PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

ARTIGO CIENTÍFICO

COLETA E MONETIZAÇÃO DE DADOS PESSOAIS NA ESFERA DIGITAL: AMEAÇA AO DIREITO À PRIVACIDADE E À AUTODETERMINAÇÃO INFORMATIVA

ORIENTANDA: ESTER MIURA FREITAS PAIXÃO

ORIENTADOR: PROF. DOUTOR FAUSTO MENDANHA GONZAGA

GOIÂNIA-GO
2025

ESTER MIURA FREITAS PAIXÃO

COLETA E MONETIZAÇÃO DE DADOS PESSOAIS NA ESFERA DIGITAL: AMEAÇA AO DIRETO À PRIVACIDADE E À AUTODETERMINAÇÃO INFORMATIVA

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás.
Prof. Orientador: Dr. Fausto Mendanha Gonzaga.

GOIÂNIA-GO
2025

ESTER MIURA FREITAS PAIXÃO

COLETA E MONETIZAÇÃO DE DADOS PESSOAIS NA ESFERA DIGITAL: AMEAÇA AO DIREITO À PRIVACIDADE E À AUTODETERMINAÇÃO INFORMATIVA

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientador: Prof. Dr. Fausto Mendanha Gonzaga Nota

_____

Examinadora Convidada: Profª. Dra. Jumária Fernandes Ribeiro Fonseca Nota

COLETA E MONETIZAÇÃO DE DADOS PESSOAIS NA ESFERA DIGITAL: AMEAÇA AO DIREITO À PRIVACIDADE E À AUTODETERMINAÇÃO INFORMATIVA

Ester Miura Freitas Paixão[1]

O presente artigo investigou os impactos da coleta e monetização de dados pessoais na esfera digital, com foco nos ricos dessas práticas ao direito à privacidade e à autodeterminação informativa. Por meio de uma metodologia bibliográfica, que incluiu o levantamento de legislações, doutrinas, monografias e artigos acadêmicos para embasar a temática, o trabalho objetivou, em um primeiro momento, compreender as interpretações e conceitos acerca do direito à privacidade, bem como as regulamentações a ele associadas. Ademais, buscou-se investigar as técnicas utilizadas nas coletas de dados e como essas afetam a proteção dos direitos individuais, sobretudo a privacidade e a autodeterminação informativa. Além disso, o estudo examinou os aspectos mercadológicos envolvidos na captura e monetização de dados pessoais e discorreu sobre os efeitos da vigilância digital nos direitos fundamentais dos indivíduos. Por fim, a pesquisa concluiu que as atividades que envolvem o tratamento de dados pessoais representam desafios à proteção dos direitos fundamentais, sobretudo a necessidade de uma regulação robusta e eficaz para assegurar o direito à privacidade e a autonomia informativa dos indivíduos.

Palavras-chave: Coleta. Monetização. Dados pessoais. Privacidade. Autodeterminação informativa.

[1] Acadêmica do Curso de Direito da Pontifícia Universidade Católica de Goiás.

SUMÁRIO

INTRODUÇÃO

O avanço das tecnologias digitais e a expansão da coleta e do mercado de dados pessoais levantam questões cruciais sobre o direito à privacidade e à autodeterminação informativa. A crescente circulação e comercialização de dados e o estímulo à decisões automatizadas, pautadas em sistemas preditivos de supervisão, persuasão e controle de práticas que incidam no desempenho mercadológico, motivam uma análise crítica dos dispositivos nacionais que regulamentam a privacidade e a proteção de dados pessoais e se esses têm efetivamente resguardado os direitos individuais contra manipulações indevidas dos atuais insumos informacionais.

Dessa economia informacional, emergiu uma privacidade dúbia e vulnerável e o paradoxo funcionamento das tecnologias, pautadas na modernização e na conveniência da vida digital, acabam por mitigar os aspectos da vida privada, quando do rastreamento, armazenamento e a monetização de dados pessoais.

No âmbito nacional, essa realidade levou às medidas legislativas adequadas, de modo que, na Constituição Federal e em legislações infraconstitucionais específicas, a privacidade passou a ser considerada um direito fundamental e um direito da personalidade, elevada inclusive ao patamar de cláusula pétrea pela CF/88.

Tamanha a necessidade de adequação do tema aos novos ditames do ciberespaço, sobretudo no que tange às atividades decorrentes da utilização de dados pessoais, que foi aprovada a Emenda Constitucional n. 115/2022, a qual incluiu no art. 5º da CF/88 a proteção de dados no meio digital como direito fundamental.

Importante ressaltar que a privacidade ganha novos contornos na sociedade da informação e os avanços tecnológicos e sociais mudam constantemente sua concepção. Atualmente, esse direito perpassa o entendimento de o titular de dados decidir, ao menos minimamente, de forma consciente, o fluxo de suas informações pessoais, o que demandou a criação de legislações específicas como o Marco Civil da Internet e a Lei Geral de Proteção de Dados.

Por fim, a forma como a privacidade tem sido recepcionada pelo ordenamento jurídico brasileiro e o modo como ela se manifesta nas relações indivíduo e tecnologia, propõe reflexões sobre a necessidade de regulamentações mais robustas e de

práticas de proteção de dados que assegurem um equilíbrio entre inovação tecnológica e direitos individuais.

1 DIREITO À PRIVACIDADE

1.1 DEFINIÇÕES E CONTEXTUALIZAÇÕES

A promulgação da Constituição brasileira de 1988 consagrou a dignidade da pessoa humana como um de seus pilares e nesse viés, passou a disciplinar expressamente sobre o direito fundamental à privacidade.

Ao tratar do assunto, o constituinte incluiu entre as garantias e direitos fundamentais elencados no artigo 5°, inciso X da CF/88, a proteção da “intimidade” e da “vida privada”, as quais, juntamente com a “imagem” e a “honra”, norteiam aspectos inerentes a privacidade dos cidadãos, sendo esses fundamentos maximizados, na própria Carta Constitucional, em seu artigo 60, § 4º, IV, ao status de cláusula pétrea.

O direito à privacidade expresso na Constituição encontra-se nas expressões "intimidade" e "vida privada". Embora esses termos sejam frequentemente considerados sinônimos no discurso cotidiano e em diversos textos legais e jurisprudenciais, a doutrina cuidou de interpretá-los e diferenciá-los.

É que o direito à intimidade abarcaria o intrínseco da pessoa, seus aspectos subjetivos e mais íntimos, incluindo o modo de ser, as relações familiares e amizades, enquanto a vida privada abrangeria os demais aspectos, inclusive objetivos, atinentes às relações individuais, como as comerciais e as de trabalho, pertencentes às esferas privadas (MORAES, 2020, p. 151; VASCONCELOS, 2017, p. 233). Essa distinção, na percepção de Moraes, demonstra o vínculo entre os conceitos de intimidade e vida privada “por meio da menor amplitude do primeiro, que se encontra no âmbito de incidência do segundo.” (MORAES, 2020, p. 151).

O Código Civil de 2002, em semelhante viés constitucional, previu, em seu artigo 21, em capítulo reservado aos direitos da personalidade, a inviolabilidade da vida privada da pessoa natural, direito esse inalienável, indisponível, intransmissível e irrenunciável, protegido contra qualquer forma de abuso ou violação, sendo possível

a adoção de providências necessárias para impedir ou fazer cessar ato contrário à mencionada norma.

Depreende-se, portanto, que os textos legais, apesar de não conceituarem o termo privacidade, especificaram suas espécies, quais sejam: a intimidade, vida privada, honra e imagem.

Essa orientação da privacidade rememora as mais diversas relações humanas. Em uma percepção histórica, Doneda (2020, p. 83) recorda que a privacidade, hoje codificada, foi objeto de previsões em sociedades antigas como na Grécia e China antigas, bem como em tribos hebraicas e em sociedades iliteratas, porém, eivadas pelas concepções e contextos históricos próprios de cada sociedade.

Ainda, para Doneda (2020, p. 80-83), é possível identificar a evolução do tema sob uma dicotomia público-privada, através da delimitação da propriedade privada. Nesse cenário, em uma análise temporal, “[...] o surgimento do conceito de privacidade coincide com a desagregação da sociedade feudal e com o crescimento da classe burguesa em um contexto de mudanças sociais e econômicas relacionadas à Revolução Industrial. Época em que o isolamento era privilégio de poucos.” (NAVARRO, 2014, *apud* GHISLENI, 2015, p. 17).

Cabe rememorar, conforme citaram Simão Filho e Schwartz (2016, p. 8) o pioneirismo dos advogados Warren e Louis Brandeis ao inaugurarem juridicamente e doutrinariamente a abordagem do direito à vida privada, com o artigo *The Right to Privacy*, publicado em 1890. Por meio dele, os advogados investigaram o direito do resguardo à vida privada diante das notórias invasões a ela perpetradas, especialmente no que diz respeito às intromissões dos meios de comunicação impressos e à publicação de fotografias instantâneas, tecnologias difundidas há época do estudo.

Nessa perspectiva, Gazolla (2020, p. 64) aponta que necessário se fez maior aperfeiçoamento, em âmbito mundial, sobre a tutela do direito à privacidade, o qual notavelmente foi reconhecido no artigo 12 da Declaração Universal dos Direitos do Homem em 1948. Posteriormente, esse direito foi incorporado a pactos, convenções e documentos internacionais, como na Convenção Americana sobre Direitos Humanos, que assim como a Declaração Universal coibiu, sobre qualquer cidadão, ingerências arbitrárias e abusivas de sua vida privada, de sua família, de seu domicílio, sua correspondência e ofensas ilegais à sua honra e reputação.

Em âmbito nacional, a matéria se revelou de maneira mais explícita na legislação do Marco Civil da Internet e, posteriormente, na Lei Geral de Proteção de Dados. Contudo, a materialização jurídica do tema, nos dizeres de Branco e Mendes (2021, p. 548-549) ainda é imprecisa, não taxativa, sem uma definição exata acerca do direito à intimidade e à vida privada.

Por outro lado, Doneda (2020, p. 80-81) entende que apesar de referida definição ser incerta, é pertinente o uso do termo específico privacidade, o qual contempla os valores atribuídos aos vocábulos intimidade e vida privada, sendo por vezes, desnecessário se conferir rígida diferenciação entre mencionados conceitos, considerando que são tratados pela doutrina com enfoque na identidade havida entre eles.

Portanto, a noção do que se entende por privacidade se adequa às mudanças tecnológicas e sociais próprias de cada contexto histórico e cultural vivenciado e o ordenamento jurídico deve estar apto a recepcioná-la e adaptar-se constantemente.

1.2 PRIVACIDADE À LUZ DA LGPD

A tendência mundial em concretizar juridicamente a proteção de dados frente à ressignificação da privacidade na sociedade da informação, fez com que os países se despertassem para a necessidade de se adotarem iniciativas legislativas pátrias que buscassem minimizar o desafio que é efetivar a preservação mínima da privacidade e do direito de os cidadãos disporem de seus dados ao utilizarem dos meios eletrônicos como suporte para diversas funcionalidades.

Nessa conjuntura, como expôs Gazzola (2020), a *General Data Protection Regulation* (GDPR), editada em 2016 e aplicada em 2018, como a regulação geral europeia sobre dados pessoais, vislumbrou normas a serem efetivadas em toda União Europeia no intuito de equacionar a privacidade e o aclamado progresso tecnológico. O regulamento, ainda em vigor, tem como premissa o consentimento livre, explícito e esclarecido do titular de dados, bem como princípios como licitude, lealdade e transparência.

Em uma perspectiva nacional, a promulgação do “Marco Civil da Internet”, lei n.º 12.965, de 23 de abril de 2014, inaugurou explicitamente a proteção da privacidade

e dos dados pessoais. O diploma estabeleceu diretrizes, princípios, garantias, deveres, fundamentos e objetivos do uso da internet no país, com enfoque na liberdade de expressão e na privacidade, bem como as obrigações e sanções aplicadas ao descumprimento dos comandos da lei.

Embora o Marco Civil da Internet tenha sido um avanço para proteção do titular de dados, o tratamento de dados, com maior abrangência e especificações, foi efetivamente regulamentado na Lei Geral de Proteção de Dados (LGPD), instituída pela Lei nº 13.709, publicada em 2018.

O regramento da LGPD, influenciado pela GDPR, se organiza como uma espécie de manual técnico, no qual são delimitados conceitos, fundamentos, princípios, condições para o tratamento de dados e possíveis sanções para infrações cometidas às normas previstas na Lei.

A lei, dispondo sobre o tratamento de dados pessoais da pessoa natural, por pessoas físicas ou jurídicas, de direito público ou privado, logo em seus artigos 1º e 2º demonstra seu objetivo de proteger os direitos fundamentais de liberdade e de privacidade, bem como os direitos da personalidade e a inviolabilidade da intimidade, da honra e da imagem, adotando como fundamentos que merecem destaque, a privacidade e a autodeterminação informativa.

Nesse sentido, a LGPD dispõe o seguinte em seus artigos 1º e 2º:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
>
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.
>
> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I - o respeito à privacidade;
>
> II - a autodeterminação informativa;
>
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV - a inviolabilidade da intimidade, da honra e da imagem; [...]

O artigo 5º da lei em comento cuidou listar as definições dos principais termos envolvendo as atividades sobre as quais os dados estão submetidos, cabendo aqui transcrever os seguintes:

> Art. 5º Para os fins desta Lei, considera-se:

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
>
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
>
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; (...)
>
> IX - agentes de tratamento: o controlador e o operador;
>
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; [...]

O dado pessoal, conceituado como informação relacionada à pessoa natural identificada ou identificável e o dado pessoal sensível, assim definido por englobar informações mais íntimas do indivíduo, tais quais as referentes à religião, origem étnica, saúde e vida sexual, revelam que o objeto da lei não se limita à proteção dos dados em si, mas do próprio titular desses dados, considerado vulnerável à violação de sua privacidade.

Na LGPD, o protagonismo conferido ao titular também se manifesta por meio do consentimento exigido nas hipóteses legais de tratamento de seus dados pessoais, em especial os sensíveis. É o que se observa pelos artigos 7º e 11º da LGPD, os quais elegem o consentimento como a chave para a autodeterminação informativa do cidadão, “[...] significando que, ao se abrir mão parcialmente de sua privacidade para se inserir na era digital, deve ser resguardado o direito ao ser humano de um controle — mesmo que mínimo — de suas informações.” (CAMURÇA; MATIAS, 2021, p. 13).

Nessa perspectiva, o artigo 5º, inciso XII da legislação em análise, define consentimento como a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.

Assim, é possível perceber a valoração da demonstração da vontade do detentor dos dados em cedê-los. Vontade essa que deve ser livre e obtida mediante a consciência prévia e expressa do usuário, informando-lhe sob quais condições e para

quais finalidades específicas está fornecendo seus dados, sendo vedado o vício de consentimento e termos genéricos para o tratamento dos dados.

Além disso, a LGPD estabelece uma base principiológica em seu artigo 6º, cabendo destacar os princípios da finalidade, necessidade, adequação, livre acesso, transparência e segurança, todos devidamente delimitados e conceituados no texto legal. Esses princípios, em suma, orientam a legalidade das operações envolvendo o tratamento de dados, as quais devem pautar-se pela coleta e utilização de informações de forma clara, justificada e estritamente necessária, evitando excessos e assegurando o atendimento ao propósito específico a que se destinam.

Cabe ressaltar que o acesso facilitado às informações referentes ao tratamento de dados, a serem disponibilizadas de forma clara, adequada e ostensiva, é direito conferido ao titular de dados no artigo 9º da LGPD. Por sua vez, o artigo 42 e subsequentes tratam da responsabilização do controlador ou operador pelos danos causados no exercício da atividade do tratamento de dados ou pela violação da legislação aplicável.

A ideia da LGPD é, portanto, garantir que, ao lidar com dados, as entidades responsáveis cumpram obrigações para preservarem os direitos fundamentais do titular, notadamente sua privacidade. Nessa lógica, busca-se assegurar que o tratamento seja realizado de maneira ética, transparente e segura, a fim de evitar que o uso inadequado ou não autorizado dos dados resulte em danos à pessoa, afetando aspectos de sua identidade, dignidade e liberdade.

Nesse contexto, apesar de a LGPD, em comparação com o Marco Civil da Internet, aparentar maior especificidade quanto à delimitação da privacidade, na prática, observaram Fonseca e Mendes (2020) a limitação de um texto legal norteado pelo consentimento e por princípios que aclamam à autodeterminação informativa. Isso, porque o aparato digital se autorregula diariamente, em uma lógica de transação informacional, na qual o titular de dados, mesmo conhecendo as finalidades do tratamento, não consegue mensurar os riscos à sua personalidade advindos da captação e circulação de seus dados.

Portanto, a LGPD não é taxativa e a sua promulgação demostra que o aparato legal deve estar apto ao aperfeiçoamento conjunto com a evolução digital, buscando-

se garantir a privacidade dos indivíduos pela conciliação entre os interesses envolvidos em uma relação informacional desigual.

2 COLETA DE DADOS E DIREITO À AUTODETERMINAÇÃO INFORMATIVA

2.1 ASPECTOS SOBRE AS TÉCNICAS DE COLETAS DE DADOS

O rápido avanço das facilidades e ferramentas *online* inseriu no cotidiano das pessoas processos em que empresas e até governos extraem e acumulam grandes volumes de informações sobre os cidadãos, com diversos objetivos, especialmente para a aplicação em estratégias mercadológicas e comportamentais.

À medida que aproveitam os inúmeros serviços disponíveis, os indivíduos estão constantemente expostos à captura de seus dados. O preenchimento de formulários, a concessão consciente ou inconsciente de informações e a formalização de contratos por meio de simples “cliques” de concordância com os famosos “termos de privacidade”, são etapas exemplificativas de como recorrentemente, diversos registros — e-mail, CPF, número de telefone, escolaridade, estado civil, preferências e gostos pessoais — são fornecidos e posteriormente manipulados e processados, compelindo os usuários a aceitarem as condições das coleta de seus dados para acessarem serviços essenciais.

Depreende-se, por meio dos conceitos trazidos nos incisos I e II do artigo 5º da LGPD, que parte significativa do que circula no ambiente digital pode ser considerado dado pessoal, pois diz respeito às informações vinculadas a uma pessoa física, seja ela identificada ou passível de identificação.

Nessa lógica, todas as ações individuais no ciberespaço resultam em registros em vastos bancos de dados, gerenciados por meio do processamento de dados organizados e não organizados, de modo que assim dispuseram Simão Filho e Schwartz:

> Informações que resultam em dados estruturados são aquelas objetivamente coletadas e dirigidas, passando a formar um banco de dados específicos. Por sua vez, o conjunto de informações truncadas ou não, que compõem um conceito de dados não estruturados, decorrem tanto da captação autorizada ou não (por meio de cookies ou outra forma tecnológica), dos rastros digitais

> deixados pelo usuário em internet, quando este trafega em páginas e sites ou, ainda, por sistema de telefonia ou qualquer outro meio eletrônico de comunicação. (SIMÃO FILHO; SCHWARTZ, 2016, p. 5)

Diante disso, o rápido aprimoramento da coleta, tratamento e a aplicação desses dados, motivou a promulgação da Emenda Constitucional n. 115/2022, a qual incluiu no art. 5º da Constituição Federal, por meio do inciso LXXIX, o direito à proteção dos dados pessoais, assegurado nos termos da lei, inclusive nos meios digitais.

A trajetória percorrida por esse dado pessoal protegido constitucionalmente, seja ele estruturado, ou seja, aquele não precisa de maiores processamentos, ou não estruturado, submetido a um processo de análise e interpretação, foi subdividida por Colombo e Neto nos conceitos de dado, informação e conhecimento pelo seguinte exemplo:

> O número de curtidas pelos internautas sobre um vídeo musical postado na rede mundial de computadores é meramente um dado. Atribuir a este número a compreensão que revela a plena aceitação do músico ou, quem sabe, a sua rejeição, é uma informação. Já promover ou não a contratação do artista para ligar o nome e a imagem à determinada marca ou organização é conhecimento, pois representa tomada de decisões. (COLOMBO; NETO, 2017, p. 4)

Nesse cenário, explicita Bioni (2019, p. 56) que a dinâmica de formação de um banco de dados revela um processo de coleta e organização dos dados, passa pela extração de informações e, por fim, culmina na geração de conhecimento, o que influencia sobretudo na tomada de decisões.

Nas etapas de captação, condicionamento e processamento de dados, a participação do usuário se manifesta apenas na fase inicial, a de geração de dados, e pode ocorrer de forma ativa ou passiva. Na primeira, o indivíduo, em tese conscientemente, fornece seus dados a um terceiro. Já na forma passiva, o fornecimento é inconsciente, e se opera por exemplo, por meio de cliques para se obter mais informações, garantindo dados de comportamentos que serão manejados fora do alcance do usuário (JORGETTO, MARTINS e SUTTI, 2019, p. 6).

Dentro desse ciclo que envolve diversos passos subsequentes, cabe mencionar, conforme analisou Zuboff (2021, p. 90-91), o pioneirismo da Google, a qual, por meio de suas técnicas de coleta de dados, reconheceu que o fluxo contínuo de dados comportamentais gerados por seus usuários poderia resultar em um constante aprendizado e aprimoramento de seus serviços. A empresa passou a aproveitar informações que surgiam como subprodutos das interações dos usuários, chamadas de “*data*

exhaust", e a reutilizá-las para aprimorar sua atividade e criar novos produtos, de modo que esse processo permitia que os algoritmos da empresa aprendessem a oferecer resultados de busca cada vez mais relevantes e precisos (ZUBOFF, 2021, p. 90-91).

Dentre as várias técnicas utilizadas, os *cookies* se destacam como ferramentas amplamente aplicadas nas coletas de dados e funcionam como elementos-chave na vigilância digital.

Nessa perspectiva, a Autoridade Nacional de Proteção de Dados (ANPD), por meio do Guia Orientativo sobre os Cookies e Proteção de Dados Pessoais, (ANPD, 2022, p. 6) dispõe que os *cookies* são pequenos arquivos instalados nos dispositivos de um usuário após alguma atividade online, os quais permitem a coleta de dados, o armazenamento de preferências previamente registradas, o reconhecimento do usuário, a aferição de audiência e a segmentação de publicidade. Essas informações, quando combinadas, criam perfis comportamentais, o que sujeita a utilização de *cookies* e tecnologias semelhantes às disposições da LGPD (ANPD, 2022, p. 8-9).

Esses arquivos de monitoramento e aperfeiçoamento podem ser divididos em diversas categorias e variam de acordo com sua finalidade, necessidade e período de retenção. Dessa forma, quando selecionados, podem ser empregados para diversos objetivos, por tempo determinado ou indeterminado, tanto para melhorar o desempenho do próprio site, quanto para monitorar a atividade dos usuários, seus hábitos de navegação, direcionar anúncios personalizados ou até para partilha de dados com sites diferentes do visitado originalmente (ANPD, 2022, p. 9).

Nesse cenário, a transformação no tratamento de dados pessoais se fundamenta em novos mecanismos e algoritmos e envolve especialmente a criação de perfis de comportamento com base em informações fornecidas sobre um indivíduo, em um processo denominado *profiling*, o qual, por meio de estatísticas e inteligência artificial, gera uma "metainformação", que reúne padrões de costume, predileções, tendências e outros dados úteis sobre a vida de uma pessoa (DONEDA, 2021, p. 148-149).

Diante disso, as coletas de dados compõem as mais variadas técnicas de captação, por simples navegações *online*, para posterior refino e aplicação, sobretudo comercial, das informações obtidas. Há, portanto, um ciclo de coleta, no qual se

investe em formas de captar os dados, que serão cedidos pelo indivíduo ao usufruir, gratuitamente ou onerosamente por serviços, viabilizando o reinvestimento em novas formas de se atrelar o titular do dado à conteúdos e serviços, o que revela potenciais ofensas à direitos fundamentais individuais.

2.2 AUTODETERMINAÇÃO INFORMATIVA E CONSENTIMENTO NAS COLETAS DE DADOS

O consentimento e a autodeterminação informativa, fundamentos da Lei Geral de Proteção de Dados Pessoais (LGPD) são princípios essenciais para as discussões sobre a legalidade da coleta e tratamento de dados pessoais.

A ideia trazida pela normativa é que ao fornecer consentimento, o indivíduo, por ato livre e inequívoco, passível de revogação, tenha plena consciência dos dados que estão sendo coletados, para quais finalidades, por quem serão utilizados e por quanto tempo serão armazenados, em uma lógica de que o titular seja capaz de autorregular suas informações pessoais.

Sobre o tema, a doutrina tem se manifestado nos seguintes termos:

> Historicamente, a proteção dos dados pessoais tem sido compreendida como o direito de o indivíduo autodeterminar as suas informações pessoais: autodeterminação informacional. Recorre-se, por isso, à técnica legislativa de eleger o consentimento do titular dos dados pessoais como seu pilar normativo. Por meio do consentimento, o cidadão emitiria autorizações sobre o fluxo dos seus dados pessoais, controlando-os. (BIONI, 2019, p. 28)

O protagonismo dado ao consentimento levou aos provedores de plataforma na internet a disponibilizarem suas políticas de privacidade, por meio das quais o titular deveria tomar conhecimento amplo de toda a atividade que envolverá a informação fornecida, de modo que observa Ghisleni:

> A maneira como os dados dos usuários são tratados pelos sistemas está prevista nas normas que regulam o seu uso. Estas normas, geralmente descritas em documentos denominados ‘Termo de Uso’ ou ‘Política de Uso’, demandam adesão para possibilitar o acesso aos serviços. (GHISLENI, 2015, p. 13)

Nesse viés de ciência e decisão a ser tomada pelo titular do dado, a doutrina analisa que o direito assegurado à vida privada possui não só um aspecto negativo em se evitar intromissões alheias, mas também positivo, ao “[...] assegurar à pessoa

o controle do que deve ser conhecido e o que não deve ser conhecido pelos demais, expressão da liberdade que lhe é intrínseca.” (GAZOLLA, 2020, p. 68).

Nesse cenário utópico de pleno conhecimento e efetivo poder de escolha do usuário, Bruna Oliveira pontua o que segue:

> O “Direito de Decidir” consiste na possibilidade de deliberar a respeito da utilização dos dados e, ao fazê-lo, garantir que a informação chegue sem manipulação pelas plataformas utilizadas, viabilizando a formação da opinião sem influências indevidas e permitindo que se tome uma decisão apenas pelo exercício da autonomia individual, não pela condução do padrão comportamental por intermédio da inteligência artificial. Considerando que a autodeterminação é um ato ou efeito de decidir por si, tem-se que a autodeterminação informativa corresponde aos aspectos decisórios no exercício da autonomia individual em relação à informação. (OLIVEIRA, 2020, p. 4).

Doutrinariamente, se recorda que a autodeterminação informacional foi reconhecida pela Suprema Corte alemã, em 1980, como “o poder do indivíduo de deliberar sobre a divulgação de seus dados pessoais, escolhendo a quem serão divulgados e com quais finalidades podem ser usados” (OLIVEIRA, 2020, p. 6). No entanto, o exercício desse direito tem se revelado um desafio diante das transformações nos métodos de coleta e processamento de dados pessoais, impulsionadas pela informatização.

Seguindo essa perspectiva, entendem Fonseca e Mendes (2020) que o indivíduo consentir com as práticas da coleta informadas, funciona como uma espécie de simulação. Isso porque, a inépcia das políticas de privacidade se revela pela incapacidade de o titular de dados sopesar, no momento da leitura dos termos, os efetivos riscos à sua privacidade, pela existência da cláusula do “*take it or leave it*”, já que não possuem outra escolha caso almejem usufruir do serviço disponibilizado.

Ademais, mesmo inteirado das condições da coleta, é inviável que o usuário mensure as posteriores etapas de processamento e gerenciamento de seus dados, as quais podem até mesmo exceder as finalidades para as quais se destinavam (FONSECA; MENDES, 2020).

Nessa mesma perspectiva, menciona Bruno Bioni: “o fluxo das nossas informações pessoais é exponencial e os caminhos por ele percorrido estão, em tese, descritos nas políticas de privacidade, cujos textos são longos, de difícil compreensão e nos deixam poucas escolhas.” (BIONI, 2019, p. 27).

Além disso, cabe lembrar que na maioria das vezes, são disponibilizadas finalidades genéricas e imprecisas, incompatíveis com parte do texto legal ou distintas do real destino atribuído ao dado coletado, situação que distancia cada vez mais a administração do titular sobre seus dados e torna nulo o suposto consentimento oferecido.

Diante do exposto, o consentimento, a autodeterminação informativa e a transparência, pilares da LDPD, passam a se revelar como instrumentos de eficácia questionável nas relações assimétricas entre o operador de serviços e o titular de dados.

A construção de uma esfera pessoal, na qual a liberdade de escolha e o desenvolvimento da personalidade estão em ameaça, é comprometida quando não há uma garantia do real consentimento do titular, o qual, muitas vezes sem controle sobre a primeira fase de fornecimento das informações, se distancia cada vez mais da capacidade de gerenciar os próximos caminhos percorridos por seu dado.

2.3 EFEITOS DA COLETA DE DADOS NA PRIVACIDADE E NA AUTODETERMINAÇÃO INFORMATIVA

Cada vez mais, as atividades de processamento de dados têm ingerência na vida das pessoas e as interferências externas que se manifestam por diversos meios: anúncios, mensagens, ligações e *spams* indesejados são exemplos perceptíveis de como a vida privada das pessoas deixou de ser um campo inviolável.

As ferramentas tecnológicas que adentram na privacidade, coletam, interpretam e transmitem informações geradas em mediações digitais, são de extrema valia para composição de perfis retidos em bancos de dados que serão constantemente atualizados para fins de direcionamento de publicidade, aferição de comportamentos e para finalidades futuras e incertas (SIMÃO FILHO; SCHWARTZ, 2016, p. 13).

Percebe-se que até mesmo a dimensão emocional dos usuários não foge do monitoramento e interpretação de dados não estruturados. Textos com cunho ideológico, conversas, áudios, ícones, imagens, expressões faciais e postagens que

revelam sentimentos, abastecem bancos que irão minerar e rentabilizar as emoções pessoais (BIONI, 2019, p. 45-46).

Essas práticas, realizadas sem o efetivo consentimento e na maioria das vezes de forma excessiva, impacta diretamente a privacidade e a autodeterminação informativa, pois as empresas e organizações passam a alcançar e acumular dados sensíveis sobre a vida dos usuários, o qual perde o controle sobre suas informações e está sempre sujeito ao risco de abusos, como o uso desmedido ou a venda sem autorização de seus dados.

Além disso, ao se tornar indiscriminada e pouco fiscalizada, a coleta de dados compromete a capacidade do indivíduo de decidir sobre suas próprias informações, afetando sua autonomia e liberdade. Isso resulta em uma manipulação excessiva por terceiros e redução do livre desenvolvimento da personalidade do indivíduo.

Nesse contexto, o documentário *Terms and Conditions May Apply* (2013), analisa, de forma crítica, como os termos de uso e as políticas de privacidade, frequentemente obscuros e ignorados, ao invés de protegerem os indivíduos, muitas vezes fazem parte de um modelo de negócio que explora e usurpa a privacidade alheia.

A produção, ao ilustrar exemplos específicos de como o uso de indiscriminado de *cookies* e algoritmos por companhias pode prever aspectos íntimos da vida como rotina, saúde e hábitos de compra, rememora o notório escândalo da Target, onde o pai de uma jovem descobriu a gravidez de sua filha ao lhe serem direcionados pela varejista, anúncios relacionados à gestação, a partir da anterior reunião de informações sobre compras realizadas pela filha.

Essa realidade digital revela um cenário paradoxal, de lazer e de novos arranjos econômicos, trabalhistas e de interação social, mas concomitantemente, de aquisição e manipulação arbitrária de dados, as quais embasam o controle, por empresas públicas e privadas, sobre a criação de personalidades e de perfis comportamentais (GHISLENI, 2015).

Outrossim, o emblemático caso da Cambridge Analytica também demonstra como aplicativos e serviços digitais, aparentemente inofensivos, podem violar a privacidade dos usuários, cujos direitos, apesar de protegidos em textos legais, são constantemente infringidos pela captação e aplicação de dados pessoais.

No documentário Privacidade Hackeada (2019), o evento envolvendo a empresa de dados Cambridge Analytica é analisado como um exemplo de como a extração indevida de dados pessoais foi usada para manipulação eleitoral. Na produção, fica claro que a empresa inglesa teve acesso não consentido aos dados de milhões de eleitores estadunidenses, usuários do Facebook, para criação de perfis psicológicos e direcionamento de anúncios políticos personalizados, a favor da campanha do candidato à presidência Donald Trump, nas eleições de 2016.

O documentário expõe a forma como a Cambridge Analytica explorou falhas na privacidade digital para enviesamento político dos eleitores, destacando as consequências de um uso impróprio e irresponsável de dados pessoais em grande escala.

Assim, extrai-se de diversos casos concretos, que a prática da captação de dados “[...] identifica ilimitadamente o padrão de comportamento das pessoas e os antecipa, tornando-os previsíveis e modificáveis, eliminando o risco nos processos decisórios do setor político e mercadológico.” (MORELLATO; SANTOS, 2021, p. 4), anulando liberdade decisiva do titular de dados.

Nessa ótica, extrai-se dos estudos de Oliveira (2020), que técnica conhecida como *profiling* envolve o agrupamento de dados que definem características do usuário, o qual, graças aos algoritmos, permite a formação de um perfil detalhado de cada indivíduo. Por isso, para Bioni, ”[...] com base nesse mapeamento, identifica-se que há uma tensão entre os interesses econômicos e as esferas das pessoas que têm o livre desenvolvimento da sua personalidade afetado pela circulação dos seus dados.” (BIONI, 2019, p. 28).

Para Simão Filho e Schwartz (2016), o emblema reside no grande desafio para a legislação e os tribunais, que terão que buscar uma forma de equilibrar a proteção da privacidade para evitar a perda significativa de sua aplicação, ante os efeitos negativos gerados pelo sistema Big Data, especialmente no que diz respeito à violação da privacidade e da intimidade, bem como à tomada de decisões no contexto da cadeia de consumo.

Assim, embora as vantagens e facilidades do mundo digital sejam inegáveis, é essencial analisar de forma crítica como a disseminação e o uso de dados afetam de maneira significativa e invasiva a privacidade e a autodeterminação informativa,

bem como os custos que os cidadãos dispendem para aproveitar os benefícios da ubíqua digitalização.

3 MONETIZAÇÃO DE DADOS PELA VIGILÂNCIA DIGITAL E SEUS IMPACTOS NAS ESFERAS INDIVIDUAIS

A economia atual se sustenta na coleta e monitoramento contínuo de dados dos usuários, insumos fundamentais para segmentação de mercado. Esse processo implica em uma vigilância constante sobre o cotidiano das pessoas, com o armazenamento e análise de informações para fins econômicos, sociais e políticos. Como resultado, tem-se a gradativa anulação da autonomia dos indivíduos, pois suas escolhas e preferências são moldadas pelas ofertas que lhes são apresentadas.

Nesse panorama, a autora Soshana Zuboff (2019, p. 22) alcunhou a expressão “capitalismo de vigilância” para se referir ao modelo de negócio predominante na moderna sociedade digital, a qual se sustenta por um sistema de vigilância que se vale de toda experiência humana, reduzindo-a a dados pessoais. Esses dados são, então, capitalizados como matéria-prima para fins mercadológicos, com base em informações extraídas gratuitamente por meio dos rastros digitais deixados pelos usuários.

Em uma análise do elevado viés comercial atribuído aos dados, a doutrina aponta o que segue:

> [...] o ciclo de fiscalização, assim como o emprego dos dados captados, é constante e nesse processo, a mais-valia se dá quando a informação produzida pelos usuários é transformada em dados rentáveis, retornando ao usuário somente como mais serviços — que, inclusive, se aprimoram no sentido de coletar mais dados, constituindo um ciclo de despossessão. (FORNASIER; KNABEL, 2021, p. 11)

Diante disso, dados sensíveis ou não, são utilizados para segmentar anúncios, prever comportamentos e influenciar decisões, transformando aspectos da personalidade em um recurso comercial valioso.

Nesse raciocínio, para Bruno Bioni, o modelo padrão de promoção publicitária, foi mitigado, na medida em que essa passou a ser segmentada, pelo estudo da

predileção do sujeito alvo e por isso, com o progresso tecnológico, “[...] permitiu-se a criação de perfis cada vez mais intrusivos sobre o potencial consumidor, monitorando-se constantemente o seu comportamento, a ponto de inferir, até mesmo, o seu estado emocional para correlacioná-lo à mensagem publicitária.” (BIONI, 2019, p. 63).

Para ilustrar essa nova ordem econômica, pesquisadores da área chegaram à seguinte conclusão:

> [...] há a ascensão de uma nova mercadoria, que não é fruto necessariamente do trabalho industrial: a mercadoria dos dados, que tem como base as plataformas de redes sociais, nas quais os usuários entregam seus dados em troca de serviços anunciado como gratuitos, mas que são transformados em mercadoria pelas empresas responsáveis pela sua oferta no mercado. (FUCHS, 2009, p. 80-83 *apud* FORNASIER, KNABEL, 2021, p. 9)

Ao explorar essas informações, as empresas se beneficiam financeiramente, enquanto os indivíduos perdem o controle sobre sua própria esfera individual, em um reflexo de como a privacidade é deteriorada em nome do lucro.

Nessa mesma temática, para Fornasier e Knabel (2021), a assimetria informacional é o alicerce da economia de dados, onde a desigualdade entre os usuários e as empresas é fundamental para que os indivíduos cedam suas informações, não por escolha livre e consciente, mas pela falta de alternativas e pela ignorância do processo. Em decorrência disso, o mercado gerado pela vigilância oferece certezas sobre comportamentos, criando uma ilusão de previsibilidade e controle, moldada pelas necessidades comerciais.

A vigilância é contínua e se enraíza no cotidiano dos cidadãos por meio de um mercado que já se estruturou e depende da extração, monitoramento e monetização de dados, de forma que há, portanto, “um cabo de forças entre o livre trânsito e processamento dessas informações pessoais para alimentar toda uma economia deles dependente e, de outro lado, a necessidade de se impor limites para a tutela dos interesses extrapatrimoniais da pessoa.” (BIONI, 2019, p. 28).

Nessa lógica, a própria manutenção das práticas de monitoramento se dá pelo fato de que no modelo econômico atual, o consumidor não realiza pagamento direto pelos bens ou serviços que utiliza. Em vez disso, a contraprestação se dá pelo fornecimento de dados pessoais, que são utilizados para direcionar publicidade e viabilizar a oferta gratuita desses produtos. Essa forma de monetização, baseada na vigilância

constante do comportamento dos indivíduos, tornou-se o alicerce de uma nova economia, na qual as informações geram lucro exponencial (BIONI, 2019, p. 64).

Dessa forma, essa nova perspectiva de vigilância vai ao encontro da teoria do panoptismo, desenvolvida por Michel Foucault a partir do modelo arquitetônico de inspeção ideal projetado por Jeremy Bentham, onde uns vigiam sem ser percebidos. Hoje, a sua aplicação na sociedade da informação, se manifestas pelas grandes corporações, as quais por meio dos dispositivos tecnológicos, exercem suas atividades de monitoramento sem serem percebidas (GAZOLLA, 2020).

Nessa perspectiva, em um cenário não muito distante daquele esboçado pelos autores acima referidos, tem-se uma vigilância que:

> [...] praticamente se dá em todos os ambientes que o cidadão frequenta. Locais públicos e privados de qualquer natureza, possuem câmeras que registram movimentos e, em muitos casos, o som do ambiente. Redes sociais usam de meios tecnológicos para processar e transmitir na velocidade do pensamento, o conjunto de dados sequenciais, decorrentes da transformação tecnológica de sons, diálogos, fotografias, vídeos, possibilitando, através de seus geolocalizadores tecnológicos, determinar com margem de segurança e precisão, os locais de onde são provenientes as transmissões e, por via de consequência, detectar onde se encontra a pessoa, numa aparente ou clara invasão de privacidade. (SIMÃO FILHO; SCHWARTZ, 2016, p. 13)

Nesse sentido, em que pesem as benesses concedidas pelo mundo cibernético, há que se questionar o preço pago pela vigilância atual, bem como se a legislador tem procurado mecanismos jurídicos para efetivamente proteger o direito à privacidade, pois o que se percebe é o potencial lucrativo do tratamento de dados e a transformação do sujeito, o qual abre mão da sua privacidade em nome da mínima conectividade social, em um produto (GHISLENI 2015).

Percebe-se, portanto, não apenas a monetização de dados, mas sim a mercantilização de comportamentos, pautada na vigilância rotineira e perene, pela qual os sujeitos são constantemente monitorados para atender às demandas mercadológicas.

CONCLUSÃO

O presente artigo científico teve como premissa a análise do direito à privacidade e à autodeterminação informativa no contexto das complexas questões envolvendo a coleta de dados na atual economia digital.

Com base na pesquisa realizada, conclui-se que a privacidade, enquanto conceito, atravessa diferentes contextos históricos e muda ao longo do tempo e do espaço, especialmente devido aos avanços tecnológicos. Assim, seu significado não é estável, tampouco abrange todas as suas possibilidades e desdobramentos. Diante disso, surge um grande desafio: a preservação desse direito fundamental, o qual, embora essencial, ainda carece de definições precisas e de diretrizes claras sobre suas violações e formas de proteção.

Em uma perspectiva nacional, analisou-se como a privacidade foi prevista na LGPD, a qual se revelou como um marco jurídico na proteção de dados pessoais ao reconhecer o titular de dados pessoais como sujeito de direitos, garantindo-lhe maior autonomia e controle sobre as informações pessoais.

Apesar da aparente proteção conferida aos usuários, a realidade revela uma série de limitações práticas que dificultam a plena aplicação da autodeterminação informativa e do livre desenvolvimento das personalidades.

Nesse contexto, a regulamentação jurídica brasileira reconhece o problema do extrativismo de dados e a vulnerabilidade dos seus titulares. Contudo, ao mesmo tempo, fornece condições e segurança jurídica às empresas para que a entrega de dados ocorra. Dessa forma, a assimetria de poder entre o titular e as empresas detentoras das informações se revela como uma entrave para eficácia das disposições sobre consentimento, transparência, segurança e adequação presentes da LGPD, essenciais para proteção da privacidade e do livre desenvolvimento da personalidade da pessoa natural.

Constatou-se, ainda, que a coleta de dados, embora essencial para o funcionamento de diversos serviços digitais, afeta negativamente a vida privada do sujeito de direitos. Discutiu-se acerca das técnicas de coleta de dados e sobre a aplicação e limites do consentimento, evidenciando que apesar de a LGPD aclamar o

protagonismo da manifestação de vontade do titular em dispor de sua informação, as condições materiais e a assimetria de poder entre consumidores e empresas, frequentemente comprometem sua liberdade de escolha.

Ademais, foi possível observar a forma como as coletas de dados, mediante as suas mais variadas técnicas, adentram no cotidiano das pessoas e usurpam gradativamente o direito à privacidade. Essa realidade, corrobora o entendimento de que a autodeterminação informativa se encontra cada vez mais ameaçada, na medida em que os indivíduos perdem o mínimo controle sobre o fluxo da circulação de informações pessoais.

Por fim, foi investigada a monetização de dados por meio da vigilância digital, destacando-se os seus impactos nas esferas individuais. A captação de informações pessoais, prática fundamental na vigilância cibernética, se apresenta como um fenômeno atrelado à elevada lucratividade associada ao dado, os quais são empregados cada vez mais para fins monetários, sem que o indivíduo tenha efetivo controle ou real compreensão sobre as consequências dessa exploração.

Nesse viés, verificou-se a aplicação do monitoramento e monetização do dado no mercado, pela previsão de padrões de comportamento, para posterior direcionamento de conteúdos e mercadorias premeditadas, a fim de se fomentar a estabilidade da lógica de mercado.

Nesse cenário, a autonomia do sujeito passa a se revelar altamente ameaçada, já que esse não possui pleno direito decisório, quando se diz respeito à cessão de seus dados, em uma nítida anulação de sua liberdade de escolha e disposição da informação que é a ele inerente.

Ante todo o exposto, a exploração de dados pessoais, mormente para práticas mercadológicas, frequentemente sem a devida transparência ou controle por parte dos indivíduos, desafia os princípios de privacidade e da autodeterminação.

Portanto, a convergência entre o avanço da economia digital e a garantia dos direitos à privacidade e à autodeterminação informativa exige um equilíbrio efetivo entre a proteção do indivíduo e o uso responsável de seus dados pessoais, por meio da ponderação entre a salvaguarda da pessoa natural e o tratamento adequado de suas informações, sobretudo as sensíveis, de modo a assegurar, na prática, o pleno exercício da autodeterminação informativa.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 29 de maio de 2025.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Institui o Código Civil**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 29 de maio de 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 de maio de 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 29 de maio de 2025.

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

BRANCO, Paulo Gustavo Gonet; MENDES, Gilmar Ferreira. **Curso de Direito Constitucional**. 16. ed. São Paulo: Saraiva, 2021.

CAMURÇA, Lia Carolina Vasconcelos; MATIAS, João Luís Nogueira. **Direito à privacidade e à proteção de dados pessoais: análise das práticas obscuras de direcionamento de publicidade consoante a Lei.º 13.709, de 14 de agosto de 2018**. Revista Direitos Fundamentais e Democracia, Curitiba, v. 26, n. 2, p. 6-23, mai./ago. 2021.

COLOMBO, Cristiano; NETO, Eugênio Facchini. **Mineração de dados e análise preditiva: reflexões sobre possíveis violações ao direito de privacidade na sociedade da informação e critérios para sua adequada implementação à luz do ordenamento Brasileiro**. Revista de Direito, Governança e Novas Tecnologias, Maranhão, v. 3, n. 2, p. 59 – 80, Jul/Dez. 2017.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

FONSECA, Gabriel C. Soares da; MENDES, Laura Schertel. **Proteção de dados para além do consentimento: tendências contemporâneas de materialização**. Revista Estudos Institucionais, v. 6, n. 2, p. 507-533, mai./ago. 2020.

FORNASIER, Mateus de Oliveira; KNEBEL, Milton Paiva. **O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na**

Lei Geral de Proteção de Dados. Revista Direito e Práxis, Rio de Janeiro, v. 12, n. 2, p. 1002-1033, 2021. DOI: 10.1590/2179-8966/2020/46944. ISSN 2179-8966.

GAZOLLA, Frederico Jacinto Cardoso. **Direito à privacidade na sociedade da informação e o pós-panoptismo**. 2020. 246 f. Dissertação (Mestrado em Direito) - Universidade Católica de Petrópolis.

GHISLENI, Eduardo Steffenello. **Vigilância na sociedade em rede: a coleta de dados pessoais na internet e suas implicações ao direito à privacidade**. 2015. 60 f. Monografia (Monografia de Graduação) – Centro de Ciências Sociais e Humanas Curso de Direito, Universidade Federal de Santa Maria.

GORDON, Jehane. **Privacidade Hackeada (título original: The Great Hack)**. 2019. Documentário. EUA: Netflix.

Guia orientativo cookies e proteção de dados pessoais. Autoridade Nacional de Proteção de Dados ANPD. Versão 1.0. Brasília, DF, out/2022. 40 p.

HUGHES, Cullen. **Terms and Conditions May Apply**. 2013. Documentário. EUA: A Skeeter and the Machine.

JORGETTO, Leonardo Felipe de Melo Ribeiro Gomes; MARTINS, Marcelo Guerra; SUTTI, Alessandra Cristina Arantes. **Big data e a proteção do direito à privacidade no contexto da sociedade da informação**. Revista Jurídica Cesumar, v. 19, n. 3, p. 705-725, set./dez. 2019. e-ISSN 2176-9184.

MORAES, Alexandre de. **Direito Constitucional**. 36. ed. São Paulo: Atlas, 2020.

MORELLATO, Ana Carolina Batista; SANTOS, André Filipe Pereira Reid dos. **Capitalismo de vigilância e a Lei Geral de Proteção de Dados: perspectivas sobre consentimento, legítimo interesse e anonimização**. Revista Brasileira de Sociologia do Direito, v. 8, n. 2, p. 184-207, maio/ago. 2021

OLIVEIRA, Bruna Pinotti Garcia. **Inteligência artificial e proteção de dados: sobre a autodeterminação informativa e a manipulação informacional por machine learning**. Humanidades & Tecnologia (FINOM), v. 26, jul./set. 2020.

SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. **"Big data" – big problema! Paradoxo entre o direito à privacidade e o crescimento sustentável**. Copendi Law Review, Florianópolis, v. 2, n. 3, p. 311-331, jan./jul. 2016.

ZUBOFF, Shoshana. **A era do capitalismo da vigilância**: A luta por um futuro humano na nova fronteira de poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 22-27.