

UNIVERSIDADE FEDERAL DE ALAGOAS - UFAL
FACULDADE DE DIREITO DE ALAGOAS - FDA
GRADUAÇÃO EM DIREITO

ALMINIAS DA SILVA LIMA

**PROTEÇÃO DE DADOS E CONSENTIMENTO: LIMITAÇÕES E DESAFIOS PARA
O DIREITO BRASILEIRO**

Maceió/AL

2023

ALMINIAS DA SILVA LIMA

**PROTEÇÃO DE DADOS E CONSENTIMENTO: LIMITAÇÕES E DESAFIOS PARA
O DIREITO BRASILEIRO**

Monografia de conclusão de curso apresentada à Faculdade de Direito de Alagoas (FDA/UFAL) como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientadora: Prof^ª. Dr^ª. Juliana de Oliveira Jota Dantas.



Prof.ª Dr.ª Juliana de Oliveira Jota Dantas
FDA/UFAL
MACEIÓ/AL

Maceió/AL

2023

Catálogo na Fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico

Bibliotecário: Marcelino de Carvalho Freitas Neto – CRB-4 – 1767

L732p

Lima, Alminias da Silva.

Proteção de dados e consentimento : limitações e desafios para o direito brasileiro / Alminias da Silva Lima. – 2023.

57 f. : il.

Orientadora: Juliana de Oliveira Jota Dantas.

Monografia (Trabalho de Conclusão de Curso em Direito) – Universidade Federal de Alagoas. Faculdade de Direito de Alagoas. Maceió, 2023.

Bibliografia: f. 51-57.

1. Proteção de dados pessoais. 2. Consentimento. 3. Direito à autodeterminação informativa. I. Título.

CDU: 343.451

AGRADECIMENTOS

À minha mãe, Vania Campos, pelo sacrifício de uma vida e por todo o amor que nunca poderei retribuir à altura.

À minha família, por todo o incentivo e confiança depositados em mim, especialmente aos meus tios Paulo e Neiaria.

Aos amigos que a Faculdade de Direito de Alagoas me presenteou, Nina, Amanda R., Renata, Amanda F., Inayara, Brenda e Felipe, pela amizade e pelo apoio em todos os momentos ao longo da graduação.

Aos irmãos que a vida me deu, Eduardo, Felipe, Macio, Jay, Victor e Madison, pela presença diária e por todas as memórias que ainda vamos construir.

Às queridas amigas Marcelita, Gabriela e Marília, por tornarem os primeiros passos da vida profissional tão mais agradáveis.

À minha orientadora, Prof^ª Dra. Juliana de Oliveira Jota Dantas, pela confiança e paciência durante a construção desse projeto.

A todos os professores e servidores da Universidade Federal de Alagoas que me acompanharam nessa caminhada e permitiram que eu chegasse até aqui.

A todos que de alguma forma contribuíram para o desenvolvimento desse trabalho e torceram pela realização desse sonho.

“If I want to, I’ll arrive at peace
I know I decide what I remember
If this ever mended me
All the on and on just shakes my sleep all night”
Robin Pecknold

RESUMO

O presente trabalho teve como objetivo analisar a perspectiva do consentimento do titular de dados como marco regulatório da proteção de dados pessoais. Para tanto, foram abordadas questões que envolvem o paradigma do consentimento, tratando do surgimento da sociedade de informação e vigilância, dos riscos e danos a que se submetem os indivíduos diante do uso indevido de suas informações e do papel da autodeterminação informativa para a tomada de decisão informada por parte dos cidadãos. Contextualizados os obstáculos para a tutela da proteção de dados, foram apontados caminhos para a materialização desse novo direito da personalidade através da capacitação e empoderamento do titular de dados, da instrumentalização da tecnologia e da expansão normativa. Desse modo, foi verificada a necessidade de limitar a participação do indivíduo para que o consentimento opere de forma satisfatória, com intervenções na economia da informação que permitam atribuir maior autonomia à parte (hiper)vulnerável da relação informacional, atenuando a assimetria entre os agentes.

Palavras-chave: Proteção de dados. Consentimento. Autodeterminação informativa.

ABSTRACT

The present study aimed to analyze the perspective of data subject consent as a regulatory framework for personal data protection. To achieve this, issues surrounding the consent paradigm were addressed, discussing the emergence of the information and surveillance society, the risks and harms that individuals are exposed to due to the improper use of their personal data, and the role of informational self-determination in informed decision-making by citizens. After contextualizing the obstacles data protection faces, pathways for realizing this novel personality right were identified through the empowerment and capacitation of data subjects, the utilization of technology, and the expansion of regulations. Thus, the need to limit individual participation was recognized in order for consent to operate effectively, with interventions in the information economy that allow for greater autonomy to be granted to the (hyper)vulnerable party in the informational relationship, thereby mitigating the asymmetry between the parties.

Keywords: Data Protection. Consent. Informational self-determination.

SUMÁRIO

1. INTRODUÇÃO	8
2. O DESENVOLVIMENTO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS..	11
2.1 Dados Pessoais e a sociedade da informação e vigilância.....	11
2.2 Direito a proteção de dados: desenvolvimento e aspectos relevantes	18
3. AVALIAÇÃO SUBSTANTIVA E PROCEDIMENTAL DO CONSENTIMENTO ENQUANTO PROTAGONISTA DA PROTEÇÃO DE DADOS PESSOAIS	24
3.1 Identificação da (hiper)vulnerabilidade do titular de dados e a assimetria no paradigma do fluxo informacional	24
3.2 Estratégias regulatórias do consentimento	28
3.3 Posição e adjetivação do consentimento no quadro normativo brasileiro.....	32
4. PARÂMETROS PARA A PARIDADE DE PODERES NAS RELAÇÕES INFORMACIONAIS E CAMINHOS PARA A CAPACITAÇÃO DO TITULAR DE DADOS (HIPER)VULNERÁVEL	36
4.1 Pontos de interesse na capacitação e empoderamento do titular de dados	36
3.2 Instrumentalização da tecnologia e reavaliação da engenharia das redes e sistemas	41
3.3 Diretrizes para a expansão normativa da proteção de dados	45
5. CONCLUSÃO.....	49
REFERÊNCIAS.....	51

1. INTRODUÇÃO

O desenvolvimento tecnológico nas últimas décadas, marcado pelo amplo acesso das massas à internet, aos dispositivos digitais e suas camadas de aplicação trouxe consigo, de forma gradual, acentuada dependência do coletivo a novos hábitos, práticas e facilidades, permitindo que a tecnologia se posicionasse de maneira a figurar uma extensão do indivíduo.

Na medida em que se implementaram de forma conveniente no cotidiano essas novidades tecnológicas, já não se pode deixar de reconhecer que cada indivíduo produz, projeta e traz para si implicações diretas a respeito de seus dados, uma espécie de “pegada digital”, em que a personalidade passa a ser simulada enquanto representação do titular.

Essa inovação na forma de organização social não poderia deixar de trazer reflexos, também, na forma como se regula o mercado e a economia. A ciência do mercado no capitalismo, de forma natural ao seu funcionamento, identifica os dados dos consumidores como uma ferramenta apta a trazer frutos no plano de consumo, abrindo espaço para uma realidade em que a extração e manipulação de dados, já viabilizada com a tecnologia presente, passa a ser prática útil e desejável.

Como efeito, adentram ao cotidiano novos desdobramentos a partir da anuência - não precisamente funcional - dos usuários, captada através de instrumentos contratuais que se apresentam de forma predisposta, agindo meramente como breve distração ou empecilho antes que possa adquirir ou utilizar algum bem ou serviço. Ao usuário, resta concordar ou discordar com uma política de privacidade ou termo de uso.

O consentimento do titular de dados nessas hipóteses, bem como sua discussão e suas implicações, se posicionou como fator central da problemática ao longo do desenvolvimento da matéria. Se coloca dessa maneira, sobretudo, pelo caráter recorrente em que o titular se encontra diante desse paradigma, diariamente reproduzindo de forma massiva seus dados através de relações ordinárias de consumo.

À medida que a captação de dados se mostra incessante e inescapável, podendo ocorrer na prática até mesmo durante o uso de ferramentas assistenciais criadas pelo Estado em um de seus domínios governamentais, se destacam os efeitos produzidos pelo tratamento de dados ineficiente e invasivo e pelos casos de vazamento. Adentram no plano fático consequências diretas, como a venda de informações pessoais, a publicidade direcionada e discriminação

algorítmica, e o aumento exponencial no número de crimes virtuais realizados por agentes que já identificam o terreno fértil das redes sociais para consumir práticas delitivas.

O Direito, por sua vez, mostra dificuldade em acompanhar a realidade social, tendo que trilhar território inexplorado de modo a regular as relações jurídicas firmadas de forma virtual, sem barreiras ou fronteiras físicas impedindo usuários de viver realidades que possivelmente nunca teriam incidência antes do advento da rede mundial de computadores.

A análise da organização social sob o prisma da informação, consumo e vigilância é capaz de transformar informações aparentemente insignificantes em perfis do indivíduo, impossibilitando a ausência de reverberações nos direitos sociais, à vista que a proteção de dados avança ao ponto de ser reconhecido no campo doutrinário e jurisprudencial como um direito fundamental autônomo, e, finalmente, em sua positivação no texto constitucional.

É o movimento natural da ciência jurídica, considerando este como um dos grandes avanços feitos desde o processo legislativo que culminou na Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709, de 14 de agosto de 2018), atual produção normativa basilar da discussão da proteção de dados no Brasil, além das inovações trazidas pela discussão nos tribunais que abriram o caminho para a EC 115/22.

Diante desse contexto, surge o problema de como viabilizar a efetividade do consentimento diante de um cenário de hipervulnerabilidade dos titulares de dados, que sobrepõe, por sua vez, mais empecilhos à tutela do direito à proteção de dados.

Afinal, ainda que a LGPD se mostrasse suficiente para contemplar todos os problemas e hipóteses apresentáveis e fosse devidamente respeitada pelos agentes de tratamento de dados, ainda há de se superar a maneira como o indivíduo compreende a forma como se dá o tratamento de seus dados, não sendo suficiente uma transparência formal em que não haja uma apresentação clara, precisa e de fácil acesso a todos.

A motivação deste trabalho parte do reconhecimento da urgência de vislumbrar os empecilhos para a concretização da proteção de dados, partindo de um exame da prática do consentimento e entendendo os problemas que atingem tanto o cidadão mais preparado para enfrentar a nova realidade, quanto aqueles atingidos pelo status de hipervulnerabilidade, como crianças, idosos e pessoas sem conhecimento técnico mínimo para manusear as novas tecnologias.

Assim, o objetivo do texto é estudar a impossibilidade atual de alcançar um consentimento livre, inequívoco, informado e específico de fato no tratamento dos dados

personais, considerando os riscos envolvidos no mau uso das informações pessoais pelos agentes do mercado informacional.

Sob essa perspectiva, a pesquisa propõe a análise do tema em três momentos. Para sua consecução, foi utilizado o método de abordagem hipotético-dedutivo diante das categorias jurídicas abstratas do objeto, sendo levantada bibliografia concernente à proteção de dados, o consentimento e a hipervulnerabilidade no ordenamento pátrio, mediante ensinamentos doutrinários, artigos publicados em periódicos e revistas jurídicas, produções normativas atribuídas na extensão do diálogo das fontes e os precedentes jurisprudenciais que auxiliam a ampliar o entendimento a respeito do tema.

Desse modo, no primeiro capítulo, é introduzido um breve panorama histórico a respeito do desenvolvimento da sociedade informacional e do caminho percorrido até que a proteção de dados fosse reconhecida juridicamente como um direito, contextualizando o quadro em que se dispõe o paradigma do consentimento na discussão da matéria.

Logo após, no segundo capítulo, parte-se à observação do quadro regulatório firmado pelo ideal de autodeterminação informacional centrado no consentimento, analisando as falhas para sua concretização e apontando a forma como o ordenamento jurídico atualmente aborda essa acepção.

Por fim, no terceiro capítulo, faz-se uma análise dos caminhos que podem ser tomados a fim de materializar o direito à proteção de dados, indo além do papel individual do titular de dados pessoais e ponderando novas perspectivas tecnológicas, normativas e culturais que sejam capazes de instrumentalizar uma autonomia material dos indivíduos, atendendo às limitações impostas pelo atual modelo regulatório do consentimento na autodeterminação informativa.

2. O DESENVOLVIMENTO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

2.1 Dados Pessoais e a sociedade da informação e vigilância

Os dados pessoais, conceituados como informação em estado bruto e potencial que pode ser atrelada a uma pessoa através da extração de seu conteúdo em um processo cognitivo¹, após a virada do século, figuram como um dos objetos centralizados na discussão normativa e na produção jurídica em todo o planeta.

Cumprir analisar de que maneira e em que momento a informação assumiu esse papel de protagonismo, a ponto de revolucionar integralmente a estrutura das relações sociais e a forma como essas se apresentavam nas mais diversas camadas da sociedade.

A transformação da estrutura social, ao longo da história da humanidade, foi o motor que impulsionou a mudança gradual da forma como o ser humano vive em suas comunidades. O marco temporal de cada grande ruptura já presenciada pela história pode ser associado a peças-chave e momentos decisivos, e historiadores e cientistas apontam esses momentos de colisão e ruptura desde a revolução agrícola, momento em que surgem as primeiras civilizações organizadas em torno do processo de cultivo da terra e do escambo dos frutos dessa nova prática².

O processo de ampliação ao redor do mundo desse primeiro grande momento transformativo ainda perdurava quando, no século XVIII, a revolução industrial captou na estrutura das máquinas a vapor o vórtice para expandir a produção econômica da época além das fontes de riqueza provindas da terra, conseguindo se ampliar ao redor do mundo em três séculos. A partir desse momento, novos conceitos como o de consumidor passam a figurar como elementos estruturantes da organização econômica³.

Após a Segunda Guerra Mundial surge o terceiro momento de ruptura, impulsionado desta vez pelos serviços na sociedade pós-industrial. Dessa vez, em questão de décadas⁴, a economia não mais se limitava ao que era produzido pela indústria e pela agricultura, mas pela oferta dos setores de serviços profissionais emergentes como os bancos, seguradoras, educação, mídia e consultoria jurídica⁵.

¹ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

² TOFFLER, Alvin. **The third wave**. Bantam Books, 1986, p. 21.

³ *Idem, ibidem*, p. 53.

⁴ *Idem, ibidem*, p. 12.

⁵ MURRAY, Andrew. **Information, technology, law**. OUP Oxford, 2019, pp. 40-41.

Nesse período do século XX também se percebem os primeiros passos da revolução tecnológica que, com seus rápidos avanços, viabilizou acelerada transformação dos paradigmas sociais. Esses processos, que em sua gênese duraram milhares de anos para se espalhar pelo globo, agora encontram dificuldade em não serem reproduzidos de forma massificada nas mais variadas organizações sociais em poucos anos.

Com a disposição das novas tecnologias, não mais existem as barreiras temporais e físicas que impediam um rápido processo antropofágico. À medida que a informação e o conhecimento passam a ser ativos valorizado pela economia, as ferramentas para seu processamento, transmissão, difusão e consumo em grandes quantidades e alta velocidade foram construídas de maneira concomitante, caracterizando uma progressão natural resultante no fluxo informacional livre, sem a clássica limitação de tempo e espaço aplicada até então.

Esse mais recente momento da história social vem sendo identificado pelos estudiosos da teoria das civilizações como a “sociedade da informação”. A busca pela conceitualização partindo da ideia de que a informação é a força capaz de transformar e desenvolver essa nova forma de sociedade⁶. Nesse sentido, sua utilização como recurso econômico passa a ser elemento estruturante para reorganização social, numa aplicação semelhante àquela vista pela agricultura, pela indústria e pelos serviços nos modelos de organização social que a precederam.

As transformações verificadas em escala mundial após o advento de inovações tecnológicas como o primeiro computador apontam para modificações nas relações sociais, na cultura e na economia, criando um novo modo de desenvolvimento reestruturante nunca antes testemunhado na evolução histórica do capitalismo.

Identificado por Manuel Castells como informacionalismo, considera-se um processo organizado em escala global e munido de uma rede interativa, capaz de criar um sistema econômico distinto.

Nesse sentido expõe o autor:

Informação e conhecimento sempre foram elementos cruciais no crescimento da economia, e a evolução da tecnologia determinou em grande parte a capacidade produtiva da sociedade e os padrões de vida, bem como formas sociais de organização econômica. Porém, estamos testemunhando um ponto de descontinuidade histórica. A emergência de um novo paradigma tecnológico

⁶ KARVALICS, László. **Information Society – what is it exactly?** (The meaning, history and conceptual framework of an expression). Budapeste, 2007, p. 11. Disponível em: <https://www.researchgate.net/publication/237332035_Information_Society_-_what_is_it_exactly_The_meaning_history_and_conceptual_framework_of_an_expression>. Acesso em: 15 Jul. 2023.

organizado em torno de novas tecnologias da informação, mais flexíveis e poderosas, possibilita que a própria informação se torne o produto do processo produtivo⁷.

Conforme anotado, os produtos das indústrias emergentes são dispositivos de processamento de informação ou o próprio processamento desta, e estabelecem ligações infundáveis entre diversas áreas, elementos e agentes. É um modelo econômico extremamente independente, capaz de reinvestir qualquer novo avanço que produza no próprio processo de conhecimento, ciclo extremamente produtivo e eficiente que possibilita a transformação na organização social em abreviados lapsos temporais.

Ao passo que a informação antes armazenada em folhas de papel através da escrita começa a ser reproduzida de forma digital através do sistema binário de *bits*, se deu o acúmulo rápido e exponencial de dados aglomerados, utilizando de novos recipientes ao longo do tempo, como os *hardwares* que a cada década suportam uma maior quantidade de informação gravada: basta lembrar a capacidade de armazenamento dos CDs e disquetes no início do século XXI e compará-la com a memória disponível nos aparelhos eletrônicos agora disponíveis no mercado.

O sistema binário adotado permite, além do aspecto quantitativo massivo de armazenamento de dados, maior facilidade no acesso às informações, contando com novas estruturas de organização, sendo possível a consulta descomplicada da informação a qualquer momento e em qualquer lugar⁸.

Nesse momento histórico, surge outro conceito relevante para a dinâmica da proteção de dados. Como anotam Ehrhardt Júnior e Peixoto⁹, os sistemas de armazenamento de dados computadorizados desenvolveram técnicas que permitiam vincular determinadas informações àqueles que a produziram ou terceiros, gerando o que se entende como *Personally Identifiable Information (PII)*, conceito central no estudo da privacidade informacional que se distingue da concepção de informação pessoal ou dado pessoal ao englobar também as informações que podem vir a ser identificadas e associadas a alguém.

Uma vez instaurado o fluxo informacional que atua como recurso determinante da economia, as empresas organizadas e posicionadas no sistema de rede global, amparadas pelos

⁷ CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 2008, p. 119.

⁸ BROOKSHEAR, Glenn. **Ciência da Computação: Uma Visão Abrangente**. 11. ed. São Paulo: Bookman, 2013, p. 23.

⁹ EHRHARDT JÚNIOR, Marcos; PEIXOTO, Erick Lucena Campos. Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias. **Revista Jurídica Luso-brasileira – RJLB**, Lisboa, a. 6, n. 2, 2020. Disponível em: <https://www.cidp.pt/revistas/rjlb/2020/2/2020_02_0389_0418.pdf>. Acesso em: 25 Jul. 2023.

avanços tecnológicos e de comunicação, estão prontas para influenciar a economia de novas maneiras.

Os dados pessoais dos cidadãos passaram a ser um ativo na economia de informação e a influenciar diretamente o mercado, que rapidamente analisou a dinâmica emergente e identificou que estes deveriam se tornar elemento basilar de suas estratégias de marketing e publicidade.

Ao ser tratada, a informação bruta passa a gerar novos conhecimentos, que, por consequência, serão utilizados na economia visando aprimorar serviços, criar novos modelos de negócio, otimizar processos e a atividade daqueles que os regulam, personalizar ofertas, e trazer vantagens competitivas aos agentes com sua posse. Não se restringindo a tanto, podendo, dentre outra infinidade de hipóteses, influenciar políticas públicas e as decisões que os cidadãos fazem em suas vidas particulares, como no processo de escolha de candidatos durante o período eleitoral.

Os bens de consumo passam a ser modificados pela indústria e reintroduzidos para o público de acordo com a reação dos consumidores, através da informação gerada pelo público-alvo. Os empreendimentos passam a ser mais eficazes conforme os hábitos de consumo viram objeto de análise pela indústria, diminuindo a chance de retornos desfavoráveis¹⁰.

É um processo crítico para a atividade empresarial, considerando que não só aperfeiçoa os produtos e serviços de acordo com os pontos positivos e negativos indicados por quem consome, como também altera a estratégia de publicidade utilizada para que prosperem e gerem o maior lucro possível.

O consumidor deixa de ser um agente passivo na engrenagem do capitalismo, e sua contribuição não mais se limita ao ato de consumir. O agente final na cadeia de consumo passou a atuar também no processo de produção dos bens e em sua divulgação, agindo naturalmente no cotidiano como um vendedor de forma voluntária.

O consumo passa a ser extremamente influenciado pelas opiniões dos usuários, e o marketing boca a boca se torna fator capaz de determinar se determinado bem ou serviço será

¹⁰ EVANS, David. The Online Advertising Industry: Economics, Evolution, and Privacy. **Journal of Economic Perspectives**, v. 23, n. 3, p. 22, 2009. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1376607>. Acesso em: 2 Ago. 2023.

um grande sucesso ou um prejuízo catastrófico aos seus idealizadores em indústrias como a cinematográfica¹¹.

A publicidade, cuja estratégia dominante por muito tempo objetivou atingir o maior número de pessoas em suas ações para que, então, pudesse alcançar o público-alvo após o afunilamento dos interlocutores, agora não mais tolera alocar esforços que atingem expressiva parcela de um público que jamais consumiria aquilo que está sendo promovido.

Nesse sentido, expõe o economista David Evans¹²:

Esses dados detalhados de navegação são valiosos para os provedores da indústria de publicidade online. Eles permitem que esses provedores ofereçam perspectivas de maior qualidade aos anunciantes e, portanto, cobrem um valor mais alto pelo inventário de publicidade que fornecem. Eles também possivelmente oferecem anúncios mais valiosos aos usuários, que por sua vez terão maior probabilidade de visitar sites que apresentam anúncios mais adequados às necessidades do usuário. Considerando que um site irá exibir um anúncio, os consumidores podem preferir que o anúncio seja mais relevante do que não¹³.

Através dessa estratégia, a abordagem padronizada e ineficiente dá espaço a propaganda direcionada, que veicula a comunicação para um público específico. Através de análise prévia da ciência mercadológica, com base nos dados de navegação dos consumidores, aqueles a quem não interessa a mensagem publicitária são excluídos da narrativa, personalizando a abordagem e atingindo diretamente a parte do público mais inclinada a adquirir aquilo que está sendo ofertado. É um processo duplamente benéfico, que corta custos ao mesmo tempo em que otimiza o alcance ao sujeito final da cadeia.

Naturalmente, surge um novo mercado especializado em extrair e manipular esses dados, utilizados como um *commodity*, e que atrai o questionamento a respeito da proteção dos dados pessoais e a forma como esta é feita.

¹¹ LIU, Yong. Word of Mouth for Movies: Its Dynamics and Impact on Box Office Revenue. **Journal of Marketing**, v. 70, n. 3, 2006, p. 27. Disponível em: <<https://journals.sagepub.com/doi/10.1509/jmkg.70.3.074>>. Acesso em: 2 Jul. 2023.

¹² EVANS, David. The Online Advertising Industry: Economics, Evolution, and Privacy. **Journal of Economic Perspectives**, v. 23, n. 3, 2009, p. 30. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1376607>. Acesso em: 2 ago. 2023.

¹³ Tradução livre de “These detailed data on browsing are valuable to online advertising industry providers. They enable these providers to provide higher quality prospects to advertisers and to therefore charge more for the advertising inventory they supply. They also possibly provide more valuable advertisements to users who in turn will be more likely to visit web sites that present advertisements that are more tailored to the needs of the user. Given that a web site is going to display an advertisement consumers might prefer that the advertisement be more relevant than not”.

Invenções tecnológicas como os *cookies*¹⁴ viabilizam essa espécie de utilização dos dados pessoais, captando os interesses do público e criando um perfil do potencial consumidor. A navegação cotidiana permite que agentes externos passem a conhecer interesses, e dentre esses, o que cada pessoa pode vir a efetivamente consumir, partindo desse retrato comportamental construído de forma digital e autônoma.

Importa destacar a escala em que o corpo social está inserido nessa realidade e passível de testemunhar os efeitos do tratamento dos dados que venha a produzir. À proporção que internet se tornou essencial para a participação em sociedade, sociólogos já compreendem, por exemplo, que a interação humana nas redes sociais se estende além dos ideais clássicos de comunidade¹⁵. A adesão, por sua vez, se mostra massiva: com o barateamento dos recursos tecnológicos, 90% dos domicílios brasileiros já possuíam acesso à internet em 2021¹⁶.

O ambiente virtual, devidamente ocupado pela sociedade civil, se encontra saturado de comércio, com crescimento exponencial ano após ano, e essa economia tem como cerne a vigilância. Os comportamentos dos indivíduos, observados e analisados de forma permanente, geram as informações pessoais que serão a matéria prima a ser explorada no processo de geração de riqueza, utilizando técnicas para captação de ricos perfis pessoais e catalogando o comportamento dos usuários.

A liberdade do indivíduo de escolher se deseja ou não se envolver nesse sistema e dispor de seus dados já pode ser considerado um ideal distante e utópico. Na sociedade em que os dados pessoais são requisitados de forma incessante, o ato consciente de não os fornecer vem

¹⁴ “*Cookies*” são uma das ferramentas utilizadas pelos websites para rastreamento e identificação dos usuários, sendo pequenos arquivos de texto que normalmente contém uma linha de números que podem ser utilizados para identificar um computador. Por exemplo, um website pode instalar um cookie de rastreamento no computador de um usuário utilizando uma chave (nomenclatura dada a esses dispositivos) composta por uma “id” e um número único (utilizado para diferenciar cada usuário), como “123456789”. Publicitários podem então acessar o cookie “id” e rastrear a forma como o usuário 123456789 visita diferentes websites e trafega na internet. O problema envolvendo privacidade e proteção de dados na dinâmica dos *cookies* decorre da agregação desse rastreamento em diferentes websites para criar perfis e das tentativas de vincular esse perfil à identidade do usuário. Ao rastrear esses identificadores em sites visitados pelos usuários, os anunciantes podem inferir os interesses dos usuários, talvez até interesses sensíveis, como condições médicas, opiniões políticas ou até mesmo fetiches sexuais (Tradução livre). HOOFNAGLE, Chris Jay et. al. Behavioral Advertising: The Offer You Cannot Refuse. **Harvard Law & Policy Review**, v. 6, 2012, p. 276. Disponível em: <<https://ssrn.com/abstract=2137601>>. Acesso em: 08 Jul. 2023.

¹⁵ COSTA, Rogério. **Por um novo conceito de comunidade**: redes sociais, comunidades pessoais, inteligência coletiva. Interface - Comunic., Saúde, Educ., v.9, n.17, 2005, p. 239.

¹⁶ IBGE Notícias. **Internet já é acessível em 90% dos domicílios do país em 2021**. Disponível em: <<https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021>>. Acesso em: 10 Jul. 2023.

com um custo a ser pago, que vai de uma simples abdicação do acesso a uma opção lúdica de lazer, até a impossibilidade de prestação de serviços públicos ofertados pelo Estado.

Mendes¹⁷ evidencia que que esses custos sociais enfrentados pelos indivíduos são expressivos e notáveis, visto que esses produtos e serviços já foram completamente integrados no cotidiano da sociedade, e se aprofundaram na vida social e dentro das dinâmicas político-econômicas que os indivíduos exercem com sua comunidade, com a indústria e com o Estado.

Cabe atentar, ademais, que mesmo em casos alinhados à hipótese de tratamento de dados feita pelo Estado e por seus agentes, a garantia de segurança dos dados e proteção do cidadão pode não ser presumida, apesar da responsabilidade institucional desses atores de atender os interesses da população em diversos âmbitos e esferas¹⁸.

Zuboff¹⁹ comenta que se trata de uma escolha fundamentalmente ilegítima. O capitalismo de vigilância, estrutura que serve de base para a economia de vigilância, habitua a psique individual a realidade de estar sendo seguido, analisado, minerado e modificado e a guia a ser complacente. Por mais que se tente racionalizar esse processo com um grau de cinismo enquanto mecanismo de defesa, imaginando que não há problema, ou que não existe nada a ser escondido, se cria tão somente uma falsa sensação de segurança.

A autora defende que esse sistema age por meio de assimetrias nunca antes vistas referentes ao conhecimento e ao poder dele resultante, acumulando vastos domínios de conhecimento novo gerados pela população, mas que serão utilizados por terceiros. Em suas palavras:

O capitalismo de vigilância vai na direção oposta à do sonho digital dos primeiros tempos, relegando o *Aware Home* a dias longínquos. Em vez disso, despe a ilusão de que a forma conectada em rede tem algum tipo de conteúdo moral inerente, que estar “conectado” seja, de alguma forma, intrinsecamente pró-social e inclusivo ou com uma tendência natural à democratização do conhecimento. A conexão digital é agora um meio para fins comerciais de terceiros. Ele revive a velha imagem que Karl Marx desenhou do capitalismo como um vampiro que se alimenta do trabalho, mas agora com uma reviravolta. Em vez do trabalho, o capitalismo de vigilância se alimenta de todo aspecto de toda a experiência humana.²⁰

¹⁷ MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

¹⁸ G1 MG. **Sites educacionais dos governos de MG e SP coletaram dados de estudantes para empresas de publicidade, diz Human Rights Watch**. Disponível em: < <https://g1.globo.com/mg/minas-gerais/noticia/2023/04/03/sites-educacionais-de-mg-e-sp-coletaram-e-enviaram-dados-de-estudantes-para-empresas-de-publicidade-diz-human-rights-watch.ghtml>>. Acesso em: 14 Maio 2023.

¹⁹ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**. 1. ed. Rio de Janeiro: Intrínseca, 2021, p. 23.

²⁰ *Idem, ibidem*, p. 24.

Para os grandes pioneiros desse movimento como o Google e o Facebook, não existiu uma frente contrária expressiva, e a implantação do sistema se deu sem grandes empecilhos jurídicos, culturais ou legislativos. Dessa maneira, dados os processos apontados até aqui, em última análise, mesmo os “usuários resistentes não serão obstáculos à expropriação de dados. Nenhuma restrição moral, jurídica ou social vai impedir as empresas de encontrarem, reivindicarem e analisarem o comportamento alheio com propósitos comerciais”²¹.

Os questionamentos a respeito da regulamentação dos dados pessoais, ou de qualquer resposta do Direito aos efeitos produzidos pela sociedade da vigilância no âmbito das relações sociais, deve considerar o quadro aqui exposto, partindo da premissa base de que a economia de vigilância se constituiu a partir de um ativo que, inerentemente, não é de sua titularidade.

Importa, pois, interromper o fluxo de submissão aos interesses econômicos da indústria, fortalecendo a discussão a respeito da proteção dos dados pessoais, impulsionando mais avanços normativos, e convidando os indivíduos à conversa a respeito de seus dados, devidamente empoderando a classe que vem tendo suas informações captadas de forma ilícita, sobretudo por meio de táticas que os alienam da racionalização a respeito do que ocorre de fato.

2.2 Direito a proteção de dados: desenvolvimento e aspectos relevantes

A regulamentação da proteção de dados pessoais implica diretamente em uma disciplina da liberdade, da inovação e do desenvolvimento. E, num mundo em que a forma como cada indivíduo vem a ser enxergado está associada a projeção de seus dados pessoais, transborda também no exercício da cidadania e na caracterização de seus direitos²².

Nesse contexto, historicamente, as normas de proteção de dados pessoais incumbiram-se de garantir a privacidade e os direitos fundamentais e, também, estimular o desenvolvimento da economia, agindo numa função dupla.

Desde o julgamento da constitucionalidade da Lei do Censo alemã em 1983, que reconheceu pela primeira vez o ideal de autodeterminação informativa²³, a compreensão a

²¹ *Idem, ibidem*, p. 105.

²² BIONI, Bruno Ricardo. **Por que proteção de dados importa?** TEDxPinheiros, 2018. Disponível em <<https://www.youtube.com/watch?v=TzI5VfvQA6I>>. Acesso em 28 Jul. 2023.

²³ TSCHENTSCHER, Peter; BROICHHAGEN, Seven. Urteil des Ersten Senats vom 15 Dezember 1983 auf die mündliche Verhandlung vom 18 und 19 oktober in den Verfahren über die Verfassungsbeschwerden. 1983. Disponível em: <<http://www.servat.unibe.ch/dfr/bv065001.html>>. Acesso em: 18 Jul. 2023

respeito da proteção de dados vem envolvendo o direito do indivíduo de autodeterminar as suas informações pessoais.

Essa vertente perdura até hoje, diante da tendência legislativa de utilizar o consentimento do titular como pilar normativo, idealizando que este seria capaz de controlar seus dados através da emissão de autorizações. O uso dessa terminologia, ademais, costumeiramente abre espaço a uma interpretação equivocada de que o consentimento do titular dos dados teria primazia na proteção dos dados pessoais, com a intenção de que o próprio indivíduo se responsabilize por suas informações pessoais²⁴.

O movimento global moderno de regulação e normatização da proteção de dados ganhou força e impulso com o Regime Geral de Proteção de Dados - RGPD, que entrou em vigor em maio de 2018 substituindo leis e regulações nacionais em vigor na Europa até então. Os esforços do texto guiavam à eliminação das inconsistências em leis nacionais, ampliação do âmbito de proteção da privacidade e modernização legislativa frente aos novos desafios tecnológicos, políticos e econômicos.

Se considera a redação da RGPD o ponto de chegada da longa jornada europeia em busca da proteção de dados pessoais e da necessidade de implementar uma dinâmica de segurança de dados consistente e uniforme em todo o território do continente. Suas repercussões, todavia, ultrapassaram tal limite geográfico, impulsionando a criação de novas legislações ao redor do mundo para que países sem previsões legais a respeito de matéria não se encontrassem impossibilitados de negociar com membros da União Europeia, consequência da sanção prevista pela RGPD com o intuito de garantir maior segurança jurídica²⁵.

Até a aprovação da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), a matéria contava apenas com leis setoriais para sua regulamentação no Brasil. Era o caso do Código de Defesa do Consumidor, que disciplinou os bancos de dados e cadastros de consumidores; da Lei do Cadastro Positivo (Lei 12.414/2011), que disciplinou os bancos de dados utilizados para concessão de crédito; e do Marco Civil da Internet (Lei 12.965/2014), que elencou a proteção da privacidade e dos dados pessoais como um de seus pilares, somados a neutralidade de rede e a liberdade de expressão.

²⁴ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 198.

²⁵ BIONI, Bruno Ricardo; MENDES, Laura Schertel. Regulamento europeu de proteção de dados pessoais e a lei geral brasileira de proteção de dados: mapeando convergências na direção de um nível de equivalência. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato (Coord.). **Lei geral de proteção de dados e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 550.

Nesse cenário, o Direito se via limitado a fazer um trabalho de recorte e colagem para tratar do tema, num panorama repleto de lacunas em diversos setores relevantes da economia e sem uma abordagem consistente no regramento. Em diversos países, as leis gerais de proteção de dados de quarta geração que antecederam a LGPD procuravam suprir as desvantagens da abordagem individualista a respeito da autodeterminação informacional. Como sustenta Doneda:

Entre as técnicas utilizadas, estas leis procuraram fortalecer a posição da pessoa em relação às entidades que coletam e processam seus dados, reconhecendo o desequilíbrio nesta relação, que não era resolvido com medidas que simplesmente reconheciam o direito à autodeterminação informativa; outra, paradoxalmente, é a própria redução do papel da decisão individual de autodeterminação informativa. Isto ocorre porque se parte do pressuposto de que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, à qual não pode ser conferida exclusivamente a uma decisão individual²⁶.

O retrato caracterizava uma evidente insegurança jurídica, dificultando a formulação de políticas públicas associadas ao manuseio de dados e de parcerias público-privadas, obstando a comunicação entre setores da indústria para o desenvolvimento de novos modelos de negócio, e deixando o cidadão comum sem qualquer previsão de proteção integral de seus dados²⁷.

Aprecia-se, nesse contexto, a inserção da proteção de dados pessoais como um novo direito da personalidade, superando finalmente as posições de que esta seria uma implicação do direito à privacidade. Stefano Rodotà, um dos precursores da discussão a respeito do tema, foi pioneiro no apontamento da proteção de dados como uma categoria autônoma²⁸.

O direito à privacidade, convencionado a ser compreendido como o direito de ser deixado só, tem seu conteúdo configurado numa lógica subentendida enquanto liberdade negativa do indivíduo de não sofrer interferências alheias²⁹. A proteção de dados, por sua vez, requer o dinamismo de uma liberdade positiva do controle das informações pessoais, e demandou a ampliação normativa que reconhecesse sua autonomia e os efetivos desdobramentos de sua tutela jurídica.

²⁶ *Idem, ibidem*, p. 169.

²⁷ BIONI, Bruno Ricardo. **Brasil precisa ser competitivo em uma economia de dados**. *Jornal Valor Econômico*, jul. 2018. Disponível em: < <https://www.valor.com.br/opiniaio/5669703/paisprecisa-ser-competitivo-em-uma-economia-de-dados>>. Acesso em: 14 Maio 2023.

²⁸ RODOTÀ, Stefano. Trad. Maria Celina Bodin de Moraes. **A Vida na Sociedade da Vigilância: Privacidade Hoje**. 1 ed. Rio de Janeiro: Renovar, 2008.

²⁹ COSTA JÚNIOR, Paulo José da. **O direito de estar só: tutela penal da intimidade**. São Paulo: Revista dos Tribunais, 2007. Acesso em: 10 Jun. 2023.

Para tanto, o poder constituinte derivado reformador consolidou o entendimento dos tribunais, que por muito tempo atuaram como um dos mecanismos de combate a insegurança jurídica causada pela falta de regulamentação da matéria no Brasil, e através da EC 115/22 incluiu a proteção de dados pessoais no rol de direitos e garantias fundamentais da Constituição Federal³⁰.

Sarlet expõe que a proteção de dados, agora direito fundamental, assumiu particular relevância quando compreendidas também as lacunas regulatórias presentes na LGPD, reconhecendo a existência de uma “zona livre” de proteção de dados no sistema brasileiro, que requer do Estado não só o zelo pela consistência constitucional, mas também integração que assegure ao direito fundamental sua eficácia e efetividade³¹.

Ademais, no âmbito constitucional, percebe-se que a Carta Magna, em seu Art. 170, *Caput* e inciso V, ao apontar a proteção do consumidor e a dignidade da pessoa humana como princípios da ordem econômica, corrobora com o entendimento de que as normas de proteção de dados perfeitamente atuam na dupla função há pouco mencionada.

Tal comando constitucional foi internalizado pela LGPD, visto que em suas disposições preliminares enuncia a disciplina de proteção de dados pessoais objetivando a proteção dos direitos fundamentais e o livre desenvolvimento da personalidade, sendo estes, somados ao desenvolvimento econômico-tecnológico e a inovação, os fundamentos que a dão causa³².

Foi estabelecido no corpo da lei uma dialética normativa de conciliação das diversas nuances do tema, num esforço para permitir a entrada dos cidadãos no plano de controle de seus dados pessoais, atentando ao fato de que a forma como o consentimento deve ser trabalhado na regulamentação é extremamente particular.

³⁰ BRASIL. Constituição (1988). **Emenda constitucional nº 115**, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm>. Acesso em 20 Jul. 2023.

³¹ SARLET, Ingo. **A EC 115/22 e a proteção de dados pessoais como Direito Fundamental**. Revista Consultor Jurídico, São Paulo, 11 de mar. de 2022. Disponível em: <https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protexao-dados-pessoais-direito-fundamental>. Acesso em: 24 Jun. 2023.

³² BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/114020.htm>. Acesso em: 14 Jun. 2023.

Para que a chamada autodeterminação informacional seja efetiva na discussão do consentimento do titular de dados pessoais, o elemento volitivo expresso pelo cidadão deve ser associado à segurança do fluxo informacional, garantindo, por fim, a tutela do direito.

A LGPD adjetiva o consentimento em seu art. 5º, XII, enquanto “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. Sua posição topográfica no texto final, aprovado e sancionado, afastou sua atuação como única base legal para o tratamento de dados que havia se estipulado no anteprojeto de lei, ao passo que foi posicionado somente como uma das hipóteses legais para o tratamento de dados e não como a cabeça do dispositivo³³. Não foi posto, ademais, como superior hierárquico das demais bases legais, estando todas elas dispostas de forma horizontal nos incisos do Art. 7º da LGPD³⁴.

Entretanto, a carga participativa do indivíduo no fluxo informacional não deixou de ser posicionada de forma central, apesar da multiplicidade de bases legais dispostas na lei. O consentimento é abordado de forma extensiva ao longo do texto, sendo citado expressamente 35 vezes ao longo da LGPD, e a regulação proposta não é meramente quantitativa diante do esforço em atribuir maiores entornos à figura do consentimento³⁵.

Não houve, todavia, previsão suficiente em relação à dificuldade que a lei enfrentaria para se concretizar diante dos termos de uso de redes sociais, visto que a estrutura não se adequa de forma satisfatória. Houve uma autorregulação do mercado de dados, feita como

³³ Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

³⁴ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Gen, Editora Forense, 2020, p. 157.

³⁵ *Idem, ibidem*, p. 158.

forma de manobra através das políticas de privacidade. É uma modalidade de regulação falha em sua gênese, considerando hipóteses como as do recolhimento do consentimento expresso feito, basicamente, por meio de um contrato de adesão³⁶.

Este trabalho busca compreender o paradigma normativo que envolve o consentimento, avançando para a análise da posição onde este se encontra na discussão a respeito da proteção de dados pessoais. Para tanto, deve diagnosticar o momento em que se situa no ordenamento jurídico brasileiro pós-LGPD e reavaliar a estratégia regulatória adotada pelo legislador a respeito da autodeterminação informacional, para que possa, por fim, vislumbrar soluções efetivas no processo de empoderar os titulares de dados pessoais, sem que haja uma atribuição do dever de proteção à esfera individual, impedindo, em última análise, a concretização do direito.

³⁶ *Idem, ibidem*, p. 188.

3. AVALIAÇÃO SUBSTANTIVA E PROCEDIMENTAL DO CONSENTIMENTO ENQUANTO PROTAGONISTA DA PROTEÇÃO DE DADOS PESSOAIS

3.1 Identificação da (hiper)vulnerabilidade do titular de dados e a assimetria no paradigma do fluxo informacional

Leciona Bauman³⁷ que a vigilância na modernidade se tornou líquida, e não consta mais com o caráter sólido e firme que um dia se considerou possível através de um único observador. As pessoas agora vivem em constante estado de vigilância, e esta é feita de forma dispersa, extensiva e opaca.

O fluxo informacional aponta para a necessidade de reavaliação de sua estratégia regulatória a partir do reconhecimento do caráter fluído dos dados pessoais, sendo este mais um fator que dificulta o reconhecimento da autodeterminação informacional na realidade fática dos titulares de dados.

A complexidade desse fluxo compreende a estruturação física da rede (*network*), e o entendimento que a captação e tratamento do agregado de dados são feitos por um aglomerado de agentes antes de culminarem nas abordagens publicitárias personalizadas.

No entendimento de Barocas e Nissenbaum³⁸, os agentes que ativamente compõem essa rede tratam as pequenas informações pessoais, e como fruto do esforço de agregar e compilar esses dados, criam um perfil preciso dos hábitos de consumo do cidadão. A pluralidade de agentes, bem como a impossibilidade de determinar e prever esse fluxo informacional, contribuem para a concepção do seu caráter fluído.

Aqui, pode ser considerado descaracterizado o sistema de vigilância imaginado por Orwell³⁹, que ao idealizar uma sociedade distópica em seu celebrado romance “1984” atribuiu à entidade centralizada do Grande Irmão o acesso irrestrito aos cidadãos. O status de observação constante ainda se mostra presente, mas o autor não pôde prever que a realidade contemporânea se mostraria ainda mais opressiva diante da estrutura do fluxo informacional, não havendo momentos em que os cidadãos pudessem fugir do controle e da vigilância a que se submetem.

A problemática se desenvolve quando analisada a capacitação do indivíduo para controlar seus dados pessoais. O processo de racionalização e as características psicológicas

³⁷ BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida**. 1. ed., Rio de Janeiro: Zahar, 2014, p. 10.

³⁸ BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run Around Consent and Anonymity. *Em*: LANE, Julia et al. **Privacy, Big Data and the Public Good**. Cambridge: Cambridge University Press, 2014, p. 59.

³⁹ ORWELL, George. **1984**. São Paulo: Principis, 2021.

individuais se apresentam imediatamente como fatores que obscurecem o desenvolvimento da tomada de decisão.

Ian Kerr⁴⁰, nos seus estudos a respeito da teoria da decisão, identifica ponto integral nesse quadro ao apontar que o valor utilitário subjetivo atribuído pelos indivíduos a determinado resultado varia de acordo com o tempo que levará para que este produza seus efeitos. Basicamente, o valor que se atribui a uma perda ou ganho vivido no presente é maior do que o valor atribuído a mesma coisa, mas no futuro.

Esse entendimento é o que evidencia a propensão do titular de dados de minar o controle de seus dados pessoais a favor de benefícios imediatos promovidos pela indústria da informação, como bens de consumo digital ou serviços disponibilizados on-line.

Ademais, ainda na hipótese otimista de uma reavaliação da tomada de decisão após o usufruto gozado pelo sujeito, raramente haverá uma revogação futura do consentimento, que entende mais significativo o bem ou serviço “gratuito” que a segurança de seus dados. Os consumidores, de modo geral, não retiram seus dados em um momento futuro caso se tornem insatisfeitos com o tratamento de dados feito pela empresa⁴¹.

Os potenciais danos sofridos pela perda do controle dos dados não são considerados, visto que se trata de efeitos que somente se apresentarão no futuro, e o processo de racionalizar esse quadro poderia implicar na escolha ativa de abdicar de um benefício apresentado no presente.

É o que Trandburg⁴² compreende como o modelo adotado pela publicidade comportamental, em que o “compre agora, pague depois” implica em coletas de dados contínuas ao longo do tempo para que se possa continuar aproveitando de um serviço. Evidencia a autora que

Ao contrário de um aluguel ou de uma assinatura de academia, os pagamentos não são fixos antecipadamente nem são coletados em intervalos de uma maneira que seja evidente para o consumidor. Em vez disso, o acesso de uma empresa aos dados do consumidor ocorre silenciosamente e de forma incremental nos bastidores, a menos que e até que algum dano potencial detectável e rastreável se concretize.

⁴⁰ KERR, Ian; BARRIGAR, Jennifer; BURKELL, Jacquelyn; BLACK, Katie. Soft surveillance, hard consent. *Em*: KERR, Ian et al. **Lessons from the identity trail : anonymity, privacy and identity in a networked society**. New York: Oxford University Press, 2009, p. 19.

⁴¹ TRANDBURG, Katherine. **Free Fall: The Online Market's Consumer Preference Disconnect**. NYU School of Law, Public Law Research Paper, 2013., p. 52. Disponível em: <<https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1511&context=uclf>>. Acesso em: 10 Ago. 2023.

⁴² *Idem, ibidem*, p. 57.

Nesse sentido, Bioni⁴³ aponta que após o ganho imediato proposto, o usuário se encontra exposto ao tratamento dos dados triviais que forem agregados, sendo este capaz de gerar uma plêiade de situações adversas. Informações sensíveis podem ser reveladas, uso inadequado dos dados pode resultar em danos patrimoniais e extrapatrimoniais, e os dados podem ser compartilhados com terceiros, minando ainda mais a perspectiva de controle dentro do fluxo informacional.

Diante desse paradigma, Modesto⁴⁴ sinaliza que

[...] Deve-se evitar a lógica do “tudo ou nada”, isto é, ou o titular consente com o tratamento de seus dados pessoais ou não pode ter acesso a determinado serviço, uma vez que isso representaria um demasiado custo social ao titular, a ser suportado em nome da sua autodeterminação informativa, levando o indivíduo a fornecer seu consentimento apenas porque é pré-requisito para a utilização de um serviço de que necessita. Não há, nessas hipóteses, liberdade de escolha, uma vez que o indivíduo é pressionado a fornecer seus dados.

Estudos empíricos demonstram que os usuários não estão capacitados para tomar decisões informadas a respeito de seus dados pessoais⁴⁵, e mesmo alocando esforços para que os consumidores se tornem aptos a controlar seus dados, a indústria se desenvolve e cria novos mecanismos capazes de neutralizar essas diligências⁴⁶.

A estruturação da rede pode simplesmente optar por deliberadamente se omitir do papel de atribuir clareza ao procedimento de captura de dados, utilizando termos técnicos que não facilmente compreendidos pela massa de usuários, ainda que sejam conceitos amplamente utilizados, como os *cookies*. Expressiva parte da população não compreende o significado dos símbolos adotados e as implicações de suas escolhas.

Ainda que considerem injustificada e indesejável a coleta de seus dados pessoais, os usuários aceitam a dinâmica como algo inevitável. Holland⁴⁷ identifica o fenômeno como o

⁴³ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Gen, Editora Forense, 2020, p. 175.

⁴⁴ MODESTO, Jéssica Andrade. **O direito à privacidade na sociedade da informação à luz da lei geral de proteção de dados pessoais: uma análise da (in)efetividade da lei nº 13.709/2018 no Brasil a partir do estudo comparativo com o regulamento geral de proteção de dados da União Europeia**. 2021. 364 f. Dissertação (Mestrado em Direito) - Universidade Federal de Alagoas, Alagoas, 2021, p. 125.

⁴⁵ CRANOR, Lorrie Faith; MCDONALD, Aleecia. **Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising**, p. 1. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092>. Acesso em: 05 Ago. 2023.

⁴⁶ UTZ, Christine et al. (Un)informed consent: studying GDPR consent notices in the field. *Em: 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*, November 11–15, 2019, London, United Kingdom. ACM, New York, NY, USA. Disponível em: <<https://arxiv.org/pdf/1909.02638.pdf>>. Acesso em: 08 Ago. 2023.

⁴⁷ HOLLAND, Brian. **Privacy Paradox 2.0**. 19 Widener L.J., 2010.. Disponível em: <<http://ssrn.com/abstract=1584443>>. Acesso em: 05 Ago. 2023.

paradoxo da privacidade, onde o indivíduo atribui valor a sua privacidade, mas ainda toma atitudes que dificultam sua proteção. O consumidor, em última análise, se apresenta resignado diante desse quadro, e a indústria aproveita da situação para impulsionar uma narrativa de que os indivíduos não se importam ou aceitam a dinâmica econômica em tela⁴⁸.

É um quadro traiçoeiro e que facilita a manipulação da tomada de decisão, importando na convicção de que a criação de tecnologias voltadas à tutela da proteção de dados deve se atentar a sua capacidade de produzir os efeitos desejados, utilizando uma arquitetura clara e funcional.

Essa análise de comportamento e autonomia mistifica a crença de que se pode esperar tomadas de decisão racionais por parte dos titulares de dados no processo de controle das suas informações, evidenciando o status de vulnerabilidade e afastando ainda mais um ideal utópico de simetria entre estes e os agentes da economia da informação.

A vulnerabilidade do cidadão é identificada, portanto, a partir da sua maior suscetibilidade a sofrer danos decorrentes de sua inserção no mercado informacional, e a assimetria se apresenta em um modelo híbrido, tanto econômica quanto informacional, conforme o número de sujeitos no outro pólo da relação agrava o desequilíbrio entre os agentes.

Importa ao direito atuar de forma instrumental na regulação dessa assimetria, conforme o faz em outras áreas do saber jurídico. No âmbito do direito do consumidor, regula a vulnerabilidade deste diante dos prestadores e fornecedores de serviços e produtos⁴⁹. No direito do trabalho, por sua vez, identifica a vulnerabilidade do trabalhador diante do empregador no prisma da disparidade entre poderes econômicos⁵⁰. São áreas do saber jurídico onde se busca proteger o elemento mais frágil numa relação econômica, sendo necessário expandir esse olhar ao âmbito da proteção de dados.

Ao passo que a vulnerabilidade vai além da subjetividade pessoal do consumidor, ocorrendo de forma objetiva devido a nova economia que o vulnerabiliza pela própria forma como opera, se mostra necessária uma racionalização normativa direcionada. A estratégia de

⁴⁸ TUROW, Joseph; HENESSY, Michael; DRAPER, Nora. **The tradeoff fallacy: how marketers are misrepresenting and opening them up to exploitation.** Disponível em: <<https://dx.doi.org/10.2139/ssrn.2820060>>. Acesso em: 15 Ago. 2023.

⁴⁹ COMPARATO, Fábio Konder. A proteção do consumidor na Constituição brasileira de 1988. *Em*: MARQUES, Claudia Lima; MIRAGEM, Bruno (Org). **Direito do consumidor: vulnerabilidade do consumidor e modelos de proteção.** São Paulo: Revista dos Tribunais, 2011. v. 2, p. 190.

⁵⁰ LEITE, Carlos Henrique Bezerra. **Curso de direito do trabalho.** 11. ed. São Paulo: Saraiva Educação, 2019.

regulação deve afastar o ideal de que essa parte vulnerável consiste em um sujeito racional e capacitado para a proteção e controle de seus dados.

Para Blume⁵¹, a posição central do consentimento no debate normativo parte de uma perspectiva que intenta tornar válido o processo de extração de dados, sendo uma necessidade para que os controladores possam atuar de forma legal e atingir seus objetivos na economia da informação. O pilar da discussão normativa atende, de forma prioritária, uma necessidade da indústria, e não a busca pela efetivação da proteção de dados pessoais dos usuários.

A reavaliação da estrutura normativa da proteção de dados requer a compreensão do caráter (hiper)vulnerável do titular de dados dentro do fluxo informacional. Sem essa análise, não é possível confeccionar intervenções normativas que, somadas a instauração de novos parâmetros e diretrizes de construção das redes, resultem na garantia da autonomia do cidadão, condicionem a tomada de decisão informada, corrijam o papel de protagonismo do consentimento e viabilizem um quadro realizado da autodeterminação informacional.

3.2 Estratégias regulatórias do consentimento

Embora o progresso das leis de proteção ao de dados ao longo das décadas tenha trazido uma adjetivação e potencial delimitação do consentimento, conforme transcrito na LGPD no sentido de ser inequívoco, expresso, informado, específico ou livre, a forma como se dará seu tratamento não foi abordada de maneira suficiente.

Tal lacuna permitiu que o mercado informacional operasse de forma independente, realizando sua própria regulação. Foi adotada a técnica de massificação de relações contratuais ordinárias, feita com a instrumentalização das políticas de privacidade, que captam o consentimento para o tratamento de dados sem grandes empecilhos diante de sua natureza jurídica equiparável a um contrato de adesão, sem que haja a possibilidade de barganha por parte do titular de dados.

Conforme identifica Lima⁵², a manifestação expressa do consentimento em meio eletrônico se dá no momento em que o adquirente clica no ícone referente à expressão de

⁵¹ BLUME, Peter. **The inherent contradictions in data protection law**. International Data Privacy Law, 2. ed, n. 1, 2012, pp. 27-28.

⁵² LIMA, Cíntia Rosa Pereira de. **Validade e obrigatoriedade dos contratos de adesão eletrônicos (shrinkwrap e click-wrap) e dos termos e condições de uso (browse-wrap)**. Tese (Doutorado) - Faculdade de Direito da Universidade de São Paulo, São Paulo, 2009, p. 656. Disponível em

anuência, geralmente exposto com a terminologia de "eu aceito" ou "eu concordo". A partir desse momento, o indivíduo está obrigado às cláusulas contratuais impostas, com as quais expressamente concordou.

É inevitável a identificação de um teor padronizado dos instrumentos contratuais ao passo que o conteúdo abordado é integralmente regulado pelo fornecedor, e sua apresentação ao consumidor se dá de maneira predisposta⁵³. A participação do indivíduo na discussão a respeito do tratamento de seus dados não existe, e sua prerrogativa de exercer controle sobre suas informações é diluída à medida que tão somente poderá aderir ou não ao que foi previamente estabelecido pelos agentes do mercado informacional.

Como sustenta Bioni⁵⁴:

[...] Essa ferramenta contratual tem sido utilizada para o esvaziamento de qualquer esfera de controle dos dados pessoais. Tais termos contratuais impõem, às vezes, um “cheque em branco”, cujo preenchimento – a utilização dos dados pessoais – fica a belprazer daquele que estipulou unilateralmente as suas cláusulas contratuais.

Os termos de uso e políticas de privacidade não prestam informações adequadas aos usuários, costumam apresentar dificuldades para sua visualização, não são claros em sua abordagem técnica e são excessivamente longos⁵⁵. Conforme estudo desenvolvido por Cranor e McDonald, caso um usuário fizesse a devida leitura de todos os termos de privacidade que tem contato ao longo de um ano, numa análise do comportamento digital do indivíduo americano médio, o tempo despendido seria de 201 horas⁵⁶.

A transparência e a colaboração foram previstas pelo legislador na redação do Marco Civil da Internet⁵⁷ para combater essa espécie de dinâmica, mas a negligência das empresas que continuam empregando termos técnicos e jargões jurídicos em textos extensos resultam em uma

<https://teses.usp.br/teses/disponiveis/2/2131/tde-03062011-090910/publico/Tese_Final_TOTAL.pdf>. Acesso em: 10 Ago. 2023.

⁵³ GOMES, Orlando. **Contratos**. 26. ed., Rio de Janeiro: Forense, 2009, p. 159.

⁵⁴ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Gen, Editora Forense, 2020, p. 190.

⁵⁵ UNIÃO EUROPEIA. Comissão Europeia. **Special Eurobarometer 487a** - Report: The general data protection regulation. Jun. 2019, p. 6. Disponível em: <<https://cnpd.public.lu/content/dam/cnpd/fr/actualites/international/2019/ebs487a-GDPR-sum-en.pdf>>. Acesso em: 17 Ago. 2023.

⁵⁶ MCDONALD, Aleecia.; CRANOR, Lorrie Faith. **The Cost of Reading Privacy Policies**. Journal of Law and Policy for Information Society, 2008, p. 19. Disponível em <<https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>>. Acesso em: 12 Ago. 2023.

⁵⁷ “Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade.”

leitura superficial, abreviada e insuficiente por parte do usuário, que não compreende a extensão dos termos e condições impostos.

O engessamento desses contratos de adesão dificulta o processo de tomada de decisão informada e obstrui a aplicação dos princípios que guiam o ordenamento jurídico brasileiro. O equilíbrio contratual e a autonomia do indivíduo precisam ser favorecidos para que o consentimento colhido seja considerado informado.

Desse modo, as políticas de privacidade não contribuem no panorama da proteção de dados, sendo instrumentos ineficientes no processo de capacitação do cidadão para regular suas informações pessoais, e atuam efetivamente como mais um fator que evidencia a assimetria entre os pólos da relação informacional. Não podem ser consideradas ferramentas ideais para a proteção contratual do consumidor, e constam somente como elemento adicional no quadro da proteção de dados.

O objetivo de repensar esse modelo de estratégia regulatória aponta para o surgimento e expansão das PETs (*privacy enhancing technologies*), novas tecnologias que fazem contraponto aos clássicos *trackers* e *cookies* e atuam como instrumento da proteção de dados pessoais. São projetos que reutilizam os avanços tecnológicos, estruturas digitais e linguagem das redes para criar caminhos mais seguros para o tráfego de dados.

É o exemplo do desenvolvimento e ampliação dos recursos de criptografia e dos mecanismos de navegação em modo anônimo, que dão ao cidadão ferramentas úteis, de fácil acesso e de aplicabilidade extensiva ao caminhar dentro do fluxo informacional.

As PETs, enquanto tecnologias benignas que auxiliam e facilitam a privacidade, são produto alinhados à abordagem *privacy by design*⁵⁸, sendo esta internalizada no texto normativo da LGPD em seu art. 46, §2º⁵⁹. Os esforços para sua expansão e ampla utilização contém potencial para que se tornem um dos elementos mais frutíferos na discussão a respeito da proteção de dados nas próximas décadas, sendo estes alguns dos mecanismos imediatamente capazes de atribuir aos indivíduos controle sobre suas informações pessoais.

⁵⁸ Conceituação desenvolvida por Ann Couvakin, que entende necessário encorajar os agentes de tratamento de dados a desenvolver medidas de segurança e proteção da privacidade e dos dados pessoais em todas as fases de desenvolvimento de um produto ou serviço, desde a concepção até a execução, não sendo suficiente a mera produção de texto normativo que busque a tutela desses direitos e disponha de medidas repressivas *ex post* diante de abusos sofridos.

⁵⁹ Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. [...] § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Aplicar somente o Direito ou apenas a tecnologia nas estratégias de materialização da proteção de dados limitaria as possíveis conquistas e avanços na matéria, e a aliança desses dois pilares cria melhores condições para a regulação ética do fluxo de informações.

Lessig⁶⁰ salienta que o Direito não é o único vetor de regulação da internet, ao passo que convive com outros agentes responsáveis por essa função, ao exemplo das dinâmicas do mercado privado, da tecnologia e das constringências sociais. A tecnologia não deve ser interpretada somente como um fardo na luta pela tutela da proteção de dados, mas sim utilizada em novas formas que permitam a produção de efeitos positivos na busca por simetria entre os agentes do mercado informacional.

Essa aliança e atuação complementar entre o Direito e a tecnologia é um dos motores para a tutela da proteção de dados pessoais, ao passo que limitações e falhas em um âmbito podem ser atendidas pelo outro. Conforme aponta Zanatta⁶¹, a disciplina jurídica é capaz de proteger os indivíduos de violações e ofensas a seus direitos fundamentais, enquanto a tecnologia pode criar ambientes virtuais favoráveis à proteção destes.

Em síntese, corrobora Doneda⁶²:

Evidentemente, a tecnologia não pode, por si só, ser tomada como um instrumento de tutela e nem sequer é passível de ser qualificada juridicamente. Porém, na medida em que ela atua sobre a arquitetura na qual são tratados os dados pessoais, ela pode interferir concretamente na configuração jurídica do problema, assim como pode ser o instrumento de atuação de políticas públicas, por exemplo. Trata-se muito mais do que ações privadas isoladas: a utilização da tecnologia como meio para regular a proteção de dados pessoais é encarada seriamente por boa parte da doutrina e não somente em matérias relacionadas à privacidade, além de enquadrar-se no conceito de regulação por meio da manipulação da arquitetura de comunicação: assim, alterando-se a estrutura das comunicações de forma que a privacidade torne-se tecnicamente possível e acessível, assim como os instrumentos de controle sobre as próprias informações pessoais tornem-se mais claros e ostensivos, diminuir-se-ia a demanda pelas vias legais de garantia.

Nesse ponto, se estabelece uma conversa entre as novas tecnologias e o ideal de autodeterminação informacional, atribuindo aos indivíduos (hiper)vulneráveis novas formas de buscar a simetria na dinâmica da economia da informação. A tecnologia pode e deve continuar sendo usada como instrumento de operacionalização da autodeterminação, o que atribui às

⁶⁰ LESSIG, Lawrence. **Code: And Other Laws of Cyberspace**. 2. ed., New York: Basic Books, 2006, p. 226.

⁶¹ ZANATTA, Rafael. A proteção de dados entre leis, códigos e programação: os limites do Marco Civil da Internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. **Direito & Internet III: Marco Civil da Internet**. São Paulo: Quartier Latin, 2015.

⁶² DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 291.

PETs uma dimensão normativa e a posiciona como efetivo aparato no controle racional dos dados pessoais e na tomada de decisão informada⁶³.

3.3 Posição e adjetivação do consentimento no quadro normativo brasileiro

O consentimento, em sua definição clássica no âmbito do direito privado pátrio, se apresenta como um dos temas associados ao estudo dos defeitos dos negócios jurídicos, regulando a captação do elemento volitivo a fim de aferir validade a estes uma vez identificado como “livre e esclarecido”. A LGPD, em seu Art. 8º, § 3º, flerta com o Código Civil ao ponto que regula os vícios de consentimento no tratamento de dados pessoais⁶⁴.

A abertura ao diálogo entre as fontes e a aproximação do saber jurídico nas diversas áreas do conhecimento é imprescindível para analisar, delimitar e compreender o consentimento e sua função no âmbito da proteção de dados, dada a juventude da matéria quando vista junto a seus pares.

A LGPD traz em seu texto a positivação do consentimento no âmbito da tutela dos dados pessoais com os seguintes contornos:

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

[...]

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Os adjetivos escolhidos pelo legislador são uma bússola para a compreensão do ideal de consentimento válido, cabendo a análise de cada ponto elencado.

Destarte, a manifestação “livre” implica na liberdade do titular dos dados pessoais de barganhar e atuar de forma capacitada no âmbito do mercado informacional, contando com o pleno usufruto de seu livre-arbítrio. Nesse vetor, se busca mitigar a dinâmica de assimetria já destacada anteriormente.

A manifestação “informada”, por sua vez, compreende a necessidade de afastar as obscuridades e opacidades no processo de tomada de decisão, capacitando até mesmo os indivíduos mais leigos a tomar conhecimento suficiente para que atuem em sua autoproteção.

⁶³ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Gen, Editora Forense, 2020, p. 207.

⁶⁴ *Idem, ibidem*, p. 198.

É o instrumento basilar para o processo de empoderamento dos titulares de dados, e o mais efetivo na tentativa de atribuir simetria na relação entre os polos. Para tanto, as informações deverão ser “claras, precisas, e facilmente acessíveis”⁶⁵, e a pena caso esse grau de informação não seja atingido resulta na nulidade do consentimento⁶⁶.

A transparência foi evidenciada como elemento basilar para a produção do consentimento, evidenciando a necessidade de um manejo racional dos procedimentos que envolvam os dados pessoais.

Como enfatizam Ruaro e Sarlet⁶⁷,

A atual relação entre a proteção de dados pessoais e o processo de elaboração de consentimento na vida digital corresponde à observância tanto de um direito/dever de informação dos usuários quanto de um dever por parte dos agentes públicos e privados de garantir a deliberação livre e, conseqüentemente, a revisão e a possibilidade de retirada da anuência a qualquer momento sem prejuízo algum, mediante a garantia de que o tráfego desses dados não implicará em danos de espécie alguma.

Com a leitura complementar do Art. 9º, § 3º do diploma normativo⁶⁸, infere-se que nas hipóteses em que o fornecimento de dados pessoais for requerido para que se possa utilizar algum bem ou serviço, o cidadão deverá ser devidamente informado dessa dinâmica e da maneira como se dará a tutela dos seus direitos, no que pese a possibilidade de revogação do consentimento.

Por fim, a manifestação “inequívoca” remete a impossibilidade de manipulação do consentimento de modo a desvirtuar sua finalidade originária, devendo ser as atividades de controle correspondentes ao que determina o princípio da finalidade⁶⁹, especificando o propósito e o destino que se dará aos dados coletados.

⁶⁵ Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

⁶⁶ Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva. [...] § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

⁶⁷ RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da lei geral de proteção de dados (LGPD) – Lei 13.709/2018. *Em*: BIONI, Bruno et al. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, p. 302.

⁶⁸ “Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei”.

⁶⁹ Art. 6º [...] 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;

A especificação dessa finalidade permite analisar se o consentimento do cidadão foi devidamente informado, o que não é possível quando utilizadas abordagens genéricas, a exemplo de requerimentos de dados para “para fins de melhorar a experiência”⁷⁰, e potencializar o ideal de que a menor quantidade possível de dados deverá ser colhida, tão somente para suprir uma função determinada e previamente informada de forma transparente.

Afastada a incidência dessa espécie de aprovação genérica, sempre que houver a necessidade de utilizar os dados do titular para fins diversos do que deu motivo a extração inicial, deverá ser iniciado um novo processo de anuência. Mesmo considerando a existência de bases de dados extensas e diversificadas montadas ao longo das décadas em que o mercado da informação se autorregulou. Se faz necessário, portanto, que estas passem por um processo de revisão e recebam a autorização dos titulares para continuar com as atividades de tratamento e processamento dos dados armazenados, efetuando o consentimento nos moldes de um ato jurídico pleno a partir da ampliação de seu ideal de validade e perfectibilidade⁷¹.

Quanto aos desdobramentos procedimentais do consentimento, anota Miragem⁷² que

A exigência de que o consentimento seja inequívoco associa-se a requisitos formais definidos pela lei. O art. 8º, caput, da LGPD, estabelece que o consentimento “deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.” A exigência de consentimento escrito ou por outro meio que demonstre a manifestação da vontade do titular revela o propósito de assegurar a certeza sobre a existência do consentimento e seu objeto. E no caso de o consentimento ser fornecido por escrito, o §1º do art. 8º, da LGPD define, ainda, que deverá constar em cláusula destacada “das demais cláusulas contratuais”. Lendo de outro modo: integrando um determinado instrumento contratual, a cláusula que preveja o consentimento do titular deve constar em destaque em relação às demais, justamente para permitir ser identificado como tal por aquele que venha a consentir.

A LGPD prevê, ainda, o adjetivo “específico” num rol taxativo, sendo caracterizado nas seguintes hipóteses: quando houver envolvimento de terceiros que não mantêm relação direta com o titular para o tratamento de seus dados, quando o dado coletado for de natureza sensível, quando se tratar de titulares com condição de vulnerabilidade (crianças e adolescentes) e em

⁷⁰ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Gen, Editora Forense, 2020, p. 202.

⁷¹ RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da lei geral de proteção de dados (LGPD) – Lei 13.709/2018. *Em*: BIONI, Bruno et al. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, p. 300.

⁷² MIRAGEM, Bruno. **A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor**. Revista dos Tribunais, São Paulo, v. 1009, 2019, p. 19. Disponível em: <<https://www.brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf>>. Acesso em: 19 Jul. 2023.

casos de transferência internacional em que os dados sejam encaminhados para um país que não adote o mesmo nível de rigor que o Brasil na tutela dos dados pessoais⁷³.

Trata-se de um esforço adicional para estender a proteção em hipóteses consideradas mais arriscadas pelo legislador. A sua concretização, no entanto, vem com o desafio de racionalizar um método que devidamente demonstre esse elevado teor de cuidado, que ficou aberto à interpretação no plano fático. Partindo desse ponto, as diretrizes de atuação certamente deverão englobar a maior participação possível do indivíduo, motivando uma tomada de decisão precisa na informação, e eficaz na declaração de vontade⁷⁴.

A extrema relevância do consentimento para a reafirmação da autonomia, guiada pela adjetivação apresentada, entra em choque com a realidade cotidiana que a enfraquece. A formação da vontade de maneira consciente e lúcida se vê manchada pela plêiade de aspectos problemáticos da economia da informação apontados ao longo deste capítulo.

Diante do exposto, verifica-se que existe uma dissonância entre o marco normativo da proteção de dados pessoais, centralizada na autodeterminação informacional, e a indústria que opera dentro da sociedade de informação. Para que a produção normativa presente possa efetivar seu objetivo de instrumentalizar o titular de dados, capacitando-o para controlar suas informações pessoais, deverá não só se aproveitar de forma pioneira das novas tecnologias, revertendo os papéis de poder no fluxo informacional, mas também alocar esforços para uma expansão da regulamentação da proteção de dados presente no arranjo jurídico-normativo, conforme será demonstrado no próximo capítulo.

⁷³ Arts. 7º, § 5º; 11, I; 14, § 1º; e 33, VIII da LGPD.

⁷⁴ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 245.

4. PARÂMETROS PARA A PARIDADE DE PODERES NAS RELAÇÕES INFORMACIONAIS E CAMINHOS PARA A CAPACITAÇÃO DO TITULAR DE DADOS (HIPER)VULNERÁVEL

4.1 Pontos de interesse na capacitação e empoderamento do titular de dados

Conforme exposto até aqui, a construção do ecossistema tecnológico agregador de informações e dados dentro de um evoluído aparato de compartilhamento tornou o fluxo informacional altamente volátil. A análise do paradigma do consentimento e da autodeterminação informacional deve, obrigatoriamente, considerar os papéis e a atuação de cada agente envolvido nesse ambiente e analisar de forma crítica a atuação de controle e gerenciamento dos dados dos titulares.

As obstruções objetivas vivenciadas de forma cotidiana pelos usuários no exercício do consentimento não podem ser ignoradas, e a capacitação para a tomada de decisão de forma informada será um dos maiores desafios para as próximas décadas do desenvolvimento da tutela desse novo direito da personalidade.

As problemáticas resultantes do uso em massa das redes sociais e da produção massiva de dados, desde a dinâmica do *trade-off* até a discriminação algorítmica, convidam a si a atenção de todo o corpo social para que se busquem avanços no entendimento da matéria e nos entraves para sua garantia. A expansão das formas de exploração de dados e os riscos emergentes demonstram a necessidade de englobar parâmetros de legitimidade mais amplos que a forma de consentimento atualmente adotada⁷⁵.

A constatação da limitação cognitiva do ser humano, explorada anteriormente, é o ponto de partida para instrumentalizar o consentimento e entender novas hipóteses para a materialização do direito à proteção de dados dentro da sociedade de informação e vigilância.

O ideal de autogerenciamento por parte dos usuários nas plataformas digitais requer maiores transformações na forma como estão dispostas as relações informacionais, sendo necessário revolucionar também o âmbito cultural.

A luta pela ampliação do conhecimento da população a respeito dos seus direitos básicos agora tem mais um objeto, devendo a proteção de dados ser incluída em campanhas de

⁷⁵ MENDES, Laura Schertel.; FONSECA, Gabriel Soares da. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: tendências contemporâneas de materialização. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, v. 6, n. 2, 2020, p. 510. Disponível em: <<https://www.estudosinstitucionais.com/REI/article/view/521>>. Acesso em: 14 Ago. 2023.

conscientização e demais esforços que tragam os riscos e benefícios das dinâmicas de controle de dados no cotidiano.

A inclusão dessa matéria na consciência humana deve ser feita desde a educação básica, facilitando um processo de formação que crie indivíduos inseridos no fluxo informacional cientes de seus desdobramentos, e não alvos propícios para as dinâmicas exploratórias da indústria da informação. Inserir esse debate desde a infância resulta em adultos mais preparados para controlar seus dados, munidos de um repertório básico que os auxilie na proteção de seus direitos.

Importante notar, todavia, que o papel a ser desempenhado de maneira individual por cada cidadão no gerenciamento de seus dados deverá ser acessório, estando prontamente aliado à uma rede de apoio composta por todo o aparato normativo, tecnológico, cultural e institucional que some no seu processo de capacitação e concretize seu ideal de autonomia. A diminuição dessa carga participativa do indivíduo dá fôlego ao consentimento, permitindo sua atuação nos cenários em que ele não é a base legal adequada para o tratamento de dados pessoais.

Para tanto, medidas adicionais podem ser imaginadas. O marketing direcionado deverá se pautar em novas estratégias publicitárias que não se aproveitem da identificação de informações pessoais para atingir seu público-alvo, obtendo resultados satisfatórios em suas ações por meio de estratégias efetivas incorporadas no meio digital.

Dada a presença em massa de consumidores na internet, de crianças a idosos, basta a produção de conteúdo de qualidade, pontual em sua abordagem e linguagem e destinado ao público certo, para influenciar de forma natural a compra de um serviço ou produto. Não são necessários a filtragem e manipulação de dados feitos pelo marketing invasivo e a corrida para chegar ao consumidor final, sendo possível deixar que este chegue até a propaganda sem interferência do mercado.

A tomada de postura crítica em relação aos abusos cometidos pelos agentes de tratamento de dados também enriquece a racionalidade coletiva para a tomada de decisão em respeito a suas informações. Momentos de ruptura com o status quo de complacência em relação às atividades desarrazoadas e inadequadas devem se tornar cada vez mais comuns, afastando a falácia de que os titulares não se importam com a forma que seus dados são coletados, tratados e disseminados.

Caso emblemático nesse sentido é o das políticas de privacidade do Facebook em 2014⁷⁶ associadas ao lançamento do aplicativo afiliado Messenger, que forçou os usuários da rede social a assinarem um novo termo de uso para que pudessem continuar utilizando a ferramenta de mensagem da empresa, que até então era integrada ao aplicativo “Facebook” para celulares e aparelhos móveis.

Nessa nova política de privacidade, havia uma completa alteração da dinâmica do fluxo informacional dos usuários, que para seguir mantendo contato por mensagem com familiares, colegas e amigos deveriam agora aceitar que o aplicativo gravasse áudios e vídeos, lesse e editasse mensagens, fizesse ligações e tirasse fotos, tudo sem que houvesse novas tomadas de consentimento. A reação pública foi extremamente negativa, algo raramente visto, e influenciou na reforma de termos de uso abusivos produzidos pela empresa na época.

As mudanças nos termos de adesão e políticas de privacidade, por si só, não necessariamente implicam que essas ferramentas funcionem de forma íntegra. As práticas de coleta do elemento volitivo do usuário não mudaram, e a dinâmica sempre presente do *trade-off* condicionou os titulares de dados a continuar atribuindo consentimento até mesmo em situações em que a coleta de dados é opcional, dado o quadro recorrente no passado onde recusar uma política de privacidade implicava em abdicar de um bem ou serviço ofertado durante a navegação.

Tais reflexões trazem à tona, novamente, uma perspectiva crítica da autodeterminação informacional como algo única e exclusivamente centrado no consentimento. Tal paradigma normativo não deve ser absoluto, mas, complementado por outros relatos e políticas que lhe imponham restrições e materializem seus objetivos. Ao tratar dessa problemática, Julie Cohen⁷⁷ afirma que é preciso construir zonas de autonomia, pautadas em parâmetros que contribuam ao valor social que se atribui à proteção de dados.

Helen Nissenbaum⁷⁸ apresenta o entendimento de que os agentes da economia não só utilizam o consentimento individual como um conceito construído visando atribuir legitimidade

⁷⁶ CHOWDHRY, See Amit. **Why Facebook forced users to download a separate messenger app**. Nov. 2014. Disponível em: <<http://www.forbes.com/sites/amitchowdhry/2014/11/11/why-facebook-forcedusers-to-download-a-separate-messenger-app/>>. Acesso em: 20 Jul. 2023.

⁷⁷ COHEN, Julia. Examined Lives: Informational Privacy and the Subject as Object. **Stanford Law Review**, v. 52, 2000.

⁷⁸ NISSENBAUM, Helen. **Privacy in Context: technology, policy, and the integrity of social life**. Stanford: Stanford University Press, 2010.

para a atuação no controle e manipulação de dados, como também não se atentam ao que conceitua como integridade contextual.

Essa integridade consiste num vetor de garantia de que o fluxo de tratamento de dados seja apropriado, atendendo a função e o valor social para que se destinam e se guiando por valores políticos e morais que constituem sua adequação.

O processo de racionalizar a atividade de tratamento de dados como (in)apropriada é feito levando em consideração o contexto de cada relação que decorre do uso dos dados de alguém, seja pela forma procedimental usualmente utilizada por determinado setor da indústria ou pelas características de cada caso concreto quando expostas de forma individual. A partir do uso de uma linguagem aplicada nesse quadro, se faz possível compreender o nível de integridade do tráfego dessas informações.

Utilizando a visão da autora, é possível compreender um outro caminho normativo a ser tomado, em que o consentimento não é o passo inicial na dinâmica de proteção de dados. A redação e aplicação de normas informacionais⁷⁹, guiadas pela somatória do contexto da coleta de dados e da integridade do seu tratamento, regulam o trânsito de dados e controlam o fluxo informacional antes mesmo que o elemento volitivo do titular de dados seja requerido pelos agentes de tratamento.

O contexto de aplicação do fluxo informacional compreende a identificação dos atores envolvidos e a investigação a respeito do vínculo existente entre cada um deles, o tipo de dado pessoal coletado e a forma como ele é disseminado e controlado pelos agentes. Em relação ao posicionamento desses elementos dentro do fluxo informacional, Bioni⁸⁰ propõe uma subdivisão de fluxo interno e fluxo externo.

O fluxo interno compreende os atores e os tipos de dados pessoais, identificando quem coleta as informações e de que natureza estas devem ser para que atuem e façam sentido dentro de cada contexto social. É o exemplo dos dados condizentes à saúde física e mental de um paciente, inerentes à relação destes com médicos e psicólogos, ou os desdobramentos de um fato jurídico na relação entre um advogado e seu cliente. Cada agente deverá aglutinar os dados que forem de sua competência, não sendo razoável, seguindo essas hipóteses, que um advogado

⁷⁹ NISSENBAUM, Helen. A Contextual Approach to Privacy Online. **Daedalus, the Journal of the American Academy of Arts & Sciences**, v. 140, 2011, p. 27.

⁸⁰ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Gen, Editora Forense, 2020, p. 241.

obtenha laudos médicos do seu cliente fora do contexto de sua atuação profissional, caracterizando uma desvirtuação do fluxo informacional e o tornando inapropriado.

O fluxo externo compreende a disseminação dos dados, considerando o que pode ser transmitido e para quem, sem que haja prejuízo à integridade do fluxo. O cidadão pode ter uma expectativa da sua privacidade e do tratamento de seus dados a partir da linguagem informacional aqui utilizada. Seguindo os exemplos anteriores, pode-se considerar razoável que o advogado dissemine os dados de um processo para a equipe do escritório que trabalha no caso, ou que um médico compartilhe o diagnóstico de um paciente com o restante de sua equipe clínica ou hospitalar.

No tocante ao que pode ser esperado pelos titulares no tratamento de seus dados e o que compõe essa racionalização, leciona Mendes⁸¹:

Essas “legítimas expectativas” passam a ser avaliadas a partir de elementos como: (i) o contexto em que a suposta violação ocorreu (qual era o ambiente social que estruturava o fluxo de informações analisado?); (ii) os atores envolvidos (quem eram os emissores, receptores e sujeitos do fluxo de informação?); (iii) os atributos da informação analisada (que tipo de informação se estava lidando? Informações médicas, bancárias, preferências pessoais?); (iv) os princípios de transmissão aplicáveis (quais eram os constrangimentos aplicáveis ao fluxo de informações analisado, ele estava condicionado à confidencialidade, reciprocidade, necessidade?)

Os desdobramentos do fluxo das informações são determinantes para a atuação de cada agente e para a concretização de suas funções, não devendo ultrapassar os limites impostos pelo processo de contextualização e agindo em conformidade com as demandas de integridade.

Portanto, a soma do conjunto de informações necessárias para a construção de uma análise contextual é o instrumento hábil para verificar a integridade do fluxo informacional, observando na realidade fática a valoração social atribuída à proteção de determinados dados e os limites de negociação do direito de protegê-los.

O processo de equilibrar a assimetria presente no mercado informacional implica no desenvolvimento de novas ferramentas e políticas de atuação, considerando a contradição presente na garantia artificial aplicada através de uma estratégia regulatória centrada na autodeterminação informacional.

⁸¹ MENDES, Laura Schertel.; FONSECA, Gabriel Soares da. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: tendências contemporâneas de materialização. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, v. 6, n. 2, 2020, p. 514. Disponível em: <<https://www.estudosinstitucionais.com/REI/article/view/521>>. Acesso em: 14 Ago. 2023.

O desafio de propiciar aos cidadãos, usuários, consumidores e titulares de dados maior controle sobre suas informações demonstra que o caminho a ser trilhado requer uma maior intervenção, seja na reavaliação da estratégia normativa, na arquitetura dos sistemas ou na rede de medidas paliativas adicionais que podem ser tomadas para integrar a tomada de decisão e a tutela da proteção de dados pessoais⁸².

3.2 Instrumentalização da tecnologia e reavaliação da engenharia das redes e sistemas

A expansão do uso das novas tecnologias é uma das formas de complementar o papel de protagonismo atribuído ao consentimento do titular de dados, e reforça o ideal de que o Direito não é a única força capaz de regular a internet e as relações informacionais. O desenvolvimento de modelos e estruturas favoráveis à privacidade e tutela da proteção de dados, em junção ao aparato jurídico, estabelecem melhores condições para a concretização do ideal de um titular de dados pessoais mais autônomo.

Não se trata de um abandono do consentimento como instrumento protetivo, mas sim de uma forma de enfrentar o déficit evidenciado pela multiplicidade de situações em que o consentimento se mostra insuficiente no processo de garantia da autonomia decisória dos indivíduos⁸³.

Ao passo que a evolução e a inovação do mercado solicitam uma regulamentação efetiva, viabilizando a atuação dentro da legalidade e sem prejuízos para os indivíduos, não se pode adotar uma posição paternalista à respeito desses impasses, não sendo viável uma diminuição da liberdade dos titulares de dados que acabaria estagnando o progresso no âmbito digital e a evolução social decorrente deste⁸⁴.

A atribuição da tecnologia no desenvolvimento de sistemas seguros consiste na proteção de dados atuando além do âmbito normativo ou contratual, inserindo os titulares de dados em ambientes que já foram criados com seus direitos em mente. As máximas da autodeterminação

⁸² NISSENBAUM, Helen. **Privacy as contextual integrity**. Washington Law Review, v. 79, 2004, p. 119.

⁸³ MENDES, Laura Schertel.; FONSECA, Gabriel Soares da. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: tendências contemporâneas de materialização. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, v. 6, n. 2, 2020, p. 519. Disponível em: <<https://www.estudosinstitucionais.com/REI/article/view/521>>. Acesso em: 14 Ago. 2023.

⁸⁴ *Idem, ibidem*.

informacional são inseridas na engenharia virtual, e trazem consigo efeitos exponenciais na dinâmica de empoderamento dos usuários.

Nesse diapasão, se positiva na LGPD os princípios da prevenção e da segurança, nos incisos VII e VIII do Art. 6º⁸⁵, responsáveis, respectivamente, por prevenir que danos sejam causados aos titulares devido ao tratamento de seus dados e por obter a confiança dos indivíduos através do bom uso dos sistemas para defesa de seus interesses frente aos agentes de controle.

As PETs (*privacy enhancing technologies*) também atuam nesse panorama tecnológico, e seu desenvolvimento resulta na instrumentalização que facilita e reforça a proteção de dados. Conforme anota Calo, são inovações promissoras, com muito a acrescentar nos esforços de somar ao consentimento na efetivação da tutela dessa proteção⁸⁶.

Destas, atribui-se destaque para o *Do Not Track/DNT*, que impede que a navegação do usuário seja rastreada, atuando de forma extensiva em todos os domínios em que o indivíduo acessar no ambiente virtual. Basta um clique para configurar essa escolha de não ceder dados ao fluxo, afastando as intermináveis janelas de *cookies* que surgem rotineiramente no tráfego da internet.

O controle exercido pelo titular seria extremamente simplificado, sendo possível afastar a incidência dos rastreadores de dados mesmo que o indivíduo não possua habilidades técnicas expansivas para manipular o cachê e os rastros que permeiam a navegação.

Todavia, a implementação do DNT encontrou empecilhos na forma como seria feita, não havendo consenso em relação ao agente responsável por seu desenvolvimento e programação. O World Wide Web Consortium, organização de padronização da internet que naturalmente compreendeu sua responsabilidade para tal, não chegou a um consenso junto aos agentes da indústria da publicidade comportamental, que puxaram para si a tarefa por entenderem que seriam os únicos capazes de garantir que as empresas atenderiam o protocolo, dada sua ligação direta com o setor⁸⁷.

Esse conflito de forças e interesses causou o enfraquecimento do movimento do DNT, que foi ainda mais prejudicado devido ao lobby da indústria da publicidade quando alguns

⁸⁵ Art. 6º (...) VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

⁸⁶ CALO, Ryan. Against notice skepticism in privacy (and elsewhere). **Notre Dame Law Review**, v. 87, 2012.

⁸⁷ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Gen, Editora Forense, 2020, p. 193.

navegadores anunciaram que iriam adotar esse modelo de não rastreamento de forma nativa em suas aplicações. A narrativa apresentada pelo mercado era de que a indústria da publicidade comportamental estaria fadada à morte.

O DNT restou como uma opção em alguns navegadores, não sendo capaz de vincular a atuação dos agentes e, a partir daí, impedir o rastreamento dos dados. A integração de toda a internet na universalidade do consentimento foi minada ao passo que a própria indústria que decide se cumpre ou não esse direcionamento. É mais um exemplo da falha de autorregulação do mercado informacional, evidenciando a necessidade de uma interferência regulatória que torne essa PET plenamente executável.

Além desse controle de dados no momento de coleta, a tecnologia pode empoderar o indivíduo nos demais momentos e nuances das relações informacionais. O uso e compartilhamento de dados pode ser feito pelo próprio titular através da iniciativa chamada de P3P/*Platform for privacy Preferences*⁸⁸, que permitiria a escolha de quais dados podem ser coletados, quais dados podem ser compartilhados, e a extensão desse compartilhamento.

A execução da P3P também encontrou obstruções fáticas, dada a dificuldade de padronização das políticas de privacidade que permitissem uma leitura dos dados que o consumidor escolheu compartilhar para que pudesse ter publicidade direcionada para si de acordo com seus interesses.

Essa PET seria uma das ferramentas para tornar o fluxo informacional mais fluído, ao passo que o ideal de “tudo ou nada” do *trade-off* nas políticas de privacidade abriria espaço para o que se entende como consentimento granular, baseado nas preferências de privacidade de cada pessoa. É um processo de empoderamento que devolve ao indivíduo a capacidade de barganhar, exercendo uma autonomia genuína em relação a suas informações pessoais⁸⁹.

O modelo contratualizado que surgiu diante da autorregulação do mercado poderia abrir espaço à autodeterminação informacional, universalizando o processo de tomada de decisão por toda a rede da internet e ajudando a superar a dinâmica de limitação cognitiva dos titulares.

Não mais existiria a exposição massiva aos termos de uso e privacidade arquitetados por um mercado que compreende essa limitação e a indisposição dos indivíduos em ler os extensos contratos de adesão criados para adquirir volição sem muita racionalização no processo.

⁸⁸ LESSIG, Lawrence. **Code and other laws of cyberspace**. Nova Iorque: Basic Books, 2006, p. 226.

⁸⁹ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Gen, Editora Forense, 2020, p. 195.

A criptografia vem sendo uma das tecnologias mais difundidas, sendo o modelo de “criptografia de ponta a ponta” usado de forma ampla em aplicativos utilizados por bilhões de pessoas mundialmente, como é o caso do WhatsApp. Através dessa PET, mensagens de texto, voz, imagem e vídeo são cifrados, e somente os participantes de comunicação, que aqui representam as duas pontas, têm a prerrogativa de decifrá-las⁹⁰.

Para além das iniciativas que seriam ideais, mas ainda não são executáveis, e as mais amplamente divulgadas e que já fazem parte do imaginário dos usuários das redes, existem esforços sendo feitos a todo momento para a ampliação das PETs, com projetos guiados e desenvolvidos por diversas organizações, empresas e agentes.

É o caso do Google, que divulgou em 2022 sua *toolkit* “*Protected Computing*” (Computação Protegida)⁹¹, criada com o intuito de transformar “como, quando e onde dados são processados para garantir de forma técnica sua privacidade e segurança”.

Em dezembro do mesmo ano, a empresa anunciou duas PETs do projeto, chamadas de *Magritte* e *Fully Homomorphic Encryption (FHE)*. A primeira é uma ferramenta de *blur* criada para detectar objetos que aparecem na tela e aplicar uma obstrução visual automaticamente, facilitando o processo de esconder placas de carros, rostos de pessoas, tatuagens e outras incidências de interesse de quem faça uso da aplicação. A segunda permite que programadores façam o processamento de dados encriptados sem que tenham contato com informações pessoalmente identificáveis, facilitando o trabalho das indústrias para que atuem diante de sistemas de segurança rígidos e robustos.

Estímulos governamentais para o desenvolvimento dessas tecnologias já vêm sendo aplicados, como a criação de competições feitas pelos governos dos Estados Unidos e do Reino Unido para criar PETs baseadas no controle de crimes financeiros e de emergências de saúde pública, sendo necessária a adoção e expansão desse tipo de política pública por mais Estados ao redor do planeta⁹².

⁹⁰ ABREU, Jacqueline de Souza. **Passado, presente e futuro da criptografia forte**: desenvolvimento tecnológico e regulação. Revista Brasileira de Políticas Públicas, Brasília, v. 7, n. 3, 2017.

⁹¹ GOOGLE. **How We Make Everyday Safer With Google**. 11. Maio 2022. Disponível em: <<https://blog.google/technology/safety-security/how-we-make-every-day-safer-with-google/>>. Acesso em: 20 Ago. 2023.

⁹² NIST. **Winners Announced in First Phase of UK-US Privacy-Enhancing Technologies Prize Challenges**. 10. Nov. 2022. Disponível em: <<https://www.nist.gov/news-events/news/2022/11/winners-announced-first-phase-uk-us-privacy-enhancing-technologies-prize>>. Acesso em: 20 Ago. 2023.

Interessante atentar, ainda, para o fato de que o código base dessas PETs é aberto⁹³, sendo divulgado em bases de programação como o GitHub para que programadores de todo o planeta possam contribuir com esses projetos, aprender a respeito do processo de desenvolvimento, e futuramente criar suas próprias inovações na área.

A ampliação dessas tecnologias implica na concretização do conceito de autodeterminação informativa por meio do próprio sistema que gere o fluxo informacional, e essas iniciativas cada vez mais se tornam convencionais, sendo inseridas e integradas na sociedade, podendo então guiar e regular a internet.

3.3 Diretrizes para a expansão normativa da proteção de dados

Somados aos esforços e caminhos já apresentados, a presença da discussão legal e do conhecimento jurídico no processo de materialização do direito à proteção de dados é primordial. Considerando o ecossistema em tela, um possível novo relato normativo deverá levar em consideração o preceito de norma informacional desenvolvido por Nissenbaum e exposto anteriormente, retirando da esfera pessoal do indivíduo a carga de proteção dos dados pessoais.

É possível verificar no ordenamento jurídico brasileiro uma organização de elementos que integram a órbita do consentimento, caracterizando um “núcleo duro”⁹⁴ já imposto em leis setoriais de proteção de dados. É o caso do sigilo e a inviolabilidade das comunicações privadas, bem como da proibição da manutenção de logs de dados pelos provedores de internet, todos previstos no Marco Civil da Internet, e da restrição do uso de dados pessoais para avaliação e concessão de crédito, abordada na Lei do Cadastro Positivo e na jurisprudência do Superior Tribunal de Justiça. São comandos que limitam o consentimento do titular ao passo que comandam e governam o tratamento de dados.

Se faz presente também a necessidade de combater a discriminação e a estigmatização causadas pelas decisões automatizadas pautadas nos dados coletados, que prejudicam e precarizam o livre desenvolvimento da personalidade a partir do descumprimento do princípio

⁹³ ENGADGET. **Google is making its internal video-blurring privacy tool open source**. 22. Dez. 2022. Disponível em: <<https://www.engadget.com/google-is-making-its-internal-video-blurring-privacy-tool-open-source-150052840.html>>. Acesso em: 20 Ago. 2023.

⁹⁴ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Gen, Editora Forense, 2020, p. 251.

da finalidade, resultando no contato indevido de setores da indústria com dados sensíveis que não devem ser realocados dentro do fluxo informacional.

A acomodação da LGPD no sistema jurídico nacional é dificultada pelo alto grau de impacto de uma inovação normativa dessa magnitude dentro de um ordenamento, visto que todas as camadas da sociedade civil são transformadas em grau elevado. Ao passo que o tecido social é extremamente movido pela economia de dados, leis como essa basicamente configuram um novo “contrato social”, regulando a vida em sociedade de maneira extensiva.

A interpretação hermenêutica para esse caso deve ser baseada no diálogo das fontes, permitindo que as normas se complementem e atribuam sentido umas às outras. Afastada uma interpretação de hierarquia de normas entre a LGPD e outras normas integrantes do sistema, não há hipótese de revogação, mas sim da presença de um processo lógico de coordenação⁹⁵. Nesse diapasão incorre o próprio legislador, que utilizou de uma linguagem semelhante à adotada no CDC para posicionar o diálogo entre as normas dentro do ordenamento⁹⁶.

Ademais, há uma tendência de incorporação do ideal de risco e responsabilização na legislação da matéria, que compreende a responsabilidade pela proteção de dados como algo a ser compartilhado entre todos os atores envolvidos⁹⁷. É adotada uma análise prévia dos riscos oferecidos pelo tratamento de dados, que permita a adoção de medidas de segurança apropriadas e compatíveis com os impactos ou danos razoavelmente esperados na esfera do bem jurídico tutelado.

Consoante Gellert⁹⁸:

A proteção de dados pode ser conceituada como um conjunto de regras legais e instrumentos projetados para proteger os direitos, liberdades e interesses de indivíduos cujos dados pessoais são armazenados, processados e divulgados por computadores. Por sua vez, a abordagem baseada em risco refere-se a uma tendência que surgiu desde o final dos anos 2000 e o início dos anos 2010, e que consiste em incorporar ferramentas de gerenciamento de risco nos quadros legais de proteção de dados, a fim de ter melhores chances de alcançar - ou assim se argumenta - a proteção dos dados pessoais dos cidadãos. (...) O objetivo dessas salvaguardas é garantir a proteção eficaz

⁹⁵ MARQUES, Cláudia Lima. **O “diálogo das fontes” como método da nova teoria geral do direito**: um tributo a Erik Jayme. In: MARQUES, Cláudia Lima (coord.). *Diálogo das Fontes*. São Paulo: Revista dos Tribunais, 2012.

⁹⁶ Art. 64. “Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria [...]”.

⁹⁷ BENNETT, Colin; RAAB, Charles. **Revisiting “The Governance of Privacy”**: Contemporary Policy Instruments in Global Perspective. 2018. Disponível em: <<https://ssrn.com/abstract=2972086>>. Acesso em: 20 Ago. 2023.

⁹⁸ GELLERT, Raphael. **The Risk-Based Approach to Data Protection**. Nova Iorque: Oxford University Press, 2020.

dos dados retidos contra o risco de abuso e contra qualquer acesso e uso ilegais desses dados⁹⁹.

Essa mentalidade regulatória estimula a atuação dos agentes e o desenvolvimento de condições institucionais que garantam os direitos previstos, adotando medidas de segurança de forma preventiva. Os próprios agentes se inserem numa estratégia de combate e de mitigação dos riscos gerados no desenvolvimento de suas atividades, o fazendo com o maior grau de transparência possível nessa condução¹⁰⁰. Nas lições de Aranha, se trata de um modelo híbrido e multifocal, em que os diversos atores compartilham da responsabilidade de elaborar e cumprir os parâmetros de proteção de dados.

A multiplicidade de agentes constitui um ideal de regulação por redes nodulares, onde há constante interação entre reguladores e regulados e entre os próprios reguladores, o que se diferencia de uma abordagem pautada na concentração regulatória estatal.

Como expõe Camara:

Na malha, não existe um único agente regulador, mas uma multiplicidade de fontes regulatórias que interagem entre si e gozam de autonomia mitigada. Nessa forma de regular, podem ser citadas, exemplificativamente, como fontes de regulação, ou unidades fiscalizatórias de atividades regulatórias, a) o próprio agente econômico, em autorregulação em sistemas de controles internos; b) entes associativos que representam a autorregulação voluntária; c) entes privados incumbidos da autorregulação regulada; d) organizações não governamentais; e) órgãos e entidades da administração pública que exercem a regulação estatal e; f) entes reguladores privados que exercem função pública por delegação estatal¹⁰¹.

Para atuar nesse modelo, é conferida maior liberdade aos agentes, e em contrapartida estes devem reportar falhas e riscos às autoridades, além de prestar contas de forma clara, precisa, e facilmente acessível aos titulares de dados pelos desdobramentos do tratamento efetuado.

⁹⁹ Tradução livre de “Data protection can be defined as a set of legal rules and instruments designed to protect the rights, freedoms, and interests of individuals whose personal data are stored, processed and disseminated by computers. In turn, the risk-based approach refers to a trend that has emerged since the late 2000s/early 2010s, and which consists in enshrining risk management tools in data protection legal frameworks, in order to have better chances of achieving - or so it is contended - the protection of citizens' personal data. [...] The goal of these safeguards is to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data”.

¹⁰⁰ ARANHA, Marcio Iorio; LOPES, Othon. **Estudo sobre Teorias Jurídicas da Regulação apoiadas em incentivos**. Pesquisa e Inovação Acadêmica sobre Regulação apoiada em Incentivos na Fiscalização Regulatória de Telecomunicações, Brasília: Anatel/UNB, 2019.

¹⁰¹ CAMARA, Rafael Rodrigues. Da Regulação em Rede Ingênuo à Sofisticada: riscos e oportunidades no exercício privado de funções regulatórias. **Revista de Direito Setorial e Regulatório**, Brasília, v. 8, nº 1, 2022, p. 8. Disponível em: <<https://periodicos.unb.br/index.php/rdsr/article/view/37932/33264>>. Acesso em: 20 Ago. 2023.

A combinação das abordagens preventivas e procedimentais com as considerações feitas pelo saber jurídico é possível e deve ser encorajada. A aliança da tecnologia e do Direito possibilitam a extensão dos ideais de autonomia e de empoderamento para que o titular de dados exerça sua vontade de forma livre.

Nesse escopo, a utilização de outros objetos e normas presentes no sistema jurídico brasileiro pode ser feita, inserida na rede de esforços para atingir a materialização do ideal de autodeterminação mais robusto. É o exemplo da utilização de institutos civis consagrados, como os que tratam de vício de vontade e abusos de poder, ou cláusulas gerais como a boa-fé ou a tutela de confiança¹⁰².

A intenção é adequar o consentimento à finalidade atribuída ao tratamento que será realizado, utilizando de limites materiais para revitalizar o consentimento, e não para obstruí-lo. É uma medida de extrema importância para a efetivação da proteção de dados contemporânea, pois permite uma análise desse elemento volitivo atenta à realidade e capaz de acompanhar as novidades no escopo fático e tecnológico que se apresentam rotineiramente.

¹⁰² MENDES, Laura Schertel.; FONSECA, Gabriel Soares da. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: tendências contemporâneas de materialização. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, v. 6, n. 2, 2020, p. 524. Disponível em: <<https://www.estudosinstitucionais.com/REI/article/view/521>>. Acesso em: 14 Ago. 2023.

5. CONCLUSÃO

O presente trabalho propôs um debate acerca da esfera de proteção de dados pessoais, partindo da análise dos dados pessoais como um novo direito da personalidade e um novo ativo na economia, tratando da recepção da matéria pelo ordenamento jurídico brasileiro.

O desenvolvimento da sociedade da informação e vigilância, impulsionado pelo advento da internet, originou relações humanas digitais que desafiam a forma tradicional de regulamentação jurídica e a aplicação do aparato jurídico, convidando o Direito a se reinventar de modo a atender os novos modelos de fato jurídico presentes em relações que não mais possuem limites territoriais.

Assim, a discussão se concentrou na problemática em cima dos limites do consentimento enquanto protagonista normativo da proteção dos dados dos titulares, implicando na ponderação do que pode vir a ser uma visão mais alargada da autodeterminação informacional, um dos fundamentos da LGPD, que vem sendo contratualizada pelas políticas de privacidade e termos de uso massificados.

A estratégia regulatória adotada encontra diversos obstáculos para sua materialização, considerando a racionalidade limitada dos titulares de dados e o paradoxo presente entre o comportamento adotado na tentativa de controle e proteção de seus dados e a valoração atribuída a esse direito, já que apesar do cidadão compreender o peso significativo da garantia dos seus direitos, muitas vezes toma atitudes que os atinge diretamente.

No estágio atual, em que o desenvolvimento legislativo ainda é recente e a jurisprudência em torno da matéria ainda está em construção, a regulamentação deve propor o emprego de novas estratégias, considerando o reaproveitamento da arquitetura tecnológica que estrutura as redes e serve de base para a economia da informação. A tecnologia pode ser uma ferramenta de empoderamento e capacitação do titular de dados, reparando falhas na estrutura do arranjo normativo e atribuindo bases fáticas de efetivação da autodeterminação informativa na realidade.

Deve-se buscar formas de se atingir um denominador comum entre o desenvolvimento econômico na sociedade da informação e a tutela da proteção de dados pessoais, assegurando que o papel da autonomia da vontade se estenda somente o necessário para garantir um fluxo informacional apropriado quando considerado devidamente presente e implementado um rol de medidas de regulação acessórias.

Como visto, portanto, a mera disposição do consentimento do titular de dados no processo de tomada de decisão, por si só, não é suficiente para viabilizar a garantia e a tutela do direito à proteção de dados, sendo necessário trabalhar hipóteses de intervenção normativa, tecnológica e cultural que suavizam o papel a ser desempenhado pelos cidadãos (hiper)vulneráveis dentro da economia de dados.

Através da identificação de caminhos possíveis para o trato da matéria, considerando sua novidade e complexidade, o presente trabalho reconhece a distância a ser percorrida para esgotar o tema. Analisando o quadro regulatório e as disposições normativas já incorporadas no ordenamento jurídico, se ponderou formas de diminuir a assimetria na relação de poder entre titulares e controladores de dados, buscando produzir a eficácia social idealizada pelo legislador quando regulou e positivou o consentimento como protagonista da proteção de dados pessoais.

REFERÊNCIAS

ARANHA, Marcio Iorio; LOPES, Othon. **Estudo sobre Teorias Jurídicas da Regulação apoiadas em incentivos**. Pesquisa e Inovação Acadêmica sobre Regulação apoiada em Incentivos na Fiscalização Regulatória de Telecomunicações, Brasília: Anatel/UNB, 2019.

BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run Around Consent and Anonymity. *Em*: LANE, Julia et al. **Privacy, Big Data and the Public Good**. Cambridge: Cambridge University Press, 2014, p. 59.

BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida**. 1. ed., Rio de Janeiro: Zahar, 2014, p. 10.

BENNETT, Colin; RAAB, Charles. **Revisiting “The Governance of Privacy”**: Contemporary Policy Instruments in Global Perspective. Ago. 2018. Disponível em: <<https://ssrn.com/abstract=2972086>>. Acesso em: 20 Ago. 2023.

BIONI, Bruno Ricardo. **Brasil precisa ser competitivo em uma economia de dados**. *Jornal Valor Econômico*, jul. 2018. Disponível em: <<https://www.valor.com.br/opiniaio/5669703/paisprecisa-ser-competitivo-em-uma-economia-de-dados>>. Acesso em: 14 Maio 2023.

BIONI, Bruno Ricardo. **Por que proteção de dados importa?** TEDxPinheiros, 2018. Disponível em <<https://www.youtube.com/watch?v=TzI5VfvQA6I>>. Acesso em 28 Jul. 2023.

BIONI, Bruno Ricardo; MENDES, Laura Schertel. Regulamento europeu de proteção de dados pessoais e a lei geral brasileira de proteção de dados: mapeando convergências na direção de um nível de equivalência. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato (Coord.). **Lei geral de proteção de dados e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 550.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Gen, Editora Forense, 2020.

BIONI, Bruno Ricardo; LUCIANO, Maria. **O Consentimento como Processo: Em Busca do Consentimento Válido**. In: *Tratado de Proteção de Dados Pessoais*. BIONI, Bruno (Org.). Rio de Janeiro: Forense, 2021.

BLUME, Peter. **The inherent contradictions in data protection law**. *International Data Privacy Law*, 2. ed, n. 1, p. 27.

BONNA, Alexandre Pereira; CAÑIZO, Amanda de Moura; CALZAVARA, Giovana Ferreira. **CONSENTIMENTO E LGPD: DESAFIOS DIANTE DA HIPERVULNERABILIDADE DO CONSUMIDOR**. *Revista de Direito e Atualidades*, v. 1, n. 3, 2021. Disponível em: <<https://www.portaldeperiodicos.idp.edu.br/rda/article/view/6231>>. Acesso em: 18 Maio 2023.

BRASIL. Supremo Tribunal Federal Tribunal Pleno. **Ação Direta de Inconstitucionalidade (ADI) nº 6387**. Relator: Rosa Weber. Acórdão. Julgado em: 12.11.2020, DJ 17.09.2020.

Disponível em:

<<https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>>. Acesso em 15 Maio 2023.

BRASIL. Constituição (1998). **Constituição da República Federativa do Brasil**:

promulgada em 5 de outubro de 1998. Disponível em:

<http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 20. Maio 2023.

BRASIL. Constituição (1988). **Emenda constitucional nº 115, de 10 de fevereiro de 2022**.

Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em:

<https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm>. Acesso em 20 Maio 2023.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112414.htm>. Acesso em: 12 Jul. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 15 Jul. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 24 de Jul. 2023.

BRASIL. **Lei nº 13.853, de 08 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm>. Acesso em: 24 Jul. 2023.

BROOKSHEAR, J. Glenn. **Ciência da Computação: Uma Visão Abrangente**. 11. ed. São Paulo: Bookman, 2013, p. 23.

CALO, Ryan. Against notice skepticism in privacy (and elsewhere). **Notre Dame Law Review**, v. 87, 2012.

CAMARA, Rafael Rodrigues. Da Regulação em Rede Ingênua à Sofisticada: riscos e oportunidades no exercício privado de funções regulatórias. **Revista de Direito Setorial e Regulatório**, Brasília, v. 8, nº 1, 2022, p. 8. Disponível em:

<<https://periodicos.unb.br/index.php/rdsr/article/view/37932/33264>>. Acesso em: 20 Ago. 2023

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 2008.

CHOWDHRY, See Amit. **Why Facebook forced users to download a separate messenger app**. Nov. 2014. Disponível em:

<<http://www.forbes.com/sites/amitchowdhry/2014/11/11/why-facebook-forcedusers-to-download-a-separate-messenger-app/>>. Acesso em: 20 Jul. 2023.

COHEN, Julia. Examined Lives: Informational Privacy and the Subject as Object. **Stanford Law Review**, v. 52, 2000.

COMPARATO, Fábio Konder. A proteção do consumidor na Constituição brasileira de 1988. *Em*: MARQUES, Claudia Lima; MIRAGEM, Bruno (Org). **Direito do consumidor: vulnerabilidade do consumidor e modelos de proteção**. São Paulo: Revista dos Tribunais, 2011. v. 2, p. 190.

COSTA JÚNIOR, Paulo José da. **O direito de estar só: tutela penal da intimidade**. São Paulo: Revista dos Tribunais, 2007. Acesso em: 10 jun. 2023

COSTA, Ramon; DE OLIVEIRA, Samuel. **OS DIREITOS DA PERSONALIDADE FRENTE À SOCIEDADE DE VIGILÂNCIA: PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E CONSENTIMENTO NAS REDES SOCIAIS**. 2020. Disponível em: <<https://www.indexlaw.org/index.php/direitocivil/article/view/5778>>. Acesso em: 21 Abr. 2023.

CRANOR, Lorrie Faith; MCDONALD, Aleecia. **Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising**, p. 1. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092>. Acesso em: 05 ago. 2023.

DONEDA, Danilo Cesar Maganhoto. **Da Privacidade à Proteção de Dados Pessoais: fundamentos da Lei Geral de Proteção de Dados**. 2ª Ed. São Paulo: Thomson Reuters Brasil, 2020.

EHRHARDT JÚNIOR, Marcos; PEIXOTO, Erick Lucena Campos. Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias. **Revista Jurídica Luso-brasileira – RJLB**, Lisboa, a. 6, n. 2, 2020. Disponível em: <https://www.cidp.pt/revistas/rjlb/2020/2/2020_02_0389_0418.pdf>. Acesso em: 25 jul. 2023.

ENGADGET. **Google is making its internal video-blurring privacy tool open source**. 22. Dez. 2022. Disponível em: <<https://www.engadget.com/google-is-making-its-internal-video-blurring-privacy-tool-open-source-150052840.html>>. Acesso em: 20 ago. 2023.

EVANS, David S. The Online Advertising Industry: Economics, Evolution, and Privacy. **Journal of Economic Perspectives**, v. 23, n. 3, p. 30, 2009. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1376607. Acesso em: 2 ago. 2023.

G1 MG. **Sites educacionais dos governos de MG e SP coletaram dados de estudantes para empresas de publicidade, diz Human Rights Watch**. Disponível em: <<https://g1.globo.com/mg/minas-gerais/noticia/2023/04/03/sites-educacionais-de-mg-e-sp-coletaram-e-enviaram-dados-de-estudantes-para-empresas-de-publicidade-diz-human-rights-watch.ghtml>>. Acesso em: 14 Maio 2023.

GELLERT, Raphael. **The Risk-Based Approach to Data Protection**. Nova Iorque: Oxford University Press, 2020.

GOMES, Orlando. **Contratos**. 26. ed., Rio de Janeiro: Forense, 2009, p. 159

GOOGLE. **How We Make Everyday Safer With Google**. 11. Maio 2022. Disponível em: <<https://blog.google/technology/safety-security/how-we-make-every-day-safer-with-google/>>. Acesso em: 20 ago. 2023.

HOLLAND, Brian. **Privacy Paradox 2.0**. 19 Widener L.J., 2010.. Disponível em: <<http://ssrn.com/abstract=1584443>>. Acesso em: 05 ago. 2023.

HOOFNAGLE, Chris Jay et. al. Behavioral Advertising : The Offer You Cannot Refuse. **Harvard Law & Policy Review**, v. 6, 2012, p. 276. Disponível em: <<https://ssrn.com/abstract=2137601>>. Acesso em: 08 Jul. 2023.

IBGE Notícias. **Internet já é acessível em 90% dos domicílios do país em 2021**. Disponível em: <<https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021>>. Acesso em: 10 Jul. 2023.

KARVALICS, László. **Information Society – what is it exactly?** (The meaning, history and conceptual framework of an expression). Budapeste, 2007, p. 11. Disponível em: <https://www.researchgate.net/publication/237332035_Information_Society_-_what_is_it_exactly_The_meaning_history_and_conceptual_framework_of_an_expression>. Acesso em: 15 Jul. 2023

KERR, Ian; BARRIGAR, Jennifer; BURKELL, Jacquelyn; BLACK, Katie. Soft surveillance, hard consent. *Em*: KERR, Ian et al. **Lessons from the identity trail : anonymity, privacy and identity in a networked society**. New York: Oxford University Press, 2009, p. 19.

KÖNIG, Kauana Christiano; MARCO, Aurelio Rodrigues da Cunha e Cruz; DOUGLAS, Marangon. **A LEI GERAL DE PROTEÇÃO DE DADOS E A DISCRIMINAÇÃO ALGORÍTMICA**. 2022. Disponível em: <<https://www.ufsm.br/app/uploads/sites/563/2022/11/1.7.pdf>>. Acesso em: 24 Abr. 2023.

LEITE, Carlos Henrique Bezerra. **Curso de direito do trabalho**. 11. ed. São Paulo: Saraiva Educação, 2019.

LESSIG, Lawrence. **Code and other laws of cyberspace**. Nova Iorque: Basic Books, 2006.

LIMA, Cíntia Rosa Pereira de. **Validade e obrigatoriedade dos contratos de adesão eletrônicos (shrinkwrap e click-wrap) e dos termos e condições de uso (browse-wrap)**. Tese (Doutorado) - Faculdade de Direito da Universidade de São Paulo, São Paulo, 2009, p.

656. Disponível em <https://teses.usp.br/teses/disponiveis/2/2131/tde-03062011-090910/publico/Tese_Final_TOTAL.pdf>. Acesso em: 10 ago. 2023.

LIU, Yong. Word of Mouth for Movies: Its Dynamics and Impact on Box Office Revenue. **Journal of Marketing**, v. 70, n. 3, 2006, p. 27. Disponível em: <<https://journals.sagepub.com/doi/10.1509/jmkg.70.3.074>>. Acesso em: 2 Jul. 2023.

MARQUES, Cláudia Lima. **O “diálogo das fontes” como método da nova teoria geral do direito**: um tributo a Erik Jayme. In: MARQUES, Cláudia Lima (coord.). *Diálogo das Fontes*. São Paulo: Revista dos Tribunais, 2012.

MCDONALD, Aleecia; CRANOR, Lorrie Faith. **The Cost of Reading Privacy Policies**. *Journal of Law and Policy for Information Society*, 2008, p. 19. Disponível em <<https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>>. Acesso em: 12 Ago. 2023.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel.; FONSECA, Gabriel Soares da. **PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: tendências contemporâneas de materialização**. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, v. 6, n. 2, 2020. Disponível em: <<https://www.estudosinstitucionais.com/REI/article/view/521>>. Acesso em: 14 Ago. 2023.

MIRAGEM, Bruno. **A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor**. *Revista dos Tribunais*, São Paulo, v. 1009, p. 1-35, nov. 2019. Disponível em: <<https://www.brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf>>. Acesso em: 20 Abr. 2023

MODESTO, Jéssica Andrade. **O direito à privacidade na sociedade da informação à luz da lei geral de proteção de dados pessoais: uma análise da (in)efetividade da lei nº 13.709/2018 no Brasil a partir do estudo comparativo com o regulamento geral de proteção de dados da União Europeia**. 2021. 364 f. Dissertação (Mestrado em Direito) - Universidade Federal de Alagoas, Alagoas, 2021.

MURRAY, Andrew. **Information, technology, law**. OUP Oxford, 2019, p. 40-41.

NISSENBAUM, Helen. **Privacy in Context: technology, policy, and the integrity of social life**. Stanford: Stanford University Press, 2010;

NISSENBAUM, Helen. A Contextual Approach to Privacy Online. **Daedalus, the Journal of the American Academy of Arts & Sciences**, v. 140, 2011, p. 27.

NISSENBAUM, Helen. **Privacy as contextual integrity**. *Washington Law Review*, v. 79, 2004, p. 119.

NIST. **Winners Announced in First Phase of UK-US Privacy-Enhancing Technologies Prize Challenges**. 10. Nov. 2022. Disponível em: <<https://www.nist.gov/news-events/news/2022/11/winners-announced-first-phase-uk-us-privacy-enhancing-technologies-prize>>. Acesso em: 20 ago. 2023.

ORWELL, George. **1984**. São Paulo: Principis, 2021.

RODOTÀ, Stefano. Trad. Maria Celina Bodin de Moraes. **A Vida na Sociedade da Vigilância: Privacidade Hoje**. 1 ed. Rio de Janeiro: Renovar, 2008.

COSTA, Rogério. **Por um novo conceito de comunidade**: redes sociais, comunidades pessoais, inteligência coletiva. *Interface - Comunic., Saúde, Educ.*, v.9, n.17, 2005, p. 239.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da lei geral de proteção de dados (LGPD) – Lei 13.709/2018. *Em*: BIONI, Bruno et al. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

SARLET, Ingo. **A EC 115/22 e a proteção de dados pessoais como Direito Fundamental**. *Revista Consultor Jurídico*, São Paulo, 11 de mar. de 2022. Disponível em: <https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental>. Acesso em: 24 Jun. 2023.

SILVA, Gabriela Buarque Pereira. **Responsabilidade civil, riscos e inovação tecnológica**: Os desafios impostos pela inteligência artificial. 2021. 141 f. Dissertação (Mestrado em Direito) - Universidade Federal de Alagoas, Alagoas, 2021.

TOFFLER, Alvin. **The third wave**. Bantam Books, 1986.

TRANDBURG, Katherine J. **Free Fall: The Online Market's Consumer Preference Disconnect**. NYU School of Law, Public Law Research Paper, 2013,, p. 52. Disponível em: <<https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1511>>. Acesso em: 10 ago. 2023.

TSCHENTSCHER, Peter; BROICHHAGEN, Seven. Urteil des Ersten Senats vom 15 Dezember 1983 auf die mündliche Verhandlung vom 18 und 19 oktober in den Verfahren über die Verfassungsbeschwerden. 1983. Disponível em: <http://www.servat.unibe.ch/dfr/bv065001.html>. Acesso em: 18 Jul. 2023

TUROW, Joseph; HENESSY, Michael; DRAPER, Nora. **The tradeoff fallacy: how marketers are misrepresenting and opening them up to exploitation**. Disponível em: <<https://dx.doi.org/10.2139/ssrn.2820060>>. Acesso em: 15 ago. 2023.

UNIÃO EUROPEIA. Comissão Europeia. **Special Eurobarometer 487a** - Report: The general data protection regulation. Jun. 2019, p. 6. Disponível em: <<https://cnpd.public.lu/content/dam/cnpd/fr/actualites/international/2019/ebs487a-GDPR-sum-en.pdf>>. Acesso em: 17 Ago. 2023.

UTZ, Christine et al. (Un)informed consent: studying GDPR consent notices in the field. *Em*: **2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)**, November 11–15, 2019, London, United Kingdom. ACM, New York, NY, USA. Disponível em: <<https://arxiv.org/pdf/1909.02638.pdf>>. Acesso em: 08 Ago. 2023.

VASCONCELOS, Karina de Souza. **HERANÇA DIGITAL NO DIREITO BRASILEIRO: A tutela jurídica dos bens digitais híbridos em plataformas digitais**. 2023. 164 f. Dissertação (Mestrado em Direito) - Universidade Federal de Alagoas, Alagoas, 2023.

ZANATTA, Rafael. A proteção de dados entre leis, códigos e programação: os limites do Marco Civil da Internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. **Direito & Internet III: Marco Civil da Internet**. São Paulo: Quartier Latin, 2015.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**. 1. ed. Rio de Janeiro: Intrínseca, 2021.

ZUBOFF, Shoshana. **Big Other: Surveillance Capitalism and the Prospects of an Information Civilization**. Journal of Information Technology, Boston, 2015. Disponível em: <<https://ssrn.com/abstract=2594754>>. Acesso em: 10 Maio 2023.