O FORNECIMENTO DE DADOS PESSOAIS COMO CONTRAPRESTAÇÃO CONTRATUAL PELO CONTEÚDO OU SERVIÇO DIGITAL DISPONIBILIZADOS: ANÁLISE CRÍTICA DA DIRETIVA 770/2019 DA UNIÃO EUROPEIA

Lauricio Alves Carvalho Pedrosa[1]

Resumo

O fornecimento gratuito de conteúdos e serviços digitais tornou-se bastante comum no âmbito da rede mundial de computadores. Entretanto, costuma-se exigir como contraprestação contratual a concessão de dados pessoais, considerado pela economia do compartilhamento um dos mais valiosos ativos da contemporaneidade. Por outro lado, as legislações os classificam como direito humano fundamental. A disciplina jurídica acerca dessa temática costumava proibir que a execução do contrato estivesse subordinada ao consentimento para o tratamento de dados que não fossem necessários à realização daquele acordo. Não obstante, a Diretiva europeia que disciplinou os contratos eletrônicos admitiu o fornecimento de dados como contraprestação contratual e, por conseguinte, sua utilização para outras finalidades. O presente texto almeja realizar uma análise crítica da referida regra. Ao demonstrar a existência de informações supraindividuais no conteúdo dos dados pessoais, defende-se a inadequação e a insuficiência do princípio da autodeterminação informativa como diretriz reguladora dessa temática. Pleiteia-se, por fim, a construção de um regramento mais restritivo para a coleta e tratamento de dados, em razão dos riscos que representa a direitos individuais e coletivos, bem como às conquistas mais relevantes da humanidade, a exemplo da democracia, da liberdade e do respeito à diversidade.

Palavras-chave: Dados pessoais. Contratos eletrônicos. Autodeterminação informativa. Dimensão coletiva. Plataformas digitais.

Abstract

The free provision of digital content and services has become quite common on the World Wide Web. However, the provision of personal data, considered by the sharing economy to be one of the most valuable contemporary assets, is often required as contractual payment. On the other hand, legislation classifies them as a fundamental human right. The legal discipline

[1] Professor Titular de Direito Civil da UESC (Universidade Estadual de Santa Cruz/Ilhéus). Atualmente realiza estudos pós-doutorais na Justus-Liebig Universität Giessen (Alemanha), com bolsa CNPQ. Doutor em Direito pela Universidade Federal da Bahia, com Estágio de Doutoramento na Justus-Liebig Universität Giessen. Mestre em Direito Privado e Econômico pela Universidade Federal da Bahia. Especialista em Direito Civil pela Fundação Faculdade de Direito da Bahia. Advogado e Líder do Grupo de pesquisa Democracia, Justiça, Alteridade e Vulnerabilidades (DeJAVu-UESC). Atualmente é um dos líderes da rede de pesquisadores Agendas de Direito Civil Constitucional.

on this subject used to prohibit the execution of a contract being subject to consent for the processing of data that was not necessary for the performance of the agreement. However, the European Directive governing electronic contracts has allowed the provision of data as contractual payment and, consequently, its use for other purposes. The aim of this text is to critically analyze this rule. By demonstrating the existence of supra-individual information in the content of personal data, it defends the inadequacy and insufficiency of the principle of informational self-determination as a regulatory guideline for this issue. Finally, it calls for a more restrictive regulation of data collection and processing, due to the risks it poses to individual and collective rights, as well as to humanity's most important achievements, such as democracy, freedom and respect for diversity.

Keywords: Personal data. Eletronic contracts. Informational self-determination. Collective dimension. Digital platforms.

1 INTRODUÇÃO

Com a criação das redes sociais, tornou-se bastante frequente a utilização de uma modalidade de contrato na qual o consumidor oferece dados pessoais como contraprestação ao fornecimento de conteúdos e serviços digitais, normalmente gratuitos. Não obstante tratar-se de fenômeno relativamente novo, os usuários da rede mundial de computadores têm aderido com bastante frequência a tal modalidade de contrato.

Os dados mostram que mais de 60% da população mundial é usuária de redes sociais (LUNGUI, 2023). A grande maioria, contudo, desconhece os riscos inerentes ao fornecimento indiscriminado de dados, cujo potencial danoso ameaça direitos fundamentais individuais – tanto dos usuários quanto de terceiros que sequer manifestaram seu consentimento –, coletivos e até mesmo das futuras gerações, consoante será demonstrado posteriormente.

A União Europeia, em maio de 2019, adotou a Diretiva 770, que passou a disciplinar "certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais". Dentre os seus objetivos, destacam-se a concretização do potencial de crescimento do comércio eletrônico no âmbito da União Europeia, de modo a promover o Mercado Único Digital; eliminar seus principais obstáculos; reforçar a segurança jurídica "e reduzir os custos de transação, designadamente para as pequenas e médias empresas (PME)" (Considerando 3).

Tal disciplina almeja também garantir aos consumidores o acesso e, ao mesmo tempo, facilitar o fornecimento por parte das empresas aos conteúdos e serviços digitais. De acordo com o texto da própria Diretiva, outro importante objetivo consiste em "estabelecer o

justo equilíbrio entre a consecução de um elevado nível de defesa do consumidor e a promoção da competitividade das empresas" (Considerando 2).

A referida disciplina legal, voltada para a regulação dos contratos de fornecimento de conteúdos e serviços digitais, reconheceu como pertencente ao âmbito de incidência de suas normas os acordos em que "o profissional forneça ou se comprometa a fornecer conteúdos ou serviços digitais ao consumidor e o consumidor faculte ou se comprometa a facultar dados pessoais ao profissional" (art. 3°).

Desse modo, a Diretiva admitiu que os dados pessoais sejam utilizados como contraprestação contratual, tal como já ocorre há bastante tempo no âmbito da rede mundial de computadores, especialmente para o uso das redes sociais, na qual informações personalíssimas são disponibilizadas não somente para os demais usuários, mas principalmente para os titulares das plataformas, que utilizam tal conteúdo para transformá-lo em informação comportamental, cujo tratamento tem como finalidade principal intervir na experiência humana, de modo a moldar tais comportamentos para inúmeras finalidades.

Nesse contexto, almeja-se, por meio do presente trabalho, realizar uma análise crítica acerca dessa previsão normativa, demonstrando-se os riscos envolvidos no fornecimento de dados pessoais, tanto para a esfera personalíssima do cidadão que cede de tais informações, quanto para a coletividade que, de alguma forma, com aquela pessoa se relaciona, o que revela a existência de uma dimensão coletiva inerente a tais conteúdos e, por conseguinte, a insuficiência do princípio da autodeterminação informativa, utilizado como fundamento para a construção de toda a disciplina jurídica existente acerca dessa temática.

Para tanto, será realizada uma análise crítica, por meio de pesquisa exploratória, fundada em ampla revisão bibliográfica e documental, de modo a aprofundar o estudo do tema da pesquisa, bem como a formular novas estratégias de argumentação e decisão, e sugerir formas de construção de soluções para o problema relativo aos riscos do fornecimento de dados pessoais como contraprestação contratual, que serão processados e utilizados para finalidades outras que não a execução do referido contrato.

Por fim, propõe-se uma nova classificação jurídica para os dados pessoais, que se afasta das noções de bem jurídico e de direito subjetivo, com o escopo de evitar a adoção de uma perspectiva patrimonialista, utilizada para legitimar o uso de tais informações como moeda de troca. Ademais, diante dos riscos envolvidos na coleta e no tratamento de dados pessoais, acrescidos da evidente dimensão coletiva existente em tais conteúdos, o que remete à noção de multititularidades, critica-se a disciplina europeia e sugere-se a adoção, no Brasil, de um

regramento mais rígido e restritivo, sob pena de incidir-se em inconstitucionalidade e de expor os cidadãos a violações a direitos fundamentais.

2 A ATUAL DISCIPLINA EUROPEIA ACERCA DO FORNECIMENTO DE DADOS PESSOAIS COMO CONTRAPRESTAÇÃO CONTRATUAL

Os dados pessoais consistem em informações em estado potencial, anteriores ao processo de tratamento/interpretação, bem como de elaboração (DONEDA, 2019, p. 136). Com o advento da denominada economia do compartilhamento, tais conteúdos transformaram-se em valioso ativo, objeto de interesse da grande maioria dos fornecedores de produtos e serviços aos cidadãos, uma vez que, por meio do tratamento de tais informações, é possível não apenas identificar hábitos de consumo, como também influenciá-los, de modo a ampliar o potencial lucrativo das empresas.

Por essa razão, os dados pessoais passaram a ser considerados o mais importante ativo do século XXI, o que está em consonância com a perspectiva neoliberal que considera todos os aspectos da vida como comodities (KLEIN, 2001). Não obstante tal tratamento oferecido pelos agentes econômicos dominantes, a legislação e a doutrina até então esforçaram-se para reconhecer o caráter de direito fundamental e, portanto, extrapatrimonial, dos dados pessoais.

Nesse sentido, o Conselho da Europa tratou os dados pessoais como um tema de direitos humanos desde o ano de 1981, mediante a Convenção para a Proteção dos Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais. Já a Carta de Direitos Fundamentais da União Europeia prevê a proteção de dados em seu art. 8°.

O Regulamento Geral sobre Proteção de Dados da União Europeia (Regulamento UE 2016/679, Considerando 1) afirma expressamente que tem como finalidade a tutela de um direito fundamental. No Brasil, a Lei Geral de Proteção de Dados segue a mesma orientação e destaca dentre seus principais objetivos: assegurar a liberdade, a privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1°). Não há dúvida, portanto, que as legislações sobre o tema reconhecem os dados pessoais como direito fundamental, ao mesmo tempo em que admitem a cessão de tais informações no âmbito das relações contratuais.

Em face do que dispõe a Diretiva europeia 2019/770 sobre o fornecimento de conteúdos e serviços digitais, no que se refere ao "pagamento com dados", Sebastian Martens (2022) destaca, entretanto, que tanto legislador europeu como o alemão evitaram de forma consciente, utilizar o conceito de contraprestação no contexto de um tal "pagamento com dados" e deixou a questão da definição a cargo da ciência e da práxis. Não obstante a tentativa de evitar o termo contraprestação, reconhece a doutrina que haverá, nesse caso, uma relação de troca (KROSCHWALD;POLENZ, 2022, p. 206).

Os juristas europeus têm reconhecido a prioridade do Regulamento Geral de Proteção de Dados em relação a outras normas jurídicas, que prevalecerá quando dados pessoais forem objeto de tratamento, em decorrência das relações criadas por meio de tais contratos (HERMIDA, 2022, p. 23-24). Nesse sentido, Sebastian Martens (2022) reconhece, entretanto, que a dificuldade em relação ao denominado pagamento com dados emana sobretudo da precária relação entre o direito dos contratos e o direito à proteção de dados.

Desse modo, surge a controvérsia acerca da (im)possibilidade de se assumir uma obrigação de fornecimento de dados pessoais que serão utilizados para outra finalidade, distinta da execução do contrato, como sugere o teor da referida Diretiva acerca de conteúdos e serviços digitais, bem como sobre sua compatibilidade com o direito à proteção de dados, especialmente em face do que dispõe o parágrafo 4 do art. 7° do Regulamento Geral de Proteção de Dados europeu, que contém a chamada proibição de subordinação (Kopplungsverbot):

> **"4. Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato".**

A referida norma tem o objetivo de garantir a livre tomada de decisão, sem que haja qualquer tipo de pressão, seja emocional, seja econômica, voltada para persuadir o sujeito a fornecer seus dados pessoais, destinados a finalidades outras que não aquelas necessárias à execução do contrato. Nesse sentido, Jürgen Taeger e Detlev Gabel (2022). Afirmam que o impedimento à celebração do contrato, caso o usuário se recuse a autorizar o tratamento de dados que não são necessários à execução do referido negócio jurídico, "pode constituir uma situação de pressão, especialmente se não existirem alternativas no mercado".

Em tais casos, entende-se que a pessoa deixa de exercer a chamada autoproteção informativa (informationelle Selbstschutz) e, como consequência, afasta-se o pressuposto acerca da existência de uma livre decisão como condição prévia à eficácia do consentimento. Os referidos autores, entretanto, entendem que, caso consentimento para o tratamento de dados pessoais voltado para um fim alheio ao cumprimento do contrato for visto como "contrapartida" a um serviço supostamente gratuito prestado pelo responsável pelo tratamento (pagamento com dados), a proibição de subordinação não o impede (TAEGER, GABEL, 2022, Rn. 96).

Em sentido semelhante, Sebastian Martens (2022) defende a necessidade de uma interpretação sistemática de ambas as Diretivas, em que a solução se encontraria no meio termo: uma obrigação de fornecimento de dados pessoais seria proibida (unzulässig), mas um empresário poderia tornar a sua prestação dependente em princípio de uma autorização/consentimento (Einwilligung) do consumidor para o processamento de dados pessoais disponibilizados.

Já Sebastian Schulz (2022) afirma que, em razão de os conteúdos e serviços gratuitos serem financiados por publicidade, seria absolutamente necessário, em tais situações, pelo menos em termos econômicos, o tratamento de dados fundado no consentimento. Desse modo, nas relações de troca entre conteúdo ou serviço digital, de um lado, e a disponibilização dados pessoais, do outro, se o consentimento para a divulgação de dados pessoais for também a contrapartida e existir uma relação contratual ou, de outro modo, se for suficientemente transparente que o serviço só pode ser oferecido economicamente sob esta condição, a existência de uma proibição de subordinação não deveria ser assumida, sobretudo no interesse dos consumidores.

Portanto, a maioria dos autores tem admitido o afastamento da aplicação das regras do referido Regulamento Geral de Proteção de Dados, em circunstâncias especiais, a exemplo da hipótese em que o contrato preveja o pagamento com dados como contraprestação ao fornecimento de conteúdos e serviços digitais.

Em sentido semelhante ao defendido pela doutrina alemã, o Comissário para a Proteção de Dados da Saxônia entendeu que a oferta de um download "gratuito" de um documento em troca do consentimento para o envio de um newsletter publicitário não impede o tratamento de dados pessoais. De acordo com a decisão (2019)., o comportamento da parte supostamente prejudicada pela exigência de tratamento de dados pessoais poderia ser identificado como um *venire contra factum proprium*, afinal "quem pretender celebrar um

determinado contrato não pode legalmente furtar-se ao tratamento de dados que é necessário para esse contrato"

Constata-se, por conseguinte, que a opinião majoritária na doutrina alemã, bem como a decisão mais recente de um dos seus órgãos de controle admitem o denominado "pagamento com dados", ou seja, a validade do consentimento para tratamento de dados destinados a fins publicitários como contrapartida contratual, nos casos em que não se cobra pelo conteúdo ou serviço digital disponibilizado.

Ocorre, contudo, que essa é a estratégia utilizada pela maior parte das empresas, a fim de obter o consentimento do usuário para o processamento de dados, cujas finalidades são bastante distintas daquelas que envolvem a utilização do serviço. Aplicativos que prestavam serviços aparentemente inocentes, a exemplo daquele que mostrava qual seria a aparência da pessoa daqui a alguns anos, foram utilizados para a obtenção do consentimento e o processamento de dados pessoais que permitiram a identificação do perfil dos eleitores (técnica conhecida como perfilização ou profiling) e a criação de conteúdos falsos voltados para a manipulação de eleições. Trata-se de apenas um dos exemplos dos riscos inerentes ao fornecimento indiscriminado de dados pessoais, cuja análise mais aprofundada será realizada a seguir.

3 OS RISCOS DO FORNECIMENTO INDISCRIMINADO DE DADOS PESSOAIS

A legislação criada para assegurar a proteção dos dados pessoais, compreendidos como um direito fundamental, baseia-se no pressuposto do exercício individual da denominada autonomia privada, ou seja, cada ser humano tem o direito de decidir se autoriza ou não a coleta e o processamento de suas informações pessoais.

Inicialmente, faz-se necessário desconstruir essa noção individualista de autonomia, que a identifica com o conceito de capacidade jurídica e parte do pressuposto de que toda pessoa maior e capaz possui aptidão para praticar os atos da vida civil, desde que não sofra interferências prejudiciais por parte de terceiros. Essa perspectiva adota como premissa um suposto caráter independente e autossuficiente ao ser humano, típicas da modernidade.

Entretanto, a autonomia precisa ser compreendida como abertura ao outro, pois constituição do ser humano como sujeito exige que a pessoa transcenda sua singularidade e perceba-se como membro de um mundo comum a todos os seres (RENAUT, 2004, p. 61). Faz-se necessário reconhecer que a autonomia é influenciada pelas diversas relações estabelecidas pelas pessoas, o que inclui aquelas de carácter íntimo, cultural, institucional, nacional, global e ecológico (NEDELSKY, 2011, p.46).

Por conseguinte, o exercício adequado da autonomia pressupõe o estabelecimento de relações construtivas entre os seres envolvidos em determinadas situações. Para tanto, o Direito desempenha um papel essencial, ao estabelecer regras que estruturam tais relações entre as pessoas. A qualidade desse regramento poderá tanto promover quanto restringir o exercício da autonomia. Por outro lado, a proteção à privacidade e à autonomia estão relacionadas, porque perdas de privacidade tornam fácil para os outros interferir nas vidas daquelas pessoas, consoante destaca Clarissa Véliz (2020, p. 84). Com base em tais pressupostos, será analisada a atual disciplina europeia relativa aos contratos de fornecimento de produtos e serviços digitais, especialmente para aqueles contratos nos quais a única contraprestação exigida do destinatário de tais conteúdos consistiria na disponibilização dos dados pessoais.

Faz-se necessário reconhecer que o Regulamento Geral de Proteção de Dados europeu admite que nem toda manifestação de vontade será considerada livre, tendo em vista que o parágrafo 4 do art. 7° proíbe que a execução de um contrato dependa do consentimento para tratamento de dados que não guardam relação com aquele acordo. Em tais hipóteses, ao ter que optar entre o fornecimento de dados ou a não celebração do contrato, entende-se que o destinatário dos conteúdos e serviços digitais foi submetido a uma pressão que impediu o livre exercício de sua autonomia.

A doutrina alemã, entretanto, ao analisar o art. 3° da Diretiva Europeia n. 770/2019, que disciplina os contratos de fornecimento de conteúdos e serviços digitais, tem admitido a possibilidade de o usuário, a quem seja fornecido um conteúdo ou serviço digital, ao invés de pagar um preço, disponibilizar dados pessoais como contraprestação contratual, ou seja, realizar o chamado "pagamento com dados". Caso prevaleça esse entendimento, haverá a coleta de dados destinada a outra finalidade que não a execução do próprio contrato celebrado e, desse modo, será afastada a incidência da proibição de subordinação (*Kopplungsverbot*) fixada no Regulamento Geral de Proteção de Dados europeu, consoante restou demonstrado anteriormente.

O fornecimento de conteúdos e serviços digitais aparentemente gratuitos, mas que exigem como contraprestação a disponibilização de dados pessoais, tornou-se a principal forma de obtenção dessas informações para fins de identificação do perfil de determinadas pessoas (profiling), com o escopo de utilizá-lo para a elaboração de conteúdos personalizados, voltados para manipular a vontade do cidadão por meio de informações falsas e de propagandas dissimuladas como conteúdo jornalístico, de modo que essas práticas representam não apenas uma ameaça à liberdade de escolha do sujeito, como também a outros valores sociais relevantes, a exemplo da democracia, da igualdade e do respeito à diversidade.

Por conseguinte, a coleta e o processamento de dados pessoais têm sido utilizados não somente para conhecer o comportamento das pessoas, mas também para moldá-lo (ZUBOFF, 2020, p. 08), o que não se restringe ao âmbito da economia, uma vez que se tem buscado também influenciar o resultado das eleições e ameaçar os valores democráticos. Para tanto, são produzidas propagandas personalizadas e as notícias falsas (fake news). Tais instrumentos tem se mostrado bastante eficazes, em razão de todo ser humano ser vulnerável à manipulação, afinal ninguém tem acesso imediato à maior parte das informações que acessa (VÉLIZ, 2020, p. 95), de modo que é necessário ter certo grau de confiança no conteúdo do que está sendo divulgado como notícia.

A criação de conteúdos personalizados, com base nos dados fornecidos pelos cidadãos, tem contribuído para a formação de realidades paralelas e, por conseguinte, de grupos que possuem visões de mundo constituídas por perspectivas completamente diferentes, o que dificulta a comunicação e aumenta a polarização. Por outro lado, tal fenômeno passou a ser percebido como benéfico para os criadores de conteúdo digital, pois geram debates e discussões inflamadas, o que gera o denominado “engajamento”, assegurando a permanência das pessoas por mais tempo nas redes sociais, onde estarão expostas à influência e à manipulação de suas vontades.

Esse cenário impossibilita as pessoas de interagirem de forma construtiva e se torna bastante prejudicial ao desenvolvimento da cooperação entre os membros de uma sociedade, por meio da formação de consensos em torno de soluções para os problemas comuns que são rotineiros nos mais diversos agrupamentos humanos. A perda da privacidade, portanto, impõe dificuldades a que as pessoas possam escolher seus candidatos com base no que acreditam ser o melhor para a sua comunidade, sem que haja pressões ou influências indevidas.

Por outro lado, a constante vigilância/monitoramento das pessoas gera um constrangimento no que se refere ao exercício de direitos fundamentais, a exemplo das liberdades de associação, de pensamento e até mesmo a pesquisa sobre determinados assuntos, pois provoca o receio de que tais comportamentos, ao se tornarem conhecidos do público, possam vir a gerar preconceitos, discriminações e prejuízos à pessoa que o praticou.

Com a perda de privacidade provocada pela constante vigilância, as pessoas, ao se perceberem continuamente expostas, irão se sentir sempre pressionadas a nunca cometer um erro, com receio de que a falha venha a se tornar pública. Essa preocupação provoca retrações e conformidades, a chamada espiral de silêncio, em que os sujeitos evitam compartilhar opiniões minoritárias ou divergentes daquelas que predominam na sociedade, de modo a não correr o risco de sofrer isolamento social ou outras consequências negativas.

Portanto, existem importantes consequências provocadas pela perda de privacidade que são vivenciadas coletivamente, dentre as quais destacam-se os danos causados pela cultura da exposição à sociedade, à construção social, em virtude de estimular discriminações, ameaçar a segurança nacional e a própria democracia. Nesse contexto, Clarissa Véliz (2020). afirma que os dados pessoais são tóxicos, em razão de a sua utilização poder envenenar vidas individuais, instituições e sociedades, já que possui um relevante conteúdo sensível, relacionado à personalidade dos sujeitos, altamente suscetível de ser objeto de utilização indevida, difícil de ser mantido seguro, além de desejado por muitos, desde criminosos a companhias de seguro e agências de inteligência.

Tais comportamentos, praticados em nome da atual economia de dados (*data economy*), equivalem a verdadeiros atos de espionagem e direcionamento, de natureza econômica e social, e tem provocado a erosão da igualdade, da justiça e da democracia em diversos países do mundo (EMPOLI, 2022, p. 155).

Ademais, o modelo individualista, fundado no princípio da autodeterminação informativa tem se demonstrado insuficiente, uma vez que, na grande maioria dos casos, a autorização de acesso a conteúdo supostamente personalíssimos colocará em risco dados de terceiros que sequer manifestaram seu consentimento. O constante compartilhamento entre as pessoas de sentimentos, pensamentos e informações de natureza íntima as colocam em risco, uma vez que basta a autorização de acesso aos seus contatos por uma das partes para que as informações fornecidas por toda a sua rede social sejam acessadas pelos fornecedores de produtos e serviços eletrônicos (SHAEFFER; KEEVER, 2021, p. 294-295).

Outra crítica importante consiste na patrimonialização dos dados pessoais. Por mais que o legislador europeu tenha evitado o uso da expressão "contraprestação" no texto da Diretiva que autorizou o "pagamento com dados", não há dúvida de que se trata de uma retribuição contratualmente prevista pelo conteúdo fornecido ou serviço prestado, o que provoca um distanciamento entre a regra prevista para os contratos eletrônicos e a teleologia do Regulamento Geral de Proteção de Dados europeu, que trata tal conteúdo como direito fundamental. Constata-se, portanto, que os dados passaram a ser juridicamente reconhecidos, ainda que excepcionalmente, no âmbito da União Europeia, como ativo financeiro ou moeda de troca, de modo que tais operações assemelham-se a uma "venda" dos dados pessoais.

Contudo, faz-se necessário reconhecer, consoante afirma Clarissa Véliz (2020), que a interdependência entre as pessoas em matéria de privacidade implica que ninguém possui autoridade moral para vender seus dados pessoais, tendo em vista que tal conteúdo é composto por informações personalíssimas de outras pessoas. Portanto, não é possível ser titular de dados pessoais de forma semelhante à propriedade, já que tais informações não pertencem exclusivamente a apenas um ser humano.

A coleta, o armazenamento e o processamento de dados podem gerar outro relevante efeito negativo, que consiste na manutenção do conteúdo relativo à determinada pessoa na internet por um prazo indeterminado (eterno), o que dificulta o processo de esquecimento, essencial para a saúde mental de todo ser humano, bem como para o bem-estar social, afinal, o advento das novas tecnologias contribuiu para difundir e massificar memórias, reforçando a denominada memória coletiva.

A expressão direito ao esquecimento abrange duas principais vertentes. A primeira incide sobre informações que foram divulgadas no passado, em razão da sua importância, mas que perderam relevância, atualidade ou correção em face do decurso do tempo. Nesse caso, poderá haver uma colisão com outros direitos fundamentais, cuja solução deve dar prevalência aos aspectos existenciais vinculados à dignidade da pessoa humana (MARTINS, 2021, p. 22). A segunda vertente reconhece ao titular dos dados o direito de exigir o apagamento de suas informações pessoais ao final da execução do contrato.

Não se pode negar que, de um lado, há o interesse público em manter a memória de fatos pretéritos, reforçados pela liberdade de imprensa e de expressão, bem como pelo direito da coletividade à informação. Por outro lado, não se pode admitir que uma pessoa seja perseguida a vida inteira por eventos ocorridos no passado. Desse modo, consoante destaca

Guilherme Martins (2021), a nova divulgação de fatos pretéritos relativos a algum sujeito pode impedi-lo de autoconstruir sua identidade, ao mantê-lo preso ao seu próprio passado.

Ainda que possa haver um conflito de interesses, deve-se reconhecer o direito ao esquecimento como um direito fundamental, decorrente da cláusula geral de tutela da pessoa humana, (MARTINS, 2021, p. 08-09). Portanto, é importante permitir que a pessoa se reinvente e reconstrua a própria história, abandonando no passado fatos e comportamentos que não são mais compatíveis com a sua atual identidade. Para tanto, faz-se necessário assegurar o direito ao esquecimento no âmbito digital.

Para Stéfano Rodotá (2008), determinadas informações devem ser destruídas, enquanto outras precisam ser conservadas apenas de forma agregada e anônima, "uma vez que tenha sido atingida a finalidade para a qual foi coletada ou depois de transcorrido determinado lapso de tempo". Entretanto, mesmo dados anonimizados, a depender da forma como sejam tratados, podem permitir a identificação do titular de tais informações e, até mesmo o acesso a conteúdos sensíveis acerca de determinada pessoa, relacionados, por exemplo, às convicções políticas e religiosas, à opção sexual, ao histórico médico e às informações genéticas. Por conseguinte, nem mesmo a anonimização dos dados tem assegurado uma proteção adequada ao cidadão.

Em sentido semelhante, Clarissa Véliz (2020) defende a necessidade de se introduzir prazos para que os dados pessoais possam expirar e ser esquecidos no mundo digital, destacando que tais informações não devem ser deletadas com base em fundamentos ideológicos, mas somente com o objetivo de respeitar os direitos dos cidadãos. Nos casos em que se entender importante a preservação da memória, a autora defende a restrição de acesso.

No âmbito da União Europeia, o direito ao esquecimento foi previsto no art. 17 do Regulamento Geral de Proteção de Dados (UE 2016/679), cuja finalidade consiste no apagamento dos dados pessoais em diversas hipóteses, expressamente previstas. Ao comentar o referido dispositivo do Regulamento europeu, Boris P. Paal (2021) afirma que o direito ao esquecimento busca combater o fato de uma quantidade cada vez maior de informações pessoais estar sendo divulgada por todas as partes envolvidas e tal fenômeno provoca um significativo impacto sobre a pessoa em causa. Tal direito seria uma expressão do princípio da minimização de dados (Grundsatz der Datenminimierung), segundo o qual os dados pessoais devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados. Tal direito busca assegurar um tratamento justo e transparente.

No Brasil, há um conjunto normativo que disciplina a possibilidade de apagamento dos dados pessoais. O Código de Defesa do Consumidor proíbe que os cadastros e dados de consumidores contenham informações negativas por um período superior a cinco anos (§1° do art. 43). Já o Código Penal assegura, diante da reabilitação do condenado, o direito ao sigilo dos registros sobre o processo e a condenação (arts. 93 a 95). A Lei de Acesso à Informação, datada de 2011, em seu art. 31, estabelece que "o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais". Já o Marco Civil da internet, de 2014, reconhece, no inciso X do art. 7°, o direito da pessoa de solicitar a exclusão de suas informações pessoais ao término da relação contratual, bem como no inciso IV do art. 18, o direito dos titulares de exigir "anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei". A Lei Geral de Proteção de Dados (LGPD) fixou como regra a eliminação dos dados pessoais, após o término do seu tratamento, ressalvadas algumas hipóteses excepcionais (art.16).

Para Gisela Sampaio da Cruz Guedes e Rose Melo Vencelau Meireles (2019).

, não se deve confundir o efetivo apagamento de dados dos usuários, previstos no art. 7° do Marco Civil da Internet e no art. 16 da LGPD, com o direito ao esquecimento, compreendido como uma vedação à eterna divulgação pública de fatos pretéritos que envolvem uma pessoa

Em verdade, não houve, no âmbito da LGPD, o reconhecimento expresso do direito ao esquecimento, a exemplo do que fez o Regulamento europeu. Entretanto, uma interpretação sistemática dos dispositivos legais existentes, em consonância com a cláusula geral de tutela da pessoa humana, constitucionalmente prevista, permite concluir por sua existência no ordenamento jurídico brasileiro. Tal entendimento é reforçado pelo disposto nos incisos I e II do art. 6° do referido diploma legal, que reconhece expressamente o que a doutrina denomina de princípio da minimização dos dados[2].

[2] "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;"

Não obstante os dispositivos legais acima citados, bem como o entendimento majoritário na doutrina, consubstanciado em dois enunciados das Jornadas de Direito Civil[3], o Supremo Tribunal Federal, ao analisar o Caso Aída Curi (RE 1010606), em fevereiro de 2021, utilizou tal *leading case* para aprovar tema de repercussão geral, em que afirmou a incompatibilidade do reconhecimento de um direito ao esquecimento com a Constituição, "entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social analógicos ou digitais"[4].

Não obstante ter negado a existência de um direito genérico ao esquecimento, a Suprema Corte brasileira ressaltou, contudo, a possibilidade de aplicá-lo a situações expressas e pontuais em que o decurso do tempo pode autorizar a supressão de dados e informações, a exemplo daquelas previstas no Código Penal, no Código de Defesa do Consumidor e no Marco Civil da Internet, anteriormente citadas. Ademais, a decisão não abrangeu os pedidos de desindexação, que consiste em impedir determinado URL (Uniform Resource Locator) de constar no resultado de buscas, de modo a mitigar os danos sofridos por pessoas, em razão de tais páginas vinculá-las a conteúdos prejudiciais aos seus direitos personalíssimos.

Não se pode negar, entretanto, a importância de assegurar que as pessoas possam ressignificar a sua vida com base no esquecimento de acontecimentos passados que não mais correspondem à sua atual identidade. Por outro lado, é possível que a situação concreta exija uma solução que considere os direitos à liberdade de informação, de opinião e de imprensa, e dê prevalência aos últimos. O que não se deve conceber é um tratamento preferencial e apriorístico a determinados direitos, sem analisar as circunstâncias do caso concreto, afinal a interpretação jurídica não pode ser realizada de forma indiferente à realidade social.

---

[3] Enunciado 531: "A tutela da imagem e da honra da pessoa humana na Internet pressupõem o direito ao esquecimento, tendo em vista o ambiente da rede mundial de computadores, cujos meios de comunicação potencializam o surgimento de novos danos". Enunciado 576: "o direito ao esquecimento pode ser assegurado por tutela judicial inibitória".

[4] Tema 786 "É incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais - especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral - e as expressas e específicas previsões legais nos âmbitos penal e cível". Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786#:~:text=Decis%C3%A3o%3A%20O%20Tribunal%2C%20por%20maioria,Edson%20Fachin%20e%20Gilmar%20Mendes. Acesso em 28.02.2024.

Na Alemanha, a Corte Constitucional (*Bundesverfassungsgericht*) optou pelo caminho de estabelecer parâmetros para a aplicação do direito ao esquecimento e deixou a concretização mais pormenorizada para os tribunais especializados[5], que levarão em consideração os novos desenvolvimentos técnicos (KÜHLING, 2020, p. 08).

Uma análise exaustiva acerca da possibilidade de reconhecimento de um direito ao esquecimento no Brasil se afastaria do escopo deste tópico, cuja finalidade consiste em demonstrar os riscos do fornecimento indiscriminado de dados, uma vez que a coleta, o tratamento e o armazenamento de tais informações tem sido utilizados para moldar o comportamento dos cidadãos não somente em direção ao consumo de determinados produtos e serviços, como até mesmo para a escolha de candidatos a cargos políticos, em desrespeito à liberdade de escolha e aos princípios democráticos.

Ademais, restou demonstrado que existem dimensões, aspectos e efeitos coletivos da privacidade e dos dados pessoais que não são adequadamente protegidos por meio do princípio da autodeterminação informativa, o que exige uma reflexão acerca da necessidade de se ampliar as restrições não somente ao tratamento e ao armazenamento de dados, mas especialmente à coleta, consoante será analisado a seguir.

4 DA NECESSIDADE DE AMPLIAÇÃO DAS RESTRIÇÕES À COLETA E AO TRATAMENTO DE DADOS PESSOAIS

Ao longo do texto, foi demonstrada a coexistência de dimensões individuais e coletivas tanto para a privacidade quanto para os dados pessoais, o que comprova a necessidade de se reconhecer a existência de múltiplos legitimados a 99efende-los de possíveis violações, bem como a insuficiência do princípio da autodeterminação informativa, em virtude de se propor a disciplinar tão somente a esfera individual.

A noção de multititularidade foi desenvolvida para melhor regular situações jurídicas em que um bem possua mais de uma dimensão, com diferentes titulares reconhecidos como legitimados a defender seus respectivos interesses incidentes sobre cada uma delas, a exemplo do que ocorre com os bens comuns, que consistem naqueles que devem ser livremente

[5] BVerfG NJW 2020, 300 Rn. 147.

acessados – a exemplo da água e do software livre – ou naqueles sobre os quais incide mais de uma titularidade, a exemplo do imóvel tombado pelo patrimônio histórico, artístico ou cultural. Neste último caso, constata-se que, ao lado do direito de propriedade exclusivo sobre o bem, há o interesse coletivo na preservação de suas características históricas, culturais ou arquitetônicas.

O reconhecimento dos bens comuns tem sido tratado como uma profunda transformação no âmbito das categorias tradicionais do Direito. Para Ugo Mattei (2011), trata-se de um tipo de direito fundamental 'de última geração' desvinculado do paradigma dominial (individualístico) e autoritário (Estado assistencial). Já para Gustavo Tepedino (2019), tal categoria de bens deu origem a uma nova racionalidade, fundada na conexão entre as pessoas e suas racionalidades.

O advento das novas tecnologias provocou a desmaterialização dos bens, de modo que o modelo individualista de propriedade, caracterizado pela exclusividade e perpetuidade, tornou-se insuficiente para disciplinar as novas titularidades. Diante da constatação de múltiplas dimensões tanto para a privacidade, quanto para os dados pessoais, é possível identificar também múltiplos titulares.

A multititularidades de direitos encontra-se reconhecida no ordenamento jurídico brasileiro, em virtude da consagração dos bens difusos, cuja natureza não exclusiva provocou uma reestruturação normativa capaz de assegurar uma adequada tutela de tais direitos (GUILHERMINO, 2018, p. 80).

Por outro lado, a própria Lei Geral de Proteção de Dados brasileira menciona expressamente a possibilidade de se realizar a defesa dos interesses e dos direitos dos titulares de dados de forma individual ou coletiva (art. 22). Em seguida, ao tratar da responsabilidade e do ressarcimento dos danos, o referido diploma legal prevê a possibilidade de o exercício da atividade de tratamento de dados provocar danos individuais e coletivos, sendo admitida a propositura de ações coletivas voltadas para buscar a devida reparação.

Diante da existência de interesses coletivos merecedores de tutela no âmbito da privacidade e da proteção de dados, impõe-se uma indispensável reflexão acerca da disciplina jurídica considerada mais adequada acerca da nova dimensão desses direitos fundamentais, bem como o questionamento acerca da suficiência de sua categorização como bens jurídicos ou direitos subjetivos.

O tratamento dos dados pessoais como um bem jurídico facilita a sua objetificação e a consideração de que integra o patrimônio dos titulares (TEPEDINO; SILVA, 2020, p. 134), o que não pode ser considerado adequado, em razão de a privacidade e os dados pessoais conterem aspectos relacionados à personalidade do(s) sujeito(s) envolvido(s). A mesma crítica abrange a noção de direito subjetivo, concebida para legitimar a lógica da titularidade sobre bens patrimoniais (DONEDA, 2019, p. 129).

Clarissa Véliz (2020) realizou importante diagnóstico acerca dos aspectos coletivos da privacidade e dos dados pessoais, bem como dos riscos envolvidos em sua perda. Entretanto, os classifica como bens públicos, o que atrai para si a crítica acima exposta. Ademais, propõe como soluções para o problema da coleta em massa de informações personalíssimas que cada pessoa adote medidas preventivas, dentre as quais o uso de navegadores e aplicativos elaborados para proteger tais conteúdos do acesso por parte dos interessados. Tais propostas são insuficientes, pois, como a própria autora afirmou, basta que uma ou algumas pessoas atuem de forma pouco cuidadosa com seus dados pessoais para facilitar o acesso a informações de terceiros que com ela se relacionam.

Diante do exposto, constata-se a insuficiência das categorias jurídicas tradicionais para classificar os dados pessoais, o que dificulta a instituição de uma disciplina adequada. Como solução para tal problema, propõe-se, com base na obra de Pierre Dardor e Christian Laval, que os dados pessoais sejam compreendidos como comuns, de modo a afastar a incidência da lógica proprietária. Os referidos autores criticam a utilização da noção de bem comum, por entenderem que tal conceito parte da premissa antidemocrática de que caberia ao Estado, ou a sábios, o poder de definir o que assim deveria ser considerado, enquanto os "comuns" representam um princípio político – e não um bem – que decorre do exercício de atividades realizadas em prol do interesse da coletividade. Por essa razão, haveria uma coobrigação de todos em relação à preservação dos comuns, que se caracterizariam por serem inapropriáveis (2017, p. 28 e 250).

Não obstante tratar-se de um comum, o conteúdo dos dados pessoais não deve ser livremente acessado, pois essa prática pode vir a comprometer a liberdade, a intimidade e o bem-estar das atuais e futuras gerações. Há, portanto, uma necessidade premente de elaboração de um conjunto normativo que promova maior restrição de acesso a tais informações, bem como que resista às estratégias comerciais e à lógica proprietária.

Em razão de o Direito brasileiro não se resumir às normas positivadas deve ser admitida a classificação dos dados pessoais como comuns de acesso restrito (TEPEDINO, 2019, p. 32). Caberá à coletividade instituir regras relativas ao acesso e processamento de tais informações, em suas dimensões individual e coletiva, de modo a impedir a inadequada utilização de conteúdos comprometedores dos direitos fundamentais das presentes e futuras gerações.

Em virtude de os dados pessoais envolverem aspectos relacionados a diversos direitos humanos fundamentais – cujo conteúdo não se restringe a apenas um sujeito, já que possuem dimensões coletivas – não se pode admitir, de forma genérica, sua utilização como contraprestação contratual, sob pena de se legitimarem práticas abusivas que atacam as conquistas mais importantes da humanidade.

Por conseguinte, uma interpretação sistemática do ordenamento jurídico brasileiro permite que se chegue à conclusão de que os dados pessoais, ao serem tratados como direitos fundamentais, não admitem uma disciplina fundada na lógica patrimonialista, o que afasta a possibilidade de criação de uma regra semelhante àquela instituída no âmbito da União Europeia, no sentido de permitir, de forma genérica, a utilização de dados pessoais como contraprestação contratual, sob pena de ser reconhecida a sua inconstitucionalidade. Faz-se necessário aprofundar os debates em torno da temática, com ampla participação dos mais diversos setores da sociedade, de modo a restringir o acesso a conteúdo que possa vir prejudicar uma pessoa ou os membros da coletividade.

5 CONSIDERAÇÕES FINAIS

A admissão, de forma genérica, da possibilidade de fornecimento de dados pessoais como contraprestação contratual provoca um elevado incremento dos riscos de violação a direitos humanos fundamentais, em suas dimensões individuais e coletivas, e tem causado danos a importantes valores sociais, a exemplo da democracia, da igualdade e do respeito à diversidade.

Na Europa, uma interpretação sistemática das diretrizes e regulamentos vigentes tem sido realizada de modo a legitimar a possibilidade de cessão de dados pessoais como

contraprestação contratual, não obstante o Regulamento Geral de Proteção de Dados proibir que a execução do contrato dependa do consentimento do usuário para o tratamento de dados que não guardam relação direta com aquele acordo.

Nesse caso, entende-se que tal autorização para tratamento, nas hipóteses de fornecimento de conteúdo ou serviço digital "gratuito", configuraria uma exceção autorizada pelo ordenamento jurídico europeu. Contudo, o pagamento com dados consiste na principal estratégia utilizada pelos agentes econômicos e políticos para identificar o perfil dos usuários (perfilização/profilling) e, a partir de então, traçar estratégias e criar conteúdo voltado para influenciar e até mesmo moldar a vontade dos cidadãos em torno de interesses tanto individuais quanto coletivos, o que representa uma ameaça a ambas as dimensões.

Desse modo, faz-se necessário aprofundar os debates em torno da disciplina das relações contratuais eletrônicas, especialmente no que se refere ao fornecimento de dados pessoais como contraprestação contratual, de modo a restringir o acesso a conteúdo que possa vir a ser utilizados para prejudicar os direitos das presentes e futuras gerações.

REFERÊNCIAS

DARDOT, Pierre; LAVAL, Christian. **Comum**: ensaio sobre a revolução no século XXI. Trad. de Mariana Echalar. São Paulo: Boitempo, 2017.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2ª. ed. rev. e atual. Thompson Reuters Brasil, 2019.

EMPOLI, Giuliano Da. **Os engenheiros do caos**. Trad. de Arnaldo Bloch. São Paulo: Vestígio, 2022.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do Tratamento de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

GUILHERMINO, Everilda. **A tutela das multititularidades**: repensando os limites do direito de propriedade. Rio de Janeiro: Editora Lúmen Juris, 2018.

HAN, Byung-Chul. **Sociedade da transparência**. Trad. de Enio Paulo Giachini. Petrópolis, RJ: Vozes, 2017.

HERMIDA, Alberto J. Tapia. **La nueva normativa de consumo em españa y en la unión europea**. Madrid: Reus Editorial, 2022.

HOOFNAGLE, Chris Jay; SOLTANI, Ashkan; GOOD, Nathaniel; WAMBACH Dietrich J.; and AYENSON Mika D. Behavioral Advertising: The offer you cannot refuse. **Haward Law & Policy Review**, vol. 6, p. 273-296, 2012.

KLEIN, Naomi. Reclaiming the Commons. **New Left Rewiew**, n. 9, maio-jun. 2001. Disponível em: https://newleftreview.org/issues/ii9/articles/naomi-klein-reclaiming-the-commons. Acesso em 28.09.2023.

KÜHLING, Jürgen. **Das „Recht auf Vergessenwerden" vor dem BVerfG – November(r)evolution für die Grundrechtsarchitektur im Mehrebenensystem. NJW 2020. Disponível em: http://beck-online.beck.de/Bcid/Y-300-Z-NJW-B-2020-S-275-N-1. Acesso em 29.02.2024.**

KROSCHWALD, Steffen; POLENZ, Sven. § 6 Digitale Produkte und Datenschutz. In: Brönneke/Föhlisch/Tonner. **Das neue Schuldrecht**. 1. Auflage. Baden-Baden: Nomos, 2022.

LUNGUI, Sofia. Mais da metade da população mundial é usuária de redes sociais: Quase cinco bilhões de pessoas utilizam ativamente as redes sociais. Isso equivale a 61% da população global. In**: Tecnologia**. Disponível em: https://gizmodo.uol.com.br/mais-da-metade-da-populacao-mundial-e-usuaria-de-redes-sociais/. Acesso em 14.02.2024.

MARTENS, Sebastian. **Schuldrechtsdigitalisierung***:* Einfürung in die Änderugen des Kauf- und Verbraucherrechts, insbesondere in die Regelungen der Verträge über digitale Produkte (§§ 327 ff. BGB). München: C.H.Beck, 2022.

MATTEI, Ugo. **Beni Comuni**: un manifesto. Bari: Editori Laterza, 2011.

MARTINS, Guilherme Magalhães. O direito ao esquecimento como direito fundamental. **Civilistica.com**. Rio de Janeiro, a. 10, n. 3, 2021. Disponível em: <http://civilistica.com/o-direito-ao-esquecimento-como-direito/>. Acesso em 22.02.2024.

NEDELSKY, J. **Law's relations**: a relational theory of self, autonomy and law. New York: Oxford University Press, 2011.

PAAL, Boris P.; PAULY, Daniel A. **Datenschutzgrundverornung**: Bundesdatenschutzgesetzt. 3 Auflage. C.H.Beck: München, 2021.

RENAUT, A. **O indivíduo**. Reflexão acerca da filosofia do sujeito. 2 ed. Trad. Elena Gaidano. Rio de Janeiro: Difel, 2004.

RODOTÁ, Stéfano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

SCHULZ, Sebastian. Freiwillikkeit und kopplungsverbot (Abs. 4). In: GOLA, Peter; HECKMANN, Dirk. **Datenschutz-Grundverordnung. Bundesdatumschutzgesetz: Kommentar**. 3 Auflage. München: C.H.Beck, 2022.

SHAEFFER, John; KEEVER, Charlie Nelson. Privacy As a Collective Norm. 41 Loy. **L.A. Ent. L. Rev**. p.253-303, 2021.

TAEGER, Jürgen; GABEL, Detlev. Art. 7. Bedingung für die Einwilligung, Rn. 94. In: TAEGER, Jürgen; GABEL, Detlev. **DSGVO – BDSG – TTDSG: Kommentar**. 4. Auflagen. Frankfurt am Main: Fachmedien Recht und Wirtschaft, 2022.

Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten. Dresden: Staatsbetrieb Sächsische Informatik Dienste, 2019. Disponível em: https://www.zaftda.de/tb-bundeslaender/sachsen/landesdatenschutzbeauftragter-6/750-20-tb-lfd-sachsen-2019-o-drs-nr-vom-22-12-2020/file. Acesso em 13.02.2024.

TEPEDINO, Gustavo. Acesso aos direitos fundamentais, bens comuns e unidade sistemática do ordenamento. In: MATOS, Ana Carla Harmatiuk; TEIXEIRA, Ana Carolina Brochado; TEPEDINO, Gustavo. **Direito civil, constituição e unidade do sistema**: anais do congresso internacional do direito civil constitucional. V Congresso do IBDCivil. Belo Horizonte: Fórum, 2019.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Novos bens jurídicos, novos danos ressarcíveis: análise dos danos decorrentes da privação do uso. **Revista de Direito do Consumidor**. vol. 129, p. 133-156, Maio-Jun. 2020.

VÉLIZ, Clarice. **Privacy is power**: why and how you should take back control of your data. Peguin Random House: Londom, 2020.

ZUBOFF, Shoshana. **The age of surveillance capitalism**. New York: PublicAffairs, 2020.