revelaram sua real dimensão mais de uma década depois, quando Edward Snowden divulgou as práticas de vigilância em massa da Agência Nacional de Segurança estadunidense, em 2013.

Portanto, desde os ataques de 11 de setembro de 2001, a prioridade do governo tornou-se a segurança, o que abriu espaço para que empresas realizassem um forte *lobby* para que a privacidade e proteção de dados pessoais não fosse objeto de regulação nos anos seguintes (ZUBOFF, 2019). Com isso o sistema judiciário começou a ser acionado cada vez com mais frequência.

Neste contexto, é importante destacar duas ações que estabeleceram jurisprudência sobre o direito concorrencial e à privacidade. Em 1997, "o governo americano alegou que a Microsoft utilizava sua tecnologia para manter um monopólio ilegal" (BUTTS, 2010, p. 276). O sistema operacional da empresa, o Windows, era acompanhado do navegador Internet Explorer, o que prejudicaria outras companhias, à época sobretudo o Netscape, que liderava este mercado. A iniciativa do governo foi muito criticada a partir do argumento de que o excesso de regulação nas novas tecnologias impediria inovações (FRIEDMAN, 1999). Em 2001, a Microsoft ganhou a ação abrindo precedentes para o entendimento de que empresas de tecnologia não abusam de seu poder econômico ao direcionar as pessoas a consumirem seus próprios produtos.

Por outro lado, este não é o entendimento das cortes europeias. Um caso semelhante expõe os diferentes pontos de vista. Em 2013, o Google foi alvo de investigação de órgãos de defesa dos consumidores dos Estados Unidos e da União Europeia "por favorecer seus próprios produtos nos resultados de busca em detrimento dos rivais" (LOPES-SALDANHA; PITTALUGA-HOFFMEISTER; ROSSATTO-BOHRZ, 2018, p. 77). Entretanto, o parecer das cortes foi divergente. No primeiro caso, a Comissão Federal de Comércio americana considerou que "não houve prejuízos à livre competição na manipulação dos resultados de buscas pelo Google" (LOPES-SALDANHA; PITTALUGA-HOFFMEISTER; ROSSATTO-BOHRZ, 2018 p.77). Já a Comissão Europeia condenou, em 2017, a empresa a "pagar uma multa de 2,42 bilhões de euros, à época a maior condenação da história que envolveu gigantes da internet" (LOPES-SALDANHA; PITTALUGA-HOFFMEISTER; ROSSATTO-BOHRZ, 2018 p. 77), por favorecer os próprios produtos. Deve-se considerar que a jurisprudência está em constante disputa. Nos Estados Unidos, ocorrem investigações por violações das leis de antitruste, que podem obter desdobramentos diferentes. Entretanto, deve-se questionar se a diluição das cinco *big techs* – GAFAM – em vinte ou trinta empresas, realmente é a solução, já que a quebra

do monopólio é apenas um dos aspectos do impasse. Além disso, seriam mais companhias, mas sob o controle dos mesmos operadores financeiros.

Outra ação judicial relevante para o debate sobre privacidade e proteção de dados pessoais nos Estados Unidos foi a disputa entre a Apple e o FBI (*Federal Bureau of Investigation*), ocorrida entre 2015 e 2016. A empresa era pressionada pelas autoridades a fornecer dados sobre troca de mensagens privadas entre as pessoas. Diante disso, adotou a criptografia de ponta a ponta para estas aplicações. Desta forma, blindou-se de ordens judiciais de quebra de sigilo ao alegar que não possuía acesso às mensagens, já que, em teoria, o conteúdo não fica armazenado na nuvem, sendo entregue diretamente aos destinatários finais. A disputa resultou na determinação de que a empresa não devia quebrar o sigilo de seus consumidores.

Por fim, contrariando o argumento de que regular a proteção de dados e garantir a privacidade abafa a inovação tecnológica, está o caso da Califórnia (COBB, 2016). Berço do Vale do Silício, é o estado americano detentor das legislações mais avançadas em termos de proteção de dados e privacidade. Foi o primeiro a editar uma lei sobre notificação em caso de violações de segurança, em 2003. Também foi pioneiro em reagir sobre a onipotente vigilância do Estado aprovando o *The California Electronic Communications Privacy Act*, em 2016, que limita a atuação do governo na interceptação de comunicações pessoais.

Além disso, em 2018, o estado aprovou o *California Consumer Privacy Act*, legislação que se aproxima do RGPD europeu. Com vigência a partir de 1º de janeiro de 2020, este marco normativo tem como objetivo informar quais dados pessoais são coletados, se são comercializados e para quem. Com isto permite que as pessoas neguem a comercialização de seus dados pessoais e acessem quais informações são coletadas. Por fim, estabelece que os consumidores solicitem o apagamento de informações pessoais e que não sejam discriminados por exercerem seu direito à privacidade.

Outros estados americanos também possuem leis locais sobre violação de privacidade e proteção de dados pessoais. Entretanto, a *California Consumer Privacy Act* é considerada a legislação estadunidense que mais se aproxima do modelo europeu. Sua entrada em vigor retomou debate sobre uma lei nacional exclusivamente sobre privacidade, até o momento inexistente.

Por toda a complexidade dessa série de legislações, que ainda se confrontam com regras estaduais, pode-se concluir que o marco regulatório americano não conseguiu alcançar um balanço entre a garantia dos direitos individuais e os interesses do comércio, abrindo brechas para práticas consideradas ilegais na Europa, especialmente em termos de vigilância. Este modelo confunde a segurança da informação com a proteção de dados pessoais, portanto privilegia a segurança em detrimento de direitos e liberdades individuais. Sendo assim, o Estado adquire um papel de garantidor de realização de exceções em nome de um bem maior, além de regular o setor privado de forma reativa, ou seja, muitas vezes tardiamente. Portanto, o padrão de autorregulação do setor de tecnologia e as constantes disputas em torno dos padrões de funcionamento da internet apontam para o fato de que as controvérsias estão longe de alcançar um consenso.

Privacidade e proteção de dados pessoais no Brasil

O debate sobre proteção de dados pessoais no país ganhou relevância a partir de 2007 no contexto da construção do Marco Civil da Internet (DONEDA, 2019). À época, parte da sociedade civil mobilizou-se contra um projeto de lei, cuja proposta regulamentava a internet no país pela perspectiva criminal. Como resultado direto das manifestações em torno desta proposta, foi criada, em 2009, uma consulta pública na *web*, promovida pelo Ministério da Justiça, para debater os direitos dos usuários da internet no país. Observa-se a convergência entre forma e conteúdo, ou seja, era um debate sobre a internet ocorrendo na *web*, com o mínimo de moderação por parte dos organizadores.

Em 2015, o Ministério da Justiça seguiu os mesmos passos para promover o debate sobre proteção de dados. Fortemente inspirado na legislação europeia, o projeto de lei obteve rápida tramitação no legislativo, impulsionado justamente pela entrada em vigor do regulamento europeu. Em 29 de maio de 2018, dias após a entrada em vigor do RGPD, a Câmara dos Deputados aprovou o projeto da Lei Geral de Proteção de Dados (LGPD), que não sofreu alterações no Senado Federal e seguiu para sanção presidencial.

Entretanto, a legislação sofreu alterações – por meio de vetos e decretos – que modificaram profundamente sua estrutura inicial. Boa parte de seus fundamentos, princípios e definições são idênticos ao regulamento europeu

descrito na primeira parte do artigo, sendo desnecessário repeti-los. A seguir, destacam-se os principais aspectos da legislação brasileira, suas semelhanças e diferenças do modelo europeu, assim como suas anomalias.

Em primeiro lugar, é preciso sublinhar a questão do tratamento de dados pelo poder público e para atividades de investigação e repressão de infrações penais. A lei brasileira diferencia o tratamento de dados pelo poder público daquele realizado pelos controladores e operadores privados (MEIRELES, 2023). Importante destacar que o RGPD não faz essa diferenciação, ou seja, todos atores estão sujeitos à legislação. Na prática, a lei brasileira coloca o governo em uma categoria de exceções, o que abre precedentes para o uso indevido dos dados por parte do próprio Estado.

A norma brasileira prevê o "uso compartilhado de dados" entre os entes do poder público, possibilitando a distribuição de informações pessoais sensíveis entre os órgãos da administração. Um exemplo: a foto da carteira de motorista pode ser utilizada para reconhecimento facial em espaços públicos, por agentes de segurança. Isso tudo sem que o titular de dados seja comunicado. Com isso, permite que as informações sejam utilizadas para novas finalidades, até mesmo a criação de perfis, sem o consentimento das pessoas, contrariando os próprios princípios contidos na lei (finalidade, adequação, necessidade, dentre outros).

Antes de prosseguir, é preciso enfatizar dois decretos que incidem diretamente na LGPD. O primeiro deles (Decreto nº 8.789), publicado em 2016, dispõe sobre o compartilhamento de bases de dados na administração pública federal. Na prática, ele permite a distribuição de uma série de informações cadastrais entre os órgãos do poder executivo, colocando como exceção apenas dados sob sigilo fiscal. O segundo, expedido em 2019, refere-se ao Cadastro Base do Cidadão (Decreto nº 10.046), que reunirá mais de cinquenta bancos de dados de diferentes órgãos do poder público. O decreto se diz em conformidade com a lei geral de proteção de dados, porém conta com expressões tais como "atributos biográficos" e "atributos biométricos", termos inexistentes na LGPD. De fato, essa nomenclatura indica que o uso de dados sensíveis é ignorado, assim como o princípio da finalidade, que limita a coleta de dados.

Outra brecha da norma brasileira é com relação à comunicação às autoridades em caso de violação. O RGPD determina que, em caso de falha nas

medidas de segurança, os agentes devem notificar as autoridades em até 72 horas após o ocorrido. Já o texto brasileiro declara que as violações devem ser informadas em "prazo razoável", que será definido pela Autoridade Nacional de Proteção de Dados (ANPD), órgão que é citado cinquenta e três vezes no texto da legislação. Inicialmente a agência esteve vinculada à Presidência da República, mas, a partir da Medida Provisória 1.124/2022, tornou-se uma autarquia independente, como elaborada inicialmente.

Ainda assim, a lei brasileira garante, como o RGPD, uma série de direitos aos titulares de dados. Entretanto, falha em um importante quesito com relação às decisões automatizadas, ou seja, aquelas realizadas por algoritmos. A norma brasileira não garante que a revisão dessas decisões seja realizada por pessoas. Na prática, significa que se uma pessoa solicitar a revisão de uma decisão automatizada, esta poderá ser feita justamente de forma automatizada, contrariando o princípio do consentimento.

Nesta mesma linha, alteraram-se as regras para o encarregado de proteção de dados. O texto original determinava que a função fosse exercida por uma pessoa "natural". A redação final suprime essa palavra, com isto os controladores e o próprio poder público podem indicar pessoas jurídicas para o exercício da atividade, o que retira a responsabilidade de que os agentes tenham em seu quadro interno uma pessoa encarregada da função.

Outra controvérsia da lei brasileira é a exceção para o tratamento de dados para atender aos "interesses legítimos" do controlador. Além do mais, Zuboff (2019) alerta que este recurso "oferece uma oportunidade de passar por cima dos novos marcos regulatórios" (ZUBOFF, 2019, p. 456) já que pode ser interpretado como "o direito de empreender em determinada atividade econômica, ou até mesmo exercer a liberdade de expressão" (ZUBOFF, 2019, p. 456). A legislação europeia não abre essa exceção, o que torna a interpretação sobre legítimo interesse dos controladores alvo de contestações judiciais. Além disso, adota o regime de *notice and take down* para crimes específicos já previstos em lei como racismo, xenofobia, dentre outros tipos de discurso de ódio.

É neste contexto que ocorre a grande polêmica sobre moderação e remoção de conteúdo. O artigo 19 do Marco Civil da Internet determina que as empresas não podem ser responsabilizadas por conteúdos publicados por terceiros. A legislação brasileira compreende a responsabilidade das empresas

como residual, ou seja, somente se as plataformas de conteúdo descumprirem uma ordem judicial (SANTOS, 2020). Com isto as empresas retiram conteúdo, ou suspendem contas de acordo com as suas políticas e a seu próprio tempo. Muitas vezes após a ocorrência de fatos graves, como ficou demonstrado na invasão do Capitólio em 6 de janeiro de 2021, nos Estados Unidos, e em sua versão brasileira de 8 de janeiro de 2023. De forma semelhante com o que ocorre nos Estados, onde a seção 230 está em revisão pela Suprema Corte, no Brasil, o STF (2023) discute justamente a constitucionalidade do artigo 19 do Marco Civil da Internet, dentre outros aspectos da lei, que se demonstrou ineficaz na prevenção da disseminação de conteúdo falso e abriu brechas para a perpetuação de crimes contra o próprio Estado.

Observa-se ainda a ausência da privacidade por padrão como um princípio da lei, que afeta diretamente decisões técnicas e organizacionais dos setores que atuam no tratamento de dados pessoais no país. De fato, o termo "privacidade por padrão" não está diretamente mencionado em nenhum artigo da lei brasileira.

Sendo assim, pode-se concluir que mesmo originalmente elaborada nos moldes do RGPD, a redação final da lei brasileira tornou-se um marco regulatório mais próximo do estadunidense, no sentido de conferir muito poder ao Estado sobre a gestão dos dados. Certamente deve-se considerar que o Estado deve ter o interesse presumido da coletividade em sua atuação. Por outro lado, é preciso levar em conta a questão do compartilhamento de dados pessoais pelo poder público, que fere princípios como o de reutilização de dados, limitação do tratamento, dentre outros. Outra semelhança entre estes modelos regulatórios é a dependência do sistema judicial. Este fato ficou evidente na atuação da Corte eleitoral brasileira no pleito de 2022, determinando e estabelecendo limites sobre o que as campanhas poderiam fazer ou não.

Análise comparada

Realizadas as pesquisas dos três marcos normativos sobre proteção de dados pessoais e privacidade – da União Europeia, dos Estados Unidos e do Brasil – destacam-se a seguir em um quadro comparado as principais diferenças das regras aplicadas em cada um dos países e no bloco europeu. Para sua elaboração considerou-se tanto as correlações entre as normas como suas

principais controvérsias (KING; KEOHANE; VERBA, 1994; LATOUR, 2012). Observa-se que os pontos de tensão envolvem justamente três categorias de atores: o Estado, o setor privado e os cidadãos e seus direitos individuais.

Quadro 1: Comparação dos principais aspectos dos marcos regulatórios. Fonte: A autora a partir dos marcos regulatórios analisados.

Regras	União Europeia	Estados Unidos	Brasil
1. Criação de perfis (*profiling*).	Só podem ser feitas mediante consentimento explícito do titular de dados.	Não há legislação nacional.	Prática não é proibida na LGPD.
2. Direito de não ser objeto de decisões automatizadas.	Há previsão. É necessário consentimento explícito para ser realizada.	Não há previsão legal nas normas federais.	Não há previsão. Além disso, a revisão de decisões automatizadas pode ser feita automaticamente.
3. Direito de retirar os dados pessoais de cadastros (*opt-out*).	Há previsão, com exceções.	Existem restrições a partir da *Federal Privacy Act*.	Há previsão, com exceções.
4. Utilização de dados pessoais para novas finalidades.	A norma proíbe o uso de dados para novas finalidades.	Existem restrições a partir da *Federal Privacy Act*.	A lei prevê exceções que possibilitam a reutilização de dados pessoais.
5. Informação ao titular sobre o uso dos dados pessoais.	O regulamento estabelece que os titulares sejam informados do uso dos dados.	Existem restrições a partir da *Federal Privacy Act*.	A lei permite o uso compartilhado dos dados sem informar aos titulares.
6. Remoção de conteúdo.	Regime de notificação e retirada (*notice and take down*).	Ordem judicial com base na seção 230 do *Communications Decency Act*, de 1996.	Ordem judicial – artigo 19 do Marco Civil da Internet.
7. Responsabilização de intermediários.	Responsabilidade compartilhada entre publicação original e plataformas de conteúdo.	Apenas publicação/ autor original.	Apenas publicação/ autor original.
8. Acesso aos dados pelo poder público e autoridades policiais.	Regras valem igualmente para autoridades de investigação e executivo com pequenas exceções voltadas ao interesse público.	Legislação nacional com base no Federal *Privacy Act* e no *Patrioct Act*, que amplia o acesso aos dados por agentes de segurança.	Potencializa o compartilhamento de dados entre órgãos do poder público e cria exceções para poder público e sistema de segurança.
9. Órgão regulatório de fiscalização e aplicação de sanções.	Autoridades Nacionais independentes e autoridades Europeias de coordenação.	Comissão Federal de Comércio/ *Federal Trade Administration* (FTC)	Secretaria Nacional do Consumidor (MJ), ANATEL e Autoridade Nacional de Proteção de dados.

Fonte: elaboração da autora.

Os cinco primeiros itens do quadro referem-se aos direitos dos titulares de dados em não se sujeitarem às práticas abusivas do setor de tecnologia. Conforme discutido, a criação de perfis (1) realiza uma categorização dos cidadãos, classificando-os para propósitos tais como concessão de crédito e

descontos no varejo. Ocorre que essa hierarquização também é utilizada para outras finalidades (4), como, por exemplo, o reconhecimento facial para monitoramento de atividades criminais. Categorias como cor de pele/raça/etnia e gênero cruzadas com atividades de geolocalização podem ser determinantes na abordagem de "suspeitos" em regiões onde esta prática não é proibida, atividades estas descritas como racismo algorítmico. Quando os dados são utilizados para finalidades diferentes das quais foram inicialmente coletados abrem-se brechas para práticas de discriminação, além do aumento de vigilância e monitoramento. Na União Europeia, há certas garantias, já que as atividades de *profiling* (1) e cruzamento de dados (4) só podem ser realizadas mediante consentimento explícito dos titulares de dados. Nos Estados Unidos e no Brasil não há uma proibição expressa que previna a criação de perfis, tanto por parte do governo, como por parte das empresas.

Neste contexto, há de se levar em conta ainda a utilização de dados pessoais para novas finalidades, que envolve o uso compartilhado de dados. A prática é vedada pelo RGPD. Já nos Estados Unidos existem restrições – *Federal Privacy Act* – e exceções principalmente relacionadas à segurança nacional previstas no *Patriot Act*. Entretanto, no Brasil, conforme discutiu-se, o compartilhamento de dados por parte de órgãos do governo federal é um revés, principalmente após o Decreto nº 8.789 – compartilhamento de bases de dados na administração pública federal – e o Decreto nº 10.046, referente ao Cadastro Base do Cidadão.

Por sua vez, o direito de não ser objeto de decisões automatizadas (2), ou seja, aquelas tomadas por máquinas, não tem previsão legal nem no Brasil nem nos Estados Unidos, apenas na União Europeia. Originalmente, a lei brasileira proibia a prática, como na Europa, mas ela foi modificada, abrindo precedentes para que os algoritmos revisem decisões tomadas por eles próprios. O tema é polêmico especialmente quando se considera a expansão de objetos de inteligência artificial, como, por exemplo, os carros autônomos.

De forma semelhante, o conhecido *opt-out* (3), ou seja, o direito de solicitar a retirada de seus dados pessoais de cadastros – em especial os de consumo – são permitidos na legislação europeia. No Brasil, a prática tem exceções e é dificultada pela alteração na lei do cadastro positivo que, desde 2019, passa a ser automática, ou seja, seus dados são objetos dos conhecidos "score" de

créditos, mesmo sem consentimento (IDEC, 2019). Por sua vez, nos Estados Unidos, o *Federal Privacy Act* impõe algumas restrições a esta prática. Esta legislação limita tanto a utilização de dados pessoais para novas finalidades, como determina que, em alguns casos, os titulares de dados obtenham informações sobre o uso de seus dados pessoais.

Por fim, com relação ao quinto item do quadro – informar as pessoas sobre o uso de seus dados pessoais (5) – este engloba em si os quatro direitos anteriores. Em outras palavras, os sujeitos têm o direito de ser informados se são parte de bancos de perfis (1), de saírem destes cadastros (3), se permanecerem em alguns deles, optarem por não ter suas informações alimentando decisões automáticas dos algoritmos (2) e recusarem-se a ter seus dados utilizados para outras finalidades (4). Estas regras alinham-se com uma compressão das pessoas enquanto sujeitos de direitos, não apenas consumidores.

Estes direitos e cessões são administrados pelos termos de uso das plataformas, que podem ser considerados verdadeiros contratos sociais da vida digital. Ao clicar em "eu aceito" antes de usar determinado aplicativo ou serviço, as pessoas não apenas se responsabilizam por conteúdos publicados, como cedem "voluntariamente" suas informações pessoais para estas empresas. Aliás, antes do RGPD, as pessoas forneciam seus dados para determinada finalidade, e as corporações, por meio de garantias estipuladas nos termos de uso, utilizavam estas informações para outros propósitos, muitas vezes sem o consentimento informado, ou até mesmo o conhecimento das pessoas. A partir dos novos parâmetros, há uma preocupação com a integridade contextual da informação.

Ocorre que as plataformas seguem livres para alterar estas regras dos termos de uso no momento em que acharem oportuno, tornando a adesão ao contrato bastante coercitiva. Afinal, se uma pessoa usa determinado serviço como o correio eletrônico, por exemplo, uma aparente pequena alteração contratual não representa uma motivação para suspender a utilização. Pelo contrário, os custos envolvidos em sair de um serviço e migrar para outro envolvem tempo, conhecimento, etc. Em outras palavras, com a autorregulação, as empresas estão livres para criarem suas próprias regras com pouca ou nenhuma intervenção por parte do Estado, além de se tornarem proprietárias dos dados das pessoas, que possuem pouco, ou nenhum controle sobre eles.

A correspondência teórica sobre os termos de uso no contexto das teorias da democracia é o debate sobre o contratualismo. Hobbes (1987) é o primeiro grande autor desta linha de pensamento, sendo referência para diversas correntes das ciências sociais. Para ele, a sociedade forma-se a partir do contrato, já que no estado de natureza impera o conflito e a violência entre indivíduos. Seu argumento é que a ausência de hierarquia é um problema social resolvido a partir do contrato, em que as pessoas renunciam a sua soberania e liberdade em troca da segurança de não sofrerem as brutalidades presentes no estado de natureza. Sendo assim, este contrato de submissão é motivado pelo temor, e tem como objetivo a normalização da violência, levando as pessoas a aceitarem a dominação.

Ocorre que este pacto social, em que as pessoas entregam sua liberdade ao Estado em troca de segurança, parte do princípio de que os direitos individuais são bens alienáveis. Trata-se de uma visão do indivíduo enquanto posse, em uma relação similar com que se tem com bens externos, como a propriedade, por exemplo. Entretanto, a alienação de direitos por meio contratual, que permite a legitimação de relações interpessoais de subordinação, como no trabalho ou no casamento, dá-se em uma ordem jurídica em que os direitos são inalienáveis, o que em si já é uma contradição.

Esta questão é colocada por Rousseau (1962), para quem a soberania é inalienável e a instituição do governo não pode ser entendida como um contrato. Ou seja, para o autor não é aceitável um contrato que prive uma das partes da liberdade que ela precisaria ter para entrar nele. Para superar esta contradição, é necessário romper com o individualismo possessivo, noção carregada de dubiedade, já que parte da ideia de que há propriedade na pessoa em si, e pensar o direito como usufruto e não como posse. Neste contexto, os termos de uso das plataformas digitais exploram justamente esta vulnerabilidade ao estabelecer a cessão de alguns direitos, ou dos próprios dados pessoais.

Outro ponto de fragilidade do contratualismo refere-se à entrada e saída deste pacto social. Primeiramente, deve-se levar em consideração que nem todas as pessoas participam desse acordo originário. De fato, trata-se de um processo social complexo em que não há um início fixo, ou predeterminado. Em sua formulação inicial, o contrato social referia-se a homens com propriedade, excluindo mulheres, crianças e trabalhadores. Somado a isso, é preciso

considerar a questão geracional e a inversão na arquitetura da escolha. O indivíduo já nasce no contrato aceitando os benefícios da vida social, portanto a adesão deixa de ser voluntária.

É preciso ponderar acerca dos altos custos de saída do contrato social e da vida em sociedade. Na internet, o cancelamento da adesão aos termos de uso é conhecido pelo termo *opt out* (item 3). Trata-se do direito a romper o contrato quando desejar. Ocorre que os custos da ruptura com serviços hegemônicos de e-mail, mídias sociais, sistema operacional, dentre outras ferramentas digitais, é muito alto, pois as opções alternativas são limitadas. O paralelo entre o contratualismo e os termos de uso ilustra como determinados acordos são feitos em condições assimétricas em que as possibilidades de rejeição são muito limitadas.

Neste contexto é importante destacar que uma das principais críticas articuladas ao contratualismo é de Pateman (1993). A autora busca investigar formas de submissão naturalizadas na sociedade, entender como são produzidas, e questionar seu caráter voluntário. Para ela, a simples anuência não é suficiente para legitimar a dominação que se dá por meio contratual. Portanto, faz-se necessário criar mais exigências para aumentar os critérios de autenticidade das relações de exploração, opressão e violência presentes na sociedade.

Se por um lado, o consentimento na visão liberal é voluntário, esclarecido e autônomo, Pateman (1993) destaca que muitas vezes ele é produzido por condições sociais que impedem relações mais autônomas. Para a autora, o caráter comercial do contrato, cujo modelo é de troca e venda, precisa ser superado, já que sua predominância nas sociedades contemporâneas leva à mercantilização das relações sociais.

Por outro lado, Fraser (1992) pondera que, por vezes, os contratos são importantes ferramentas de delimitação da subordinação, como, por exemplo, a limitação de horas de trabalho. No caso dos ambientes digitais, os termos de uso poderiam limitar o tratamento de dados. Ocorre que o poder de negociação é muito restrito. Em situações em que a opressão está legitimada a partir da não interferência do Estado, os sujeitos veem-se obrigados a aceitar as condições estabelecidas. Esta ponderação é válida para ambos exemplos citados: o trabalhador desempregado acata condições de trabalho insalubres para não perder a vaga para outra pessoa em condições iguais, ou até piores.

Os termos de uso das plataformas já estão redigidos e não apresentam opções alternativas ao aceite. O contrato social em forma de termos de uso apresenta, portanto, os mesmos problemas e limites do contratualismo.

Por sua vez, as normas seguintes – remoção de conteúdo (6) e responsabilização de intermediários (7) – estão diretamente associadas à liberdade do setor privado em explorar o uso indiscriminado de dados pessoais. A expansão do setor de tecnologia, a partir dos anos 2000, reflete a transição do modelo de capitalismo de corporações ao neoliberalismo. Para Dardot e Laval (2016), o neoliberalismo não é uma ideologia, mas sim uma "ordem prática", ou uma nova racionalidade, que representa o esgotamento da democracia liberal – ainda que o conceito esteja em constante disputa – já que a economia é que orienta a política e não o contrário. Trata-se do fim do pacto de bem-estar social keynesiano entre o capitalismo de mercado e as democracias liberais (DARDOT; LAVAL, 2016). Essa nova lógica é visível justamente quando cidadãos são tratados como consumidores, não sujeitos de direitos.

Além disso, essa mudança tem como característica fundamental a transformação do papel do Estado, que passa a atuar mais em defesa de interesses privados do que na proteção de direitos sociais. Estas novas formas de governo transformam a visão do que é público e privado, do que é político e do que é econômico (HARVEY, 2008; FRASER, 2009; DARDOT; LAVAL, 2016). Para se ter uma ideia da dimensão do fenômeno, as empresas de tecnologia empregam menos trabalhadores se comparadas com outros setores da economia. Zuboff destaca que "a *General Motors* empregou mais pessoas durante o pico da Grande Depressão do que o Google e o Facebook contratam juntos atualmente" (2019, p. 468). A comparação entre 1929 e 2019 demonstra a erosão do modelo em que a economia prevalece sobre a política, que leva à consolidação do neoliberalismo e à concentração de renda. Não é mais o Estado que impõe limites à atuação do mercado, nem mesmo por meio do controle de monopólio, como é o caso das GAFAM.

A controvérsia sobre a retirada de conteúdo (6) ilustra a postura destes diferentes atores sociais. Quando o material publicado online por terceiros é julgado pelas empresas a partir de sua relevância em termos de números de cliques e curtidas, volume, profundidade e capacidade de gerar lucro, pouco importa se é mentiroso, fraudulento, ou contém discurso de ódio. O

histórico de atuação destas empresas indica que sua indiferença para com os valores democráticos e de justiça não ocorreu apenas recentemente. Em 2011, o Departamento de Justiça dos Estados Unidos multou o Google em 500 milhões de dólares por anunciar e vender remédios canadenses proibidos no país desde 2003 (Zuboff, 2019, p. 475). Ignorar a legislação de drogas é apenas uma das facetas dessa indiferença que coloca o lucro em primeiro plano e demonstra como a autorregulação do setor não é suficiente. O caso ilustra como o conteúdo impulsionado obtém um tratamento diferenciado daquele "publicado por terceiros" pelo qual as plataformas não querem se responsabilizar.

É por isso que a atuação do setor privado é o tema em que há mais divergência entre as normas de proteção de dados analisadas. Os debates envolvem principalmente aspectos relacionados à suas obrigações e responsabilidades. Neste contexto, é importante destacar que as duas principais polêmicas estão relacionadas; a partir do debate sobre a responsabilização de intermediários (7) é que são determinadas as regras para remoção e moderação de conteúdo online (6). Conforme discutido na primeira parte do artigo, a jurisprudência americana, sede das GAFAM, opera com base em uma lei de 1996, que buscava prevenir a pornografia, abrindo precedentes para que as empresas de tecnologia não sejam responsabilizadas pelo conteúdo publicado por terceiros.

Entretanto, é preciso ter em mente que, à época, a internet ainda operava com limitações de interatividade. A web 2.0, ou seja, uma segunda geração de aplicações, serviços e comunidades, inicia-se a partir de 2004, e introduz fenômenos atualmente corriqueiros como o compartilhamento de informações, a colaboração, as redes sociais, a consolidação dos formatos multimídia e das plataformas de conteúdo.

A evolução do setor de tecnologia transformou o entendimento sobre o tema no âmbito da União Europeia. Entre 2009 e 2014 ocorreram os debates sobre o "direito ao esquecimento". Conforme discutido, o RGPD engloba algumas possibilidades do direito à desindexação. Entretanto, a questão está longe de se esgotar, pois envolve muito mais do que remover links para informações "irrelevantes", ou "desatualizadas". O papel do setor privado nestas questões é mais abrangente e inclui fenômenos como a disseminação de notícias

falsas, discursos de ódio e sua consequente influência no debate público e, de forma ainda mais grave, no resultado de pleitos eleitorais.

No Brasil e nos Estados Unidos, é necessária uma ordem judicial para a remoção de conteúdo. Nestas regiões, a responsabilidade da publicação é apenas do "autor original". Em contraposição, a União Europeia adota um regime misto de responsabilidade compartilhada entre as plataformas de conteúdo e a publicação inicial, recorrendo até mesmo ao controverso mecanismo de notificação e retirada (*notice and take down*).

Ocorre que as condições determinadas para a retirada de conteúdo, seja por infração de direitos autorais, seja por serem considerados ilegais, não foram suficientes para conter fenômenos como a violência política expressa tanto por meio da desinformação, como de discursos de ódio. Cada vez mais fica à cargo do setor privado distinguir sobre o que é ou não retirado do ar, tornando as plataformas de conteúdo os *gatekeepers* da informação que circula na web, em especial nas mídias sociais. Há de se levar em conta ainda os conteúdos impulsionados, ou seja, aqueles que são pagos para terem destaque nas plataformas e consequentemente não são objeto de moderação.

A censura à nudez em caso de amamentação é uma das polêmicas que demonstram que as fronteiras do que é culturalmente aceitável varia entre os países. Além disso, expõe o fato de que as plataformas possuem regras pouco transparentes para determinar o que é ou não é permitido. Torna evidente o uso automatizado de filtros de conteúdo. Neste contexto, apenas a legislação alemã – conhecida como NetzDG – inova ao prever relatórios sobre os processos de decisão envolvidos na curadoria de itens retirados do ar. Observa-se assim que o modelo regulatório europeu está focado em questões como escala e distribuição, não necessariamente na remoção do conteúdo em si.

Estas controvérsias sobre as obrigações e responsabilidades do setor privado, que envolvem os limites da liberdade de expressão e a remoção de conteúdo da internet, demonstram que as legislações, em sua maioria, focam nos sintomas e não no diagnóstico da situação. Em outras palavras, ao determinar regras para a remoção de conteúdo, o arcabouço legal não toca na questão central que são os processos algorítmicos das empresas de tecnologia. Como funcionam os mecanismos de recomendação? Quais são os critérios de priorização de conteúdo? Os procedimentos de auto completar reproduzem preconceitos?

Como funcionam os filtros das publicações? Operam a partir de bases éticas e princípios democráticos? Estas são decisões técnicas pelas quais as empresas de tecnologia podem responder, muito mais do que sobre conteúdos específicos publicados por terceiros, sejam estes seios à mostra ou incitações a golpes de Estado. Pondera-se ainda que estas são questões até superficiais quando se enxerga a tecnologia a partir de uma lupa mais ampla, em específico os dilemas morais – como o das possíveis vítimas do trem descontrolado – envolvidos nos processos decisórios de inteligência artificial.

O quadro comparativo dos marcos regulatórios de proteção de dados indica duas questões centrais na atuação dos Estados: acesso aos dados pelo poder público (8) somado à fiscalização e à aplicação de sanções (9). Neste último quesito, o RGPD prevê autoridades nacionais com poderes de *accountability*, independente dos governos, com autonomia técnica e administrativa. Suas regras contemplam tanto o setor privado como o público e suas autoridades policiais.

Já nos Estados Unidos, o órgão responsável pela regulação da proteção de dados é a Comissão Federal de Comércio, a partir de uma abordagem dos direitos do consumidor e o conjunto de leis *antitruste*. O uso de dados por parte do governo é relativamente obscuro, pois, se de um lado há regras como o *Federal Privacy Act*, há outras como o *Patriot Act*, que abrem brechas para o poder de vigilância do Estado (8). Além do mais, existem legislações regionais como o *California Consumer Privacy Act*, por exemplo.

Por fim, a lei geral de proteção de dados brasileira estabelece uma categoria diferente para o poder público no que se refere ao tratamento de dados pessoais, ou seja, exime o Estado de uma série de obrigações e responsabilidades (8). Não suficiente, exclui autoridades policiais e judiciais das determinações presentes na norma. Além disso, por meio de decretos, facilita o compartilhamento de dados pessoais entre órgãos administrativos. Desta forma, potencializa o poder de vigilância do Estado brasileiro e de seus agentes de segurança. Sendo assim, pode-se considerar que a lei geral de proteção de dados pessoais brasileira é um marco regulatório importante, entretanto débil em regular a atuação do próprio Estado.

Conclusão

Historicamente, a esfera privada foi negligenciada na teoria política pelo entendimento clássico de que era o âmbito referente à família e a casa, estando subordinada ao espaço público (*polis* grega), local de exercício da cidadania e da política. A separação entre o que é público e o que é privado é um princípio fundador da tradição liberal, já que o voto secreto – privacidade – expressa a autorização da representação política (MIGUEL, 2014). O liberalismo inaugura a noção do indivíduo enquanto uma unidade política. Ainda que reconheça a família, a autoridade no âmbito privado é exercida pelos homens, aqueles habilitados à participação na esfera pública, tanto em termos de participação política como no direito à propriedade.

No século 21, a separação da esfera pública da privada não mais se sustenta, tanto pela problematização historicamente postulada pela teoria feminista, como pela evolução das tecnologias da informação e comunicação. A privacidade consolida-se para além da noção do direito de ser deixado em paz (liberdade negativa), passando a ser compreendida como o espaço de intimidade e autonomia, essencial para o desenvolvimento da própria identidade e personalidade (*right to the self*). A liberdade, antes exercida em público, desloca-se para a esfera privada. O mercado de dados pessoais explora essa transformação, capitalizando as experiências privadas.

Sendo assim, em menos de duas décadas o capitalismo de vigilância consolidou-se silenciosamente no setor de tecnologia. O monitoramento constante e automatizado das experiências individuais faz com que a proteção de dados pessoais transforme-se em uma questão coletiva, tornando-se objeto de normas jurídicas. Adotando a metodologia de análise comparada, o artigo analisou o arcabouço de três marcos regulatórios que versam sobre o tema: da União Europeia, dos Estados Unidos e do Brasil. A avaliação teve como objetivo a identificação das principais polêmicas e divergências entre as legislações e como elas se relacionam com três categorias de atores: o setor privado, cidadãos e seus direitos e o papel do Estado em mediar estes interesses.

Observou-se que estas discrepâncias revelam até mesmo visões distintas sobre os direitos humanos, o exercício da liberdade de expressão, da cidadania, e da democracia liberal. Sobretudo, evidenciam compreensões sobre o

papel do Estado, tanto em regular o setor de tecnologia, como sobre sua própria atuação.

A partir da pesquisa comparada, foi possível concluir que o Regulamento Geral sobre Proteção de Dados da União Europeia é a legislação que mais garante direitos individuais, ao adotar mecanismos de consentimento informado, limitação das finalidades de coleta de informações, dentre outros. Reflete uma visão de democracia em que é papel do Estado proteger e garantir as liberdades, além de regular o setor privado. A norma é uma das principais reações para conter o avanço do modelo de negócios que lucra com experiências privadas. É preciso atentar para o fato de que o bloco possui uma posição estratégica na geopolítica mundial, o que possibilita um contraponto ao setor de tecnologia, em sua maioria localizado nos Estados Unidos.

Ainda assim, o problema de pesquisa permanece em constante disputa, já que o trâmite legislativo, em sua maioria, tem dificuldade em acompanhar a rápida evolução do setor de tecnologia. Por fim, em termos práticos, para a população em geral, as mudanças foram tímidas, ou quase imperceptíveis. É preciso reconhecer que ocorreu um esforço para que notificações sobre os termos de uso e a política de privacidade obtivessem relevância na experiência de uso dos sites e aplicativos digitais. Porém, há aí uma ironia. Em boa parte destes avisos, só consta a opção de "aceitar" para utilizar o serviço. A margem de negociação é mínima. Neste contexto, é preciso enfatizar que a privacidade por padrão foi pouco incorporada no design destas plataformas. A opção de saída – *opt out* – ou recusa do uso das tecnologias hegemônicas, torna os indivíduos que realizam esta escolha praticamente párias digitais. Estes acordos são feitos sobre condições impossíveis de não serem aceitas, o que leva as pessoas a abdicarem de determinadas liberdades, como a de não ser vigiado. Desta forma, o exercício dos direitos deixa de ser indivisível, interrelacionados e interdependente, corroendo as bases dos direitos humanos e das democracias liberais contemporâneas. Na teoria clássica do contrato social, as pessoas renunciam a algumas liberdades em troca da segurança oferecida pelo Estado, o único legítimo a exercer a autoridade de interferir na esfera privada (HOBBES, 1987). Atualmente, no contrato feito a partir dos termos de uso das plataformas e aplicativos digitais, a alienação de direitos é realizada para empresas privadas com interesses comerciais muitas vezes obscuros e antiéticos.

Há de se considerar ainda que a relação entre privacidade e segurança é complementar e não necessariamente existe em contraposição.

É justamente por isso que o mercado de dados tornou-se uma preocupação coletiva para as democracias contemporâneas. Faz-se necessário aplicar critérios de justiça também na esfera privada, já que no século 21 o pessoal é cada vez mais político. Os marcos normativos sobre proteção de dados pessoais mostraram insuficientes para conter o avanço do mercado de dados e a concentração de poder das empresas de tecnologia. De forma semelhante, as leis concorrenciais estadunidenses (*antitruste*) tampouco preveniram que as gigantes da GAFAM ampliassem seu monopólio no setor de tecnologia. O próprio mercado financeiro fundiu-se com estas companhias, dado que são controladas pelos mesmos agentes.

Se por um lado existe algum consenso entre as normas de proteção de dados e privacidade, o mesmo não pode ser dito sobre a controvérsia da moderação e retirada de conteúdo, diretamente associada aos limites da liberdade de expressão. O fato é que a legislação da mídia tradicional não se adapta facilmente à web, seja no modelo de concessões, na ampliação da infraestrutura, na medição de audiência, na veiculação de propaganda, na proteção da privacidade, ou dos direitos dos consumidores. Por isso, esta discussão não tem correspondência na mídia tradicional, justamente porque estes meios possuem controle editorial sobre o que é publicado. Na web cada pessoa divulga o que quiser. A jurisprudência estadunidense, onde estão sediadas as principais companhias de tecnologia, tem como base uma lei de combate à pornografia de 1996, portanto anterior à própria indexação da web. O Marco Civil da Internet brasileiro segue na mesma direção, eximindo os provedores de responsabilidade sobre o conteúdo publicado por terceiros. O ponto central deste debate é o exercício da liberdade de expressão e seus limites. Ocorre que a autorregulação do setor privado não foi suficiente para conter fenômenos antidemocráticos, a violência política e a desinformação na web. Deixar à cargo do setor privado distinguir sobre o que é ou não retirado do ar mostrou-se ineficiente, além de ampliar o constante risco da instituição de mecanismos de censura e limitação da liberdade de expressão, afetando a opinião pública enquanto um todo. Sobretudo, é preciso levar em conta que conteúdos

impulsionados, ou seja, a fonte de renda das plataformas, raramente são objeto de moderação justamente por serem patrocinados.

A principal conclusão do artigo neste sentido é que se tornou cada vez mais urgente regular os próprios algoritmos que operam a web, os sistemas de aprendizado de máquinas, o software dos carros autônomos, dos celulares e todos sistemas cibernéticos que fazem a intermediação do cotidiano das pessoas. É necessário dar publicidade aos processos decisórios dos algoritmos inteligentes. A transparência, que está presente no discurso neoliberal de desenvolvimento, torna-se fundamental na regulação do setor de tecnologia. O Estado precisa desempenhar seu papel de intermediário entre os interesses privados e a coletividade, já que a autorregulação do setor privado mostrou-se ineficiente em conter fenômenos que corroem cada vez mais as democracias contemporâneas.

Referências

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019.

BUTTS, Chris. The Microsoft case 10 years later: antitrust and new leading new economy firms. Chicago: **Northwestern Journal of Technology and Intellectual Property.** v. 8, n. 2, p. 275-291, 2010.

CAVOUKIAN, Ann. **Privacy by design in law, policy and practice**. A white paper for regulators, decision-makers and policy-makers, Ontario: Information and Privacy Commissioner, 2011.

CAPOZZI, Bruno. Julgamento que pode mudar a internet ganha novo capítulo nos EUA. **Olhar Digital**, 2023. Disponível em: https://olhardigital.com.br/2023/02/23/pro/julgamento-que-pode-mudar-a-internet-ganha-novo-capitulo-nos-eua/. Acesso em: 27 mar. 2023.

COBB, Stephen. Data privacy and data protection: US law and legislation. **An ESET White Paper**, Bratislava, p. 1-15, 2016. Disponível em: https://www.researchgate.net/publication/309456653_Data_privacy_and_data_protection_US_law_and_legislation Acesso em: 27 mar. 2023.

DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo**: ensaios sobre a sociedade neoliberal. São Paulo: Boitempo, 2016.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Thomson Reuters, 2019.

FRIEDMAN, Milton. The business community's suicidal impulse. **Cato Policy Report**, v. 21, n. 2, p. 6-7, 1999.

FRASER, Nancy. Rethinking the public sphere: a contribution to the critique of actually existing democracy. *In*: CALHOUN, Craig (ed.). **Habermas and the public sphere,** The MIT Press, 1992, p.109-142.

FRASER, Nancy. Feminism, capitalism and the cunning of history. **New Left Review**, v. 56, p. 97-117, 2009.

HARVEY, David. **O neoliberalismo**: história e implicações. Loyola, 2008.

HOBBES, T. **Leviatã**, São Paulo: Nova Cultural. 1987.

IDEC. De olho no cadastro positivo. 2019. Disponível em: https://idec.org.br/cadastro-positivo. Acesso em: 10 nov. 2022.

KING, Gary; KEOHANE, Robert O.; VERBA, Sidney. **Designing social inquiry**: scientific inference in qualitative research. Princeton: Princeton University Press, 1994.

LATOUR, Bruno. **Reagregando o social**: uma introdução à teoria do ator-rede. Salvador; Bauru: Edufba; EDUSC, 2012.

MEIRELES, Adriana. Proteção de dados e golpismo no Brasil. **ComCiência**, 2023. Disponível em: https://www.comciencia.br/protecao-de-dados-e-golpismo-no-brasil/. Acesso em: 27 mar. 2023.

LOPES-SALDANHA, Jânia Maria; PITTALUGA-HOFFMEISTER, Guilherme; ROSSATTO-BOHRZ, Clara. Práticas anticoncorrenciais das gigantes da internet no contexto brasileiro. **Opinión Jurídica**, Medellín, v. 17, n. 34, p. 63-87, dez. 2018. Disponível em: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-25302018000200063&lng=en&nrm=iso. Acesso em: 5 maio 2023.

MIGUEL, Luis Felipe. **Democracia e representação**: territórios em disputa. São Paulo: Editora Unesp, 2014.

MOVIUS, Lauren B.; KRUP, Nathalie. US and EU privacy policy: comparison of regulatory approaches. **International Journal of Communication**, v. 3, p. 169-187, 2009.

NISSENBAUM, H. **Privacy in context: Technology, policy and the integrity of social life**. Stanford, CA: Stanford University Press, 2009.

O'NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy. New York: Crown, 2017.

PATEMAN, Carole. **O contrato sexual.** Rio de Janeiro: Paz e Terra, 1993.

PATEMAN, Carole. Críticas feministas à dicotomia público privado. *In:* MIGUEL, Luis Felipe; BIROLI, Flávia. **Teoria política feminista**: textos centrais, Niterói, Eduff, 2013. p. 55-80.

ROUSSEAU, Jean-Jacques. **Do contrato social ou princípios do direito político**. Porto Alegre: Editora Globo, 1962.

SANTOS, Bruna Martins dos. **Uma avaliação do modelo de responsabilidade de intermediários do marco civil para o desenvolvimento da internet no Brasil**. Brasília: Internet Society, 2020.

STF. Audiência pública vai discutir regras do marco civil da internet: os temas abrangem a responsabilidade de provedores e as formas de retirada de conteúdos ofensivos. **Supremo Tribunal Federal**. 2023. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=503467&ori=1. Acesso em: 27 mar. 2023.

TUTT, Andrew. An FDA for Algorithms. **Administrative Law Review**, v. 69, n. 1, p. 83-123, 2017.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679 Acesso em: 7 nov. 2022.

UNIÃO EUROPEIA. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. **Official Journal of the European Union**. 2008. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0977&from=EN. Acesso em: 7 fev. 2021.

ZUBOFF, Shoshana. **The age of surveillance capitalism**: The fight for a human future at the new frontier of power. Londres: Profile Books, 2019. [digital version].

Privacidade no século 21: proteção de dados, democracia e modelos regulatórios

Resumo: A partir da teoria política sobre a distinção público privado, o artigo investiga a proteção de dados pessoais como um desdobramento contemporâneo da privacidade. Para fundamentar empiricamente a discussão, são analisados três diferentes marcos normativos de proteção de dados: da União Europeia, dos Estados Unidos e do Brasil. O objetivo é examinar como as legislações compreendem o papel do Estado, a atuação do setor privado e os direitos de seus cidadãos. A metodologia adotada é a de análise comparada com foco nas correlações e controvérsias entre as normas. Como resultado, o artigo sistematiza as principais regras adotadas em cada uma das regiões em um quadro comparativo. O diagnóstico aponta para a conclusão de que as divergências entre os modelos regulatórios refletem entendimentos sobre o próprio sistema democrático. Os resultados da discussão buscam contribuir para reflexões das ciências sociais com ênfase em tecnologia e política.

Palavras chave: privacidade, proteção de dados, democracia, tecnologia, internet.

Privacy in the 21st Century: data protection, democracy, and regulatory frameworks

Abstract: Starting from debates in political theory about the public-private distinction, the article investigates data protection as a contemporary development of privacy. To substantiate the discussion empirically, the normative frameworks on data protection of the European Union, the United States and Brazil are analyzed. The aim is to examine how these regulations define the role of the state, private sector procedures and citizen rights. The research uses a comparative analysis methodology with a focus on correlations and controversies between the legislations. The result is a systematization of the main rules adopted in each region into a comparative framework. The article concludes that the differences between regulatory models reflect distinct understandings about the democratic system itself. This discussion aims to contribute to reflections in the social sciences about the relations between technology and politics.

Key words: privacy, data protection, democracy, technology, internet.

Submetido em 19 de agosto de 2022
Aprovado em 04 de maio de 2023