UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
DEPARTAMENTO DE DIREITO PRIVADO E PROCESSO CIVIL

CLAUDEMIR DO NASCIMENTO

DADOS IMPERCEPTÍVEIS E A INSUFICIÊNCIA DO TERMO DE CONSENTIMENTO PARA A PROTEÇÃO DE DADOS PESSOAIS

PORTO ALEGRE
2022

CLAUDEMIR DO NASCIMENTO

DADOS IMPERCEPTÍVEIS E A INSUFICIÊNCIA DO TERMO DE CONSENTIMENTO PARA A PROTEÇÃO DE DADOS PESSOAIS

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Ciências Jurídicas e Sociais da Faculdade de Direito da Universidade Federal do Rio Grande do Sul.

Orientador: Prof. Dr. Fabiano Menke

PORTO ALEGRE

2022

CLAUDEMIR DO NASCIMENTO

DADOS IMPERCEPTÍVEIS E A INSUFICÊNCIA DO TERMO DE CONSENTIMENTO PARA A PROTEÇÃO DE DADOS PESSOAIS

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Ciências Jurídicas e Sociais da Faculdade de Direito da Universidade Federal do Rio Grande do Sul.

Aprovado em 11 de maio de 2022.

BANCA EXAMINADORA:

_____
Professor Dr. Fabiano Menke - Orientador

_____
Professor Dr. Gerson Luiz Carlos Branco

_____
Professor Dr. Luis Renato Ferreira da Silva

AGRADECIMENTOS

Ao final deste trabalho, resta agradecer àqueles que, de alguma forma, contribuíram para tornar esta etapa da minha vida em realidade.

Primeiramente a Deus, por ter me dado todas as condições favoráveis, bem como a força e discernimento para superar todas as adversidades surgidas ao longo do caminho.

À minha querida mãe, Maria Catarina (*in memoriam*), por ter sido a pessoa mais inspiradora e guerreira com quem tive o privilégio de crescer, conviver e aprender. Onde quer que esteja, dedico a ti, não apenas este trabalho, mas tudo que sou hoje.

À Talita, pelo companheirismo, pelos debates, pelas viagens com o GDO e, principalmente, pelo apoio nos momentos mais importantes da minha vida pessoal e acadêmica.

Ao Grupo de Debate e Oratória – GDO, projeto de extensão que mudou a minha vida e me apresentou amigos que levarei para o resto da vida, entre os quais: Rached, Antonia, Fischer, Pedro Binda, e tantos outros. Ao GDO agradeço por todas as oportunidades que me foram concedidas: debater em diversos lugares do Brasil e Portugal (UFSC, USP, UFRN, UFMG, SDUL, SDUC, etc) e representar a UFRGS em dois campeonatos mundiais. Voa GDO!

Ao Desembargador Paulo Sérgio Scarparo e sua equipe, Candi, Camila, Laura, Renato e Thiago, por todas as oportunidades, conselhos e ensinamentos ao longo dos dois anos de estágio no TJ/RS.

Por fim, agradeço ao meu orientador, Professor Fabiano Menke, não apenas pela confiança depositada em mim ao aceitar a orientação, mas também pelos ensinamentos durante a graduação e por despertar o senso de pesquisador sobre a disciplina da proteção de dados nesse acadêmico.

"*A invasão injustificada da privacidade individual deve ser repreendida e, tanto quanto possível, prevenida.*"

The Right to Privacy – S. Warren e L. Brandeis

RESUMO

O presente trabalho tem como objetivo examinar o tratamento de dados pessoais na internet com enfoque no consentimento do titular dos dados, uma vez que esse é um dos requisitos para que o procedimento seja legítimo e lícito. Na primeira parte do trabalho será abordada a origem e o desenvolvimento da matéria sobre proteção de dados pessoais, trazendo a geração de leis sobre o tema e seus princípios norteadores. Ademais, nessa parte também será apresentado o contexto brasileiro quanto a regulamentação da proteção de dados. A segunda parte será dedicada ao estudo do tratamento dos dados pessoais na economia informacional, e de que forma a sua coleta e tratamento pode ser prejudicial para a privacidade do titular dos dados. Nesse sentido, serão apresentadas as problemáticas que tornam o consentimento como insuficiente para a proteção dos dados pessoais. Por fim, serão apresentadas duas alternativas que visam mitigar os problemas que tornam o consentimento ineficiente para a proteção de dados.

Palavras-Chaves: Dados Pessoais; Proteção de Dados; Termo de Consentimento; Tratamento de Dados Pessoais.

ABSTRACT

The present work aims to examine the processing of Personal Data on the internet with a focus on the consent of the data subject, since this is one the requirements for the procedure to be legitimate and lawful. In the first part of the work, the origin and development of the matter on Personal Data Protection will be addressed, bringing the generation of laws on the subject and its guiding principles. In addition, this part will also present the Brazilian context regarding the Regulation of Data Protection. The second part will be dedicated to the study of the treatment of Personal Data in the informational economy, and how its collection and treatment can be harmful to the privacy of the data subject. In this sense, the problems that make consent insufficient for the protection of Personal Data will be presented. Finally, two alternatives will be presented that aim to mitigate the problems that make consent inefficient for Data protection.

***Keywords**: Personal Data; Data Protection; Consent Term; Processing of Personal Data.*

SUMÁRIO

1 INTRODUÇÃO

Em um mundo cada vez mais conectado, existiriam pessoas que aceitariam dar seu primogênito em troca da participação em uma rede social? Será que as pessoas também aceitariam que seus dados fossem compartilhados pela mesma rede social com a Agência Nacional de Segurança americana – NSA? Importante lembrar que essa mesma agência foi denunciada por Edward Snowden por utilizar programas ultrassecretos de vigilância até então desconhecidos nos Estados Unidos da América - EUA[1].

Ademais, em um teste realizado por dois pesquisadores nos EUA, cujo objetivo era analisar o comportamento do usuário quanto a leitura da "política de privacidade" e "termos de serviços" de uma rede social fictícia, constatou-se que mais de 70% dos participantes não leram nenhum dos dois documentos e que 98% consentiram com as duas opções mencionadas acima.

Não obstante, é notório que empresas se utilizam de diversas informações obtidas a partir do tratamento de dados dos cidadãos, com o suposto argumento de "tornar a experiência mais agradável e melhorar a navegação do usuário no site". Nesta senda, já se tornou habitual o consumidor sentir-se perseguido por anúncios sobre produtos pesquisados em dias anteriores, mas estariam os cidadãos conscientes de que seus dados são utilizados para estes fins? Saberiam eles que seus dados são utilizados para a criação de um perfil digital idêntico à sua vida real?

Veremos neste trabalho como as empresas utilizam ferramentas como os *cookies* para a captação de dados de localização, navegação e até de compras dos usuários para a criação de perfis digitais dos consumidores. Nesse cenário, importante destaque merece o experimento realizado por Joana Varon demonstrando a eficiência e o grau de acerto das mensagens publicitárias customizadas.

É neste contexto que o presente trabalho busca trazer à luz questões de como empresas tratam os dados de usuários de seus produtos a fim de torná-los não somente consumidores, mas também produtos em uma esteira que lucra (e muito) com a venda de informações obtidas, na maior parte das vezes, sem que o consumidor saiba que está autorizando através de seu consentimento, que embora seja livre, é também equivocado e sem muita transparência.

---

[1] A denúncia realizada por Edward Snowden foi publicada no jornal *The Washington Post* em junho de 2013. Disponível em: https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?hpid=z1. Acessado em 13.05.2022

Para muitas pessoas que estudam sobre o funcionamento da internet, das redes sociais, internet das coisas, e, principalmente, privacidade e proteção de dados, pode parecer fácil a compreensão de como estamos enxergando um anúncio sobre um produto que até momentos antes estávamos pesquisando em um site qualquer. No entanto, como se verá, esse complexo funcionamento da publicidade direcionada está muito relacionada com a desinformação do usuário médio, que consente com o tratamento de seus dados, e não sabe o porquê de estar sendo bombardeado diariamente com publicidade a fim de induzi-lo ao consumo.

De fato, a proteção de dados como conhecemos possui uma forte ligação com a coleta do consentimento do usuário como um processo. São diversas as discussões acerca do instituto do consentimento, que data desde as primeiras gerações de leis sobre a proteção de dados. Embora o consentimento do usuário não seja o único e nem o mais importante hierarquicamente nas bases legais para o tratamento de dados, ele é um dos mais utilizados.

Por essa razão, a pesquisa para elaborar este trabalho teve como foco o seguinte questionamento “o termo de consentimento é suficiente para proteger os dados imperceptíveis dos usuários?”.

Para tanto, o trabalho encontra-se dividido em três partes, em uma espécie de linha do tempo, com o objetivo de: i) demonstrar a construção histórica da proteção de dados como conhecemos hoje; ii) a forma pela qual os dados são tratados a fim de se obter informações relevantes dos usuários e demonstrar que o termo de consentimento, por si só, não é capaz de garantir a proteção de dados pessoais do usuário, e, por fim iii) apresentar possíveis alternativas frente à insuficiência do consentimento do usuário.

2 DA PRIVACIDADE À PROTEÇÃO DOS DADOS PESSOAIS

O direito à proteção de dados pessoais como conhecemos hoje não foi construído da noite para o dia, tampouco em anos, mas sim em décadas de debates e mudanças de conceitos e pensamentos.

Nesse sentido, o presente capítulo tem por objetivo demonstrar o desenvolvimento histórico da discussão acerca da proteção de dados, que teve seu nascimento a partir da busca por um direito à privacidade.

No decorrer desse trajeto é possível perceber uma mudança na concepção dos termos ao longo dos anos, muito em razão do surgimento de novas tecnologias, que ao fim e ao cabo, trouxeram novas terminologias, novos conceitos e novos desafios para a sociedade e cultura jurídica da época.

Por fim, veremos que o debate que se inicia por um "*right to privacy*" percorre um longo caminho, repleto de transformações, tanto da sociedade quanto da tecnologia, trazendo para a discussão direitos que em 1890 sequer eram mencionados, chegando ao debate acerca do consentimento do cidadão para o tratamento de seus dados pessoais.

2.1 A PESSOA E O DIREITO À PRIVACIDADE

Muito embora hoje tenhamos uma consciência maior acerca das questões relacionadas à nossa privacidade no meio virtual, o tema da privacidade já era próprio do direito — o que não significa dizer que o conceito de privacidade que conhecemos hoje era o mesmo em décadas passadas —, apresentando-se em diversos sentidos nas mais variadas épocas e sociedades[2].

Foi somente a partir da metade do século XIX que o debate doutrinário acerca do direito à privacidade ganhou impulso, muito em razão do surgimento de técnicas apoiadas por instrumentos tecnológicos capazes de possibilitar o acesso e a divulgação de fatos, que de alguma forma, invadiam a esfera privada do indivíduo[3].

---

[2] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 29.

[3] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Editora Saraiva, 2014 p. 27-28.

Remonta desta época o artigo *The right to privacy*, assinado pelos autores Samuel D. Warren e Louis D. Brandeis, e publicado na *Harvard Law Review* em 1890. Neste artigo os autores denunciavam a invasão de suas vidas privadas por fotografias, jornais e outras tecnologias:

> "Invenções recentes e métodos de negócios chamam a atenção para o próximo passo que deve ser dado para a proteção da pessoa, e para garantir ao indivíduo, o que o juiz chama de direito de "ficar sozinho". 4. Fotografias instantâneas e empresas jornalísticas têm invadido recintos sagrados de particulares e a vida doméstica; vários dispositivos mecânicos ameaçam fazer boa previsão de que "o que é sussurrado no armário será proclamado do telhado das casas"".[4]

Dessa forma, o direito à privacidade possuía uma conotação de individualismo, sendo inserido no ordenamento jurídico com um perfil eminentemente patrimonialista, reservado a extratos sociais bem determinados. Ainda, como nos mostra Danilo Doneda, o direito à privacidade era utilizado como subterfúgio para esconder casos dos holofotes, como retratam alguns casos do judiciário da época. Entre eles, podemos citar o caso entre o ditador Benito Mussolini e sua amante Clara Petacci[5], e tantos outros de pessoas com alguma projeção social.

O direito à privacidade estava, portanto, relacionado a uma proteção contra a inviolabilidade da personalidade. Conforme Laura Schertel, citando os autores Warren e Brandeis, "o princípio que protege escritos pessoais e outras produções pessoais, não contra o furto ou a apropriação física, mas contra toda forma de publicação, é na realidade não o princípio da propriedade privada, mas da inviolabilidade da personalidade"[6].

---

[4] Tradução livre de "*Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone". Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops*". Ver em WARREN, Samuel. D.; BRANDEIS, Louis. D. *The right to privacy*. **Harvard Law Review**, Cambridge, v. 4, n. 5, p. 193–220, 1890. Disponível em: https://www.jstor.org/stable/1321160. p. 195. Acesso em 21.12.2021

[5] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 31-32.

[6] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 28.

2.2 DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS

A ideia de direito à privacidade como forma elitista de proteção à privacidade durou até a década de 1960[7], quando a transformação do Estado, em conjunto com a revolução tecnológica, modificou o alcance e o sentido do direito à privacidade[8].

Com o aumento no volume, intensidade e até mesmo na complexidade nos tratamentos de dados pessoais, não restou outro caminho senão incorporar novos elementos a fim de garantir a tutela integral da pessoa. Dessa forma, tornou-se necessária a adoção de medidas visando ao fortalecimento de instrumentos de garantias individuais, diante da multiplicação de bancos de dados com informações pessoais[9].

Os sinais dessa mudança se tornam claros a partir de 1970, quando o direito passou a associar cada vez mais a privacidade com casos de informações armazenadas em bancos de dados. Conforme aponta Danilo Doneda, a primeira lei norte-americana sobre o assunto regulava os bancos de dados sobre consumidores, os quais eram administrados por escritórios de proteção ao crédito e cadastro de consumidores[10].

Nessa perspectiva, é possível perceber que a partir do momento em que a tecnologia possibilita o armazenamento e o processamento rápido de dados pessoais, dá-se a associação entre proteção à privacidade e informações pessoais[11]. Assim, a compreensão de privacidade modifica-se, dando origem à disciplina da proteção de dados pessoais, uma vez que não se trata mais de uma proteção à privacidade com caráter individualista, mas sim de uma situação com potencial de violar a privacidade de uma parcela da população.

Nesse contexto, conforme aponta Laura Schertel, “a proteção de dados adquire um âmbito mais abrangente, compreendendo-se como um fenômeno coletivo, tendo em vista que

---

[7] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 33.

[8] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 29.

[9] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. E-book.

[10] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 130.

[11] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 32.

os danos causados pelo processamento impróprio de dados pessoais são, por natureza, difusos, exigindo uma tutela jurídica coletiva”[12].

A partir dessa concepção de proteção de dados pessoais, desenvolveu-se em diversos países a formação das bases do direito à proteção de dados pessoais. Considerada a legislação pioneira, a lei de proteção de dados do Estado alemão de Hesse, de 1970[13], serviu como experiência para que outras legislações surgissem na Europa na década de 1970, entre elas, a Lei sueca de proteção de dados – *Datalagen* e a lei francesa de proteção de dados pessoais de 1978 – *Informatique et Libertées*[14].

Em 1983, uma decisão do Tribunal Constitucional alemão relacionada à proteção de dados pessoais foi decisiva para o desenvolvimento desse direito. Nesse caso, era contestada uma lei federal que regia o censo alemão, aprovada em 1982. De acordo com Danilo Doneda, “os motivos que levaram a Corte alemã a reconhecer a incompatibilidade da referida lei era o fato de que, caso os dados recolhidos fossem utilizados ao mesmo tempo para fins administrativos e estatísticos estaria caracterizada a diversidade de finalidades”[15].

Em outras palavras, “a Lei do Censo alemã determinava que os cidadãos fornecessem diversos dados pessoais com o objetivo de mensurar estatisticamente a distribuição espacial e geográfica da população”[16]. Entretanto, as disposições acerca da utilização dos dados dos cidadãos na referida lei eram vagas e demasiadamente amplas, o que gerou o ajuizamento de

---

[12] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 35-36.

[13] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O direito fundamental à proteção de dados. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. E-book.

[14] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. E-book.

[15] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 170-171.

[16] BIONI, Bruno. **Proteção de dados pessoais e a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

mil e seiscentas[17] reclamações constitucionais perante o Tribunal Constitucional alemão, que, consequentemente, a declarou como sendo parcialmente inconstitucional[18].

Da mesma forma, em 2020 o Governo Federal brasileiro editou a Medida Provisória 954/2020[19], a qual, nos termos de seu art. 2º, determinava que as "empresas de telecomunicação prestadoras do STFC e do SMP deverão disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas". Nesse caso, que pode ser equiparado ao julgamento do Tribunal Constitucional alemão, o Supremo Tribunal Federal, por maioria, referendou a medida cautelar suspendendo a eficácia da MP 954/20[20].

Assim, pode-se compreender que o direito à privacidade se transformou ao longo do tempo, tendo em vista que grande parcela da população se encontra sujeita a situações de violação de sua privacidade. Nesse sentido, como aponta Anderson Schreiber[21], "a tutela da privacidade, nessa nova acepção, não se contenta com a proibição à intromissão alheia na vida intima (dever geral de abstenção)". Para o mesmo autor, "impõe também deveres de caráter positivo, como o dever de solicitar autorização para a inclusão do nome de certa pessoa em um cadastro de dados ou o dever de possibilitar a correção de dados do mesmo cadastro".

Com efeito, esse novo entendimento pode ser verificado com clareza nos últimos 40 anos nas construções legislativas e jurisprudenciais acerca do tema, tanto pelo direito ao acesso aos dados armazenados pelos órgãos públicos quanto pela autodeterminação afirmativa

---

[17] MENKE, Fabiano. As origens alemãs e o significado da autoderminação informativa. **Migalhas de Proteção de Dados**, p. online, 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/335735/as-origens-alemas-e-o-significado-da-autodeterminacao-informativa. Acesso em 08.02.2022

[18] MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Revista Jurídica Luso-Brasileira**, Ano 5, n. 1, p. 781–809, 2019. Disponível em: https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf. p. 783.

[19] BRASIL, Presidência da República. **Medida Provisória nº 954, de abril de 2020**. p. Eletrônico. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em 23.01.2022

[20] BRASIL, Supremo Tribunal Federal. **ADI nº 6387. Rel. Min. Rosa Weber, Plenário, j. 06 e 07.05.2020**. p. Eletrônico. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 23.01.2022

[21] SCHREIBER, Anderson. **Direitos da personalidade: revista e atualizada.** 3. ed. São Paulo: Atlas, 2014. E-book.

estabelecida pelo Tribunal Constitucional alemão[22]. O objetivo do próximo tópico será apresentar o desenvolvimento geracional das leis de proteção de dados.

2.3 DESENVOLVIMENTO GERACIONAL DAS LEIS DE PROTEÇÃO DE DADOS

A necessidade de leis acerca da proteção de dados pessoais surge, basicamente, com a formação do Estado Moderno. Isso porque, a partir da Segunda Guerra Mundial, o Estado percebe a importância das informações pessoais da população para planejar e coordenar ações para um crescimento ordenado[23].

De acordo com Laura Schertel, a primeira geração de normas de proteção de dados pessoais surgiu como reação ao processamento eletrônico de dados nas administrações públicas e nas empresas privadas[24]. Com a mudança de um estado liberal para a o Estado de bem-estar social, houve uma grande demanda por informações pessoais da população por parte do Estado, indo desde a realização de censos até a obrigatoriedade de comunicação de determinadas informações pessoais à administração pública[25].

Inclusive, data dessa época a obra "1984", escrita por George Orwell e publicada em 1949. Essa obra, um clássico da literatura, trazia a figura do *"Big Brother"*, pelo qual o escritor britânico buscava expor os perigos do monopólio das informações por parte do Estado e o fim da privacidade através de uma vigilância ostensiva.

Entre as leis da primeira geração podemos citar as leis do Estado alemão de Hesse de 1970, a Lei de Dados da Suécia de 1973, o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz de 1974, a Lei Federal de Proteção de Dados da Alemanha de 1977[26]. Já nos EUA, em 1970 foi aprovada o *Fair Credit Reporting*, cujo objetivo era a regulamentação dos

---

[22] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 177.

[23] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[24] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 29.

[25] BIONI, Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021 p. E-book.

[26] MAYER-SCHÖNBERGER, Viktor. *Generational Development of Data Protection in Europe.* **Technology and Privacy: The New Landscape**. London: The MIT Press, 1997. p. 219–242. Disponível em: https://doi.org/10.7551/mitpress/6682.003.0010. p. 221.

relatórios de créditos dos consumidores, e o *Privacy Act* em 1974, aplicável à administração pública[27].

Conforme explica Danilo Doneda, estas leis tinham por objetivo a regulação em um cenário onde grandes centros de tratamento de dados concentrariam a coleta e a gestão de dados pessoais. Dessa maneira, o núcleo destas leis era a concessão de autorizações para a criação destes bancos de dados, bem como seu controle posterior por parte dos órgãos públicos[28].

Em síntese, pode-se concluir que a primeira geração de leis de proteção de dados tinha como foco a esfera da administração pública, e o objetivo de estabelecer normas rígidas para domar o uso da tecnologia[29].

Diante da multiplicação dos centros de processamento de dados, as leis da primeira geração logo se tornaram ultrapassadas. Assim, na segunda metade da década de 1970 surge a segunda geração de leis sobre o tema, tendo como primeiro modelo a lei francesa de proteção de dados pessoais, intitulada *Informatique el Libertés*[30].

A característica das leis da segunda geração é a transferência da responsabilidade de proteção dos dados para o titular, ou seja, se antes o fluxo das informações pessoais deveria ser autorizado pelo Estado, agora caberia ao próprio cidadão gerenciá-lo, a partir do consentimento, onde poderia autorizar sua coleta, uso e compartilhamento dos dados[31].

Entretanto, como explica Doneda, estas leis também apresentavam seus problemas, pois o fornecimento de dados por parte do cidadão tinha se tornado algo indispensável para sua efetiva participação na vida social[32]. Dessa forma, o fluxo de informações pessoais era intenso

---

[27] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 30.

[28] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 180.

[29] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[30] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 181.

[31] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[32] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 182.

tanto por parte do Estado quanto por entes privados, e quando o cidadão buscava interromper ou até mesmo questionar esse fluxo, corria-se o risco de ser excluído de algum aspecto da vida social. Nesse sentido, importante destacar o apontamento de Viktor Mayer-Schönberger acerca do assunto:

> "Direitos individuais a serviços sociais e pagamentos do governo exigem um fluxo contínuo de informações do indivíduo para a burocracia governamental. Cidadãos e sociedade estão tão intensa e subliminarmente entrelaçados que uma tentativa deliberada de um indivíduo de resistir a tais pedidos de informação, se possível, acarreta um custo social extraordinário. Da mesma forma, desde questões bancárias e financeiras até viagens e votação, a divulgação de informações pessoais é, na maioria das vezes, uma pré-condição para a participação individual"[33]

Como bem aduz Laura Schertel, a segunda geração de normas de proteção de dados pessoais suscita uma controvérsia bastante interessante, relacionada à efetividade do consentimento do cidadão e do real exercício de sua liberdade de escolha, em um contexto no qual a não disponibilização dos dados pode acarretar a sua exclusão social[34].

É nessa perspectiva que surge a terceira geração de leis de proteção de dados pessoais na década de 1980, cujo objetivo era a sofisticação da tutela dos dados pessoais, ainda centrada no cidadão, porém, passando a abranger mais do que a liberdade de fornecer ou não seus dados pessoais, mas também garantir a efetividade desta liberdade[35].

De acordo com Bruno Bioni, nesse estágio, as normas de proteção de dados pessoais procuraram assegurar a participação do indivíduo em todos os movimentos de seus dados

---

[33] Tradução livre de "*Individual entitlements to social services and government transfer payments require a continuous flow of information from the individual to the government bureaucracy. Citizens and society are so intensely and subliminally intertwined that a deliberate attempt by an individual to resist such information requests, if possible at all, carries with it an extraordinary social cost. Similarly, from bank and money matters to travel and voting, disclosure of personal information more often than not is a precondition to individual participation*". MAYER-SCHÖNBERGER, Viktor. *Generational Development of Data Protection in Europe.* **Technology and Privacy: The New Landscape**. London: The MIT Press, 1997. p. 219–242. Disponível em: https://doi.org/10.7551/mitpress/6682.003.0010. p. 229.

[34] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 40-41.

[35] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 182-183.

pessoais, desde a coleta ao compartilhamento[36], e não apenas como uma opção entre "tudo ou nada"[37].

No que tange ao desenvolvimento tecnológico, Viktor Mayer-Schönberger aponta que a tecnologia da informação se desenvolveu ainda mais no decorrer da terceira geração de proteção de dados. O processamento de dados não se dava mais por modelos centralizados, mas sim por meio de uma tecnologia de redes eletrônicas rápidas, eficientes e baratas. Assim, tornava quase impossível a localização física dos dados, pois esses estavam armazenados em redes, podendo ser transferidos em segundos[38].

Ademais, a terceira geração de normas de proteção de dados pessoais é marcada pela decisão do Tribunal Constitucional alemão, de 1983, que julgou parcialmente inconstitucional a Lei do Recenseamento. Nesse caso, o Tribunal reinterpretou a Lei Federal de Proteção de Dados Pessoais alemã à luz da Lei Fundamental de Bonn, declarando que os cidadãos teriam o direito à autodeterminação informativa[39].

Doneda explica que essa autodeterminação informativa surge como uma extensão das liberdades presentes nas leis de segunda geração, com várias mudanças na sua estrutura. O objetivo era fazer com que a pessoa participasse de forma consciente e ativa nas fases posteriores do processo de tratamento e utilização de seus dados por terceiros. Dessa forma, essas leis ainda incluíam algumas garantias, como o dever de informação[40].

Contudo, o ideal participativo dos cidadãos no controle de suas informações não era factível no mundo real. Pois, da mesma forma que ocorreu nas leis de segunda geração, as pessoas não estavam dispostas a arcar com os altos custos, tanto monetário quanto social, para exercer esse direito. Por fim, apesar das tentativas de ampliação e aplicação da lei da proteção

---

[36] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[37] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 42.

[38] MAYER-SCHÖNBERGER, Viktor. *Generational Development of Data Protection in Europe.* **Technology and Privacy: The New Landscape**. London: The MIT Press, 1997. p. 219–242. Disponível em: https://doi.org/10.7551/mitpress/6682.003.0010. p. 230.

[39] MARTINS, Leonardo (Org.). **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Fundación Konrad-Adenauer, 2005. p. 236-237.

[40] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 183.

de dados, o exercício do direito de autodeterminação informacional permaneceu como um privilégio de uma minoria[41].

De outra banda, a quarta geração de leis surge com o objetivo de sanar esses problemas apresentados nas gerações anteriores. Com isso, tem-se a disseminação de autoridade independentes para a aplicação de leis, uma vez que o cidadão não possui um grande poder de "barganha" para ter seus dados processados e utilizados por terceiros[42].

Ademais, acerca da quarta geração de leis de proteção de dados, cabe destacar as reflexões de Spiros Simitis[43] acerca do tratamento de dados pessoais sensíveis. Assim, Spiros expõe que a partir das normas da quarta geração, dados considerados sensíveis deixaram de ocupar a esfera do controle individual, passando a compor uma lista não exaustiva de dados cujo tratamento deve ser realizado de maneira distinta. Nesse sentido, é possível observar a proibição, tanto imparcial quanto total, imposta ao tratamento de dados com potencial de acarretar discriminações raciais, sobre opiniões políticas, crenças religiosas, questões relacionadas à etnia e opção sexual[44].

Entretanto, esse progresso geracional não eliminou o protagonismo do consentimento. Como aponta Bioni, o consentimento continuou com destaque na abordagem regulatória, sendo adjetivado, como devendo ser livre, informado, inequívoco, explícito e/ou específico. Em suma, o titular dos dados permanece como ponto focal, sendo replicado até os dias de hoje[45].

---

[41] MAYER-SCHÖNBERGER, Viktor. *Generational Development of Data Protection in Europe.* **Technology and Privacy: The New Landscape**. London: The MIT Press, 1997. p. 219–242. Disponível em: https://doi.org/10.7551/mitpress/6682.003.0010. p. 232.

[42] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 184.

[43] Spiros Simitis é um importante jurista, reconhecido internacionalmente como o "Pai da proteção de dados", tendo participado diretamente na edição da Lei de Hesse, de 1970, bem como a própria criação da disciplina da proteção de dados. Ver mais em MENKE, Fabiano. Spiros Simitis e a primeira lei de proteção de dados do mundo. **Migalhas de Proteção de Dados**, nov. 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/355182/spiros-simitis-e-a-primeira-lei-de-protecao-de-dados-do-mundo. Acessado em 26.04.2022.

[44] SIMITIS, Spiros. *Revisiting Sensitive Data*. **Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, Strasbourg, 24-26 November 1999. p. 1–11. Disponível em: https://rm.coe.int/09000016806845af. Acessado em 26.04.2022.

[45] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

O próximo tópico abordará o desenvolvimento de alguns princípios comuns, acompanhando a evolução das normas de proteção de dados pessoais, a fim de verificar uma forte manifestação da convergência das soluções legislativas acerca da matéria[46].

2.4 PRINCÍPIOS PARA A PROTEÇÃO DE DADOS PESSOAIS

O desenvolvimento das normas de proteção de dados trouxe ainda, com o passar dos anos, alguns princípios específicos, cuja finalidade é delimitar o tratamento de dados, além de garantir ao indivíduo o poder de controlar o fluxo de seus dados pessoais[47].

Esse quadro comum de princípios de proteção de dados é conhecido como *"Fair Information Principles"* e remonta à década de 1970, tanto nos EUA quanto na Europa[48]. Entretanto, de acordo com Doneda, alguns destes princípios já estavam presentes nas leis de primeira e segunda geração, os quais foram desenvolvidos pelas leis posteriores[49].

Dessa forma, em 1972, no Departamento de Saúde, Educação e Bem-Estar (*Department of Health, Education, and Welfare*) dos EUA, foi criado um comitê consultivo de sistemas automatizados de dados pessoais, denominado *"Advisory Committee on Automated Personal Data Systems"*[50]. Um ano após sua criação, o comitê emitiu um relatório sobre "Registros, Computadores e Direitos do Cidadão", com o objetivo de redefinir o conceito de privacidade, além de estabelecer cinco princípios fundamentais que todo processamento de dados deveria seguir:

a) Não deve existir sistema de armazenamento de dados pessoais cuja existência seja segredo;

---

[46] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 185.

[47] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 68.

[48] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 68.

[49] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 185.

[50] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 68.

b) Deve existir um meio para que o indivíduo possa ter conhecimento sobre quais informações a seu respeito estão registradas e de que forma são utilizadas;
c) Deve existir um meio para que o indivíduo possa evitar que informações a seu respeito, coletadas para um propósito especifico sejam utilizadas ou disponibilizadas para outros fins sem o seu consentimento;
d) Deve existir um meio pelo qual o indivíduo possa corrigir ou retificar um registro de informação a seu respeito;
e) Qualquer organização que crie, mantenha, use ou divulgue registros com dados pessoais identificáveis deve garantir a confiabilidade dos dados para o uso pretendido e deve tomar as devidas precauções para evitar o uso indevido destes dados[51].

Ademais, no mesmo período, a Grã-Bretanha já possuía um Comitê de Privacidade, coordenado por Kenneth Younger, cuja finalidade era analisar os riscos do tratamento automatizado de dados por parte das organizações privadas. Esse comitê emitiu um relatório sugerindo dez princípios para a proteção de dados[52].

Conforme aponta Danilo Doneda, essas regras passaram a ser encontradas em diversas normativas sobre proteção de dados pessoais, como na Convenção 108 do Conselho da Europa e nas *Guidelines* da OCDE, do início dos anos 1980[53].

Vejamos, a seguir, de forma sintetizada as principais características de alguns desses princípios para o tratamento de dados pessoais.

2.4.1 Princípio da publicidade

Também conhecido como *princípio da transparência*, exige que os bancos de dados pessoais sejam públicos[54]. Conforme aponta Laura Schertel, esse princípio tem como noção a

---

[51] EUA. HEW. Records, Computers and the Rights of Citizens. **Report of the Secretary's Advisory Committee on Automated Personal Data Systems**, p. online, Julho, 1973. Tradução livre. Disponível em: https://aspe.hhs.gov/reports/records-computers-rights-citizens. Acesso em 08.02.2022

[52] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 69.

[53] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 186.

[54] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 186-187.

ideia de que a transparência é uma das formas de combater o abuso no tratamento dos dados pessoais[55].

Assim, é dever dos bancos de dados a publicação do nome, sede e conteúdo, em registros públicos, diários oficiais ou meios de grande circulação, sob pena de ineficácia desse direito[56].

2.4.2 Princípio da finalidade

Por sua vez, o princípio da finalidade indica que o tratamento dos dados pessoais deve seguir com a finalidade informada ao cidadão quando da coleta de seus dados[57].

Esse princípio possui uma grande relevância, pois, com base nele, fundamenta-se a limitação do acesso de terceiros ao banco de dados, ou a transferência desses dados para terceiros[58].

Ademais, esse princípio também serve para determinar um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade, fora da qual estaria configurada uma abusividade por parte do agente de tratamento[59].

Por fim, cumpre salientar que esse princípio é responsável pela exigência da informação expressa e limitada acerca da finalidade dos dados pessoais. Dessa forma, o responsável pelo tratamento dos dados pessoais tem a obrigação de informar, de forma clara ao usuário, sobre como seus dados serão tratados. Ou seja, em casos de finalidades amplas ou genéricas, esse tratamento poderá ser considerado ilegítimo[60].

---

[55] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 71.

[56] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 71.

[57] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 187.

[58] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 70.

[59] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 187.

[60] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 71.

2.4.3 Princípio da qualidade dos dados

O princípio da qualidade dos dados refere-se à exigência de que os dados pessoais presentes nos bancos de dados devem ser objeto de tratamento legítimo e lícito. Além disso, esses dados devem ser objetivos, exatos e atualizados[61].

Dessa forma, como aponta Bruno Bioni, ao lado do princípio da qualidade dos dados está o direito de correção dos dados, a fim de haver uma correspondência fidedigna entre a pessoa e seus dados pessoais[62].

Portanto, para que esse princípio seja efetivo, é fundamental que o titular dos dados tenha a garantia dos direitos de acesso, retificação e cancelamento dos dados[63].

2.4.4 Princípio da segurança física e lógica

Este princípio trata da exigência básica de que todo e qualquer banco de dados pessoais deve estar protegido contra os riscos de extravio, destruição, modificação, transmissão ou acesso de pessoas não autorizadas[64].

2.4.5 Princípio do livre acesso

O princípio do livre acesso está intimamente relacionado com o princípio da qualidade dos dados pessoais, isso porque, conforme aponta Danilo Doneda, esse princípio busca garantir ao titular dos dados o acesso ao banco de dados onde suas informações estão armazenadas. Dessa forma, o usuário poderá obter cópias dos registros, e, consequentemente, ter um maior controle acerca desses dados[65].

---

[61] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 71-72.

[62] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[63] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 72.

[64] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 187.

[65] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 187.

2.4.6 Princípio do consentimento

O princípio do consentimento, por sua vez, trata sobre o exercício da liberdade do usuário em ter o controle de seus dados pessoais. Para isso, o consentimento deve ser livre, específico e informado, com exceção de casos previstos legalmente, que, dessa forma justificariam o processamento de dados sem o prévio consentimento do titular[66].

Estes princípios possuem grande relevância na construção histórica de diversas leis, tratados, convenções ou acordos entre privados[67]. O próximo tópico tem por objetivo demonstrar o desenvolvimento das normas de proteção de dados pessoais no ordenamento jurídico brasileiro, partindo do Código de Defesa do Consumidor até a mais nova legislação acerca do tema.

2.5 CONTEXTO BRASILEIRO: DO CDC À LGPD

Neste tópico abordaremos a legislação brasileira no que tange à proteção dos dados pessoais. Muito embora este não seja o tema central do presente trabalho, essa breve análise possui o condão de identificar o direito do cidadão à proteção de dados nas normas brasileiras. Ademais, servirá também como um breve resumo para elucidar os tópicos seguintes, numa espécie de linha do tempo para o leitor.

Dessa forma, analisaremos de forma sintetizada o Código de Defesa do Consumidor, a Lei de Acesso à Informação, Lei do Cadastro Positivo, Marco Civil da Internet, e, finalmente, a Lei Geral de Proteção de Dados. Essa última, que entrou em vigor recentemente, e trouxe grandes avanços para o tema da proteção de dados na legislação brasileira.

2.5.1 Código de Defesa do Consumidor - CDC

O Código de Defesa do Consumidor é considerada a primeira lei sobre privacidade e proteção de dados pessoais no Brasil[68]. As disposições do CDC trazem como foco do legislador,

---

[66] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 71.

[67] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, [*s. l.*], v. 12, n. 2, p. 91–108, 2011. Disponível em: http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315. p. 101.

[68] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 141.

o estabelecimento de um equilíbrio na relação de consumo, colocando limites ao uso das informações do consumidor por parte do fornecedor, principalmente nas informações creditícias[69].

O artigo 43, do CDC, dispõe sobre a regulamentação dos bancos de dados e cadastro dos consumidores. Nesse dispositivo podemos encontrar diversos preceitos para a proteção de dados que já mencionamos anteriormente, entre eles, *direito de acesso, princípio da qualidade dos dados, princípio da transparência*, entre outros[70].

Ademais, importante mencionar que esse artigo foi inspirado, de acordo com o próprio responsável pela elaboração do anteprojeto desta seção do CDC, na normativa norte-americana de proteção ao crédito estabelecida pelo *National Consumer Act Fair* e pelo *Fair Credit Reporting Act* – FCRA, de 1970[71].

2.5.2 Lei do Cadastro Positivo

A Lei do Cadastro Positivo surgiu em contraposição ao até então existente Cadastro Negativo, o qual mantinha apenas as informações creditícias de "maus pagadores". Com o objetivo de trazer informações de adimplemento dos cidadãos, a Lei nº 12.414/2011, tratou de disciplinar a formação e consulta a bancos de dados com informações de adimplemento para a formação de um histórico de crédito. Dessa forma, os interessados em oferecer crédito (instituições financeiras e comerciantes, por ex.) teriam acesso a uma espécie de pontuação do consumidor – quão mais alto o *score*, melhor seu histórico de bom pagador[72].

De acordo com Laura Schertel, a principal característica do Cadastro Positivo está na ampliação do fluxo de dados no mercado, onde se torna possível a formação de bancos de dados

---

[69] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 277.

[70] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 142.

[71] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 278.

[72] Renzetti, Bruno Polonio; Almeida, Luís Felipe Rasmus de; Banhos, Tiago Paes de Andrade. Implicações da Lei do Cadastro Positivo para a Proteção de Dados Pessoais no Brasil: As Dificuldades do Sistema Opt-Out. ***In*: A Lei Geral de Proteção de dados Brasileira: Uma Análise Setorial (volume I)** / Coord. Eduardo Tomasevicius Filho. 1. ed. São Paulo: Almedina, 2021. p. 130–171.

com informações de adimplemento, da mesma forma que se buscou estabelecer regras de proteção à privacidade e métodos de controle e fiscalização dessa atividade[73].

Entretanto, vale ressaltar que em sua redação original, dada pela Lei nº 12.414/2011, o consentimento do cidadão para o tratamento de seus dados estava centrado na dinâmica de *opt-in*, na qual ele não era incluído de forma automática nesses *bureaux* de crédito, mas somente se assim desejasse. No entanto, a Lei Complementar nº 166/2019 trouxe diversas mudanças na sistemática do Cadastro Positivo, como, por exemplo, a mudança de um sistema de *opt-in* para *opt-out*, ou seja, agora o cidadão deve optar por sair do cadastro[74].

2.5.3 Lei de Acesso à Informação Pública

Para os propósitos deste trabalho, importante ainda analisar a Lei nº 12.527/2011, que trata do acesso à informação pública, muito embora não seja nosso objetivo fazer um exame geral dessas leis, mas apenas apontar alguns aspectos importantes no que tange ao tratamento de dados pessoais, buscando relacionar o desenvolvimento do tema no contexto brasileiro.

A referida lei possui um papel importante para o desenvolvimento do tema no Brasil, principalmente por prever uma garantia de maior transparência na administração pública, efetivando, igualmente a autodeterminação informativa do cidadão.

Como se vê no *caput* do art. 31, "o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais". Ademais, o parágrafo 1º, inciso II, do mesmo artigo, prevê duas regras para o acesso das informações por terceiros, bem como para a divulgação dessas informações por parte da administração pública: i) mediante previsão legal; ou ii) com o consentimento do titular dos dados[75].

---

[73] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 145.

[74] Renzetti, Bruno Polonio; Almeida, Luís Felipe Rasmus de; Banhos, Tiago Paes de Andrade. Implicações da Lei do Cadastro Positivo para a Proteção de Dados Pessoais no Brasil: As Dificuldades do Sistema Opt-Out. ***In*: A Lei Geral de Proteção de dados Brasileira: Uma Análise Setorial (volume I)** / Coord. Eduardo Tomasevicius Filho. 1. ed. São Paulo: Almedina, 2021. p. 130–171.

[75] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 152.

2.5.4 Marco Civil da Internet - MCI

A Lei nº 12.965/2014, conhecida como Marco Civil da Internet teve sua aprovação pelo Congresso brasileiro em 2014, após a grande repercussão das denúncias feitas pelo ex-analista Edward Snowden, da Agência Nacional de Segurança dos Estados Unidos, acerca de alguns sistemas de monitoramento telemático: PRISM, Upstream e Xkeyscore, entre outros[76].

Importante salientar que, na época da aprovação do Marco Civil da Internet, o Brasil se tornava o quarto país no mundo a ter uma legislação para a internet, depois da Eslovênia, Holanda e Chile[77].

Ademais, vale ressaltar também que antes das denúncias de Snowden o projeto de lei do MCI era um, e logo após, recebeu diversas alterações, como por exemplo, o art. 7º, que continha apenas cinco incisos, passando a ter oito incisos, todos direcionados para a proteção dos dados pessoais[78].

Além disso, enfatizando o controle dos usuários sobre seus dados pessoais, o MCI dispõe, que a qualquer momento o usuário poderá solicitar a exclusão definitiva de seus dados fornecidos, uma vez que encerrada a relação entre as partes[79].

2.5.5 Lei Geral de Proteção de Dados – LGPD

Por fim, quase uma década após a aprovação do MCI, o Brasil finalmente aprovou uma Lei Geral de Proteção de Dados, cujo anteprojeto de lei foi colocado sob consulta pública em 2010 e tinha o consentimento como a única base legal para o tratamento de dados pessoais.

---

[76] MORAIS, José Luis B. de; NETO, Elias Jacob de M. A Insuficiência do Marco Civil da Internet na Proteção das Comunicações Privadas Armazenadas e do Fluxo de Dados a Partir do Paradgma da Surveillance. ***In*: Marco Civil da Internet / Coordenadores: George Salomão Leite, Ronaldo Lemos**. São Paulo: Atlas, 2014. p. 417–439.

[77] PAESANI, Liliana Minardi. Garantia fundamental do não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei. **Marco Civil da Internet / Coordenadores: George Salomão Leite, Ronaldo Lemos**. São Paulo: Atlas, 2014. p. 518–526.

[78] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[79] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book..

Entretanto, após as consultas públicas, com a aprovação e sanção da lei, ele acabou sendo uma das hipóteses legais e não a cabeça do dispositivo[80].

A LGPD, nas palavras de Laura Schertel e Danilo Doneda, veio para complementar o marco regulatório brasileiro da Sociedade da Informação[81], tendo como inspiração o modelo europeu de proteção de dados, a partir da Diretiva 46/95/CE e no Regulamento Geral de Proteção de Dados (Regulamento 2016/679).

Ademais, a referida lei tem por objetivo regular todas as formas de tratamento de dados pessoais, que são definidos como quaisquer informações relacionadas a pessoa natural identificada ou identificável[82], tendo como alicerce o consentimento do titular dos dados, como se compreende dos artigos 7º e 8º, salvo as exceções descritas no art. 4º da LGPD[83].

No próximo tópico analisaremos as hipóteses legais para o tratamento de dados pessoais dispostos na Lei Geral de Proteção de Dados.

2.6 CONSENTIMENTO COMO BASE LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS NO BRASIL

Como já observado, para que o tratamento de dados pessoais seja considerado legítimo e lícito, ele deve ser norteado por determinados princípios previstos na LGPD, bem como estar fundamentado em uma das hipóteses legais, que entre elas, destacam-se o legítimo interesse e o consentimento do titular[84][85], sendo este último, o tema central deste trabalho.

---

[80] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[81] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor.** São Paulo: Editora RT. 2018. v. 120, p. 469–483. *E-book.*

[82] FRAZÃO, Ana. Objetivos e Alcance da Lei Geral de Proteção de Dados. ***In*: Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 99–129.

[83] BRASIL. **Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD)**, 2018. Seção 220, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

[84] Importante observar que, embora recebam destaque de pesquisadores e estudiosos do direito, o legítimo interesse e o consentimento do titular não se tratam das únicas hipóteses legais para o tratamento de dados pessoais, e tampouco podem ser consideradas como superiores, hierarquicamente, às demais hipóteses elencadas no art. 7º da lei.

[85] VIOLA, Mario; TEFFÉ, Chiara S. de. Tratamento de dados pessoais na LGPD: Estudo sobre as bases legais dos artigos 7º e 11. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. Digital.

Como bem aponta Fabiano Menke, a necessidade de fundamentar adequadamente o tratamento dos dados pessoais em base legal é um traço característico da escola de proteção de dados com raízes europeias[86], que como mencionado no tópico anterior, o Brasil teve forte inspiração para elaboração da lei vigente.

Nesse sentido, partindo da problemática proposta para elaboração do trabalho, tomaremos como foco o instituto do consentimento, muito embora existam outras bases legais para o tratamento de dados.

2.6.1 Consentimento do titular dos dados

O consentimento para o tratamento de dados pessoais é uma forma de manifestação individual, que possui o condão de legitimar a utilização destes dados por terceiros[87].

Como pode se observar no art. 7º, I, da LGPD[88], o tratamento de dados poderá ser realizado quando houver o consentimento do titular dos dados, consentimento esse caracterizado como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"[89].

Além disso, vale ressaltar o apontamento feito pelos autores Mario Viola e Chiara S. de Teffé, no sentido de que a LGPD estabelece em seu art. 9º, § 3º, que, se o tratamento dos dados pessoais for condição para o fornecimento de produto, serviço ou exercício de um direito, o titular deverá ser informado com destaque sobre esse fato, bem como saber de que forma poderá exercer seus direitos dispostos no art. 18. Isso significa dizer que o usuário terá um poder maior acerca da utilização de seus dados por um terceiro, principalmente em situações em que haja

---

[86] MENKE, Fabiano. A possibilidade de cumulação de bases legais nas operações de tratamento de dados pessoais. **Proteção de Dados: Temas controvertidos**. Indaiatuba, SP: Editora Foco, 2021. Paginação E-pub 279-293.

[87] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 317. Conforme explica Doneda, "a fundamentação desse consentimento reside na possibilidade de autodeterminação em relação aos dados pessoais, e que essa autodeterminação deve ser levada em conta para caracterizarmos tanto a natureza jurídica bem como os efeitos desse consentimento.

[88] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento de consentimento pelo titular. Ver em BRASIL. **Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD)**, 2018. Seção 220, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

[89] Conceituação dada pelo Art. 5º, XII da LGPD. Ver em BRASIL. **Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD)**, 2018. Seção 220, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

necessidade de uma tomada de decisão no sentido de aceitar ou não fazer parte ou utilizar um serviço, por exemplo[90].

No que tange à *manifestação livre* do titular dos dados, tem-se que essa escolha do usuário deve ser realizada sem intervenções ou situações que viciem o consentimento, sendo relevante uma análise da assimetria entre as partes e eventual vulnerabilidade de algum contratante[91].

No mesmo sentido, Bruno Bioni observa que deve se verificar o "poder de barganha" do titular dos dados em relação ao tratamento de seus dados, levando em consideração as opções com relação ao tipo de dados coletados até os seus possíveis usos[92].

Ademais, para que o consentimento seja lícito, o vocábulo *informado* significa dizer que o titular deve ter a sua disposição as informações necessárias e suficientes para discernir sobre a aceitação e, principalmente, de que forma seus dados serão tratados[93].

Da mesma forma, a manifestação de vontade deve ser *inequívoca*, ou seja, de forma clara. Embora o art. 8º não exija um consentimento por escrito, ele dispõe que essa autorização seja comprovada por algum meio que demonstre a manifestação de vontade do titular.

Por fim, a *finalidade* para o tratamento dos dados do titular deve ser explícita. Isso significa dizer que a declaração de vontade do cidadão deve ter um direcionamento, caso contrário, seria o equivalente a emitir um "cheque em branco" para o agente de tratamento[94].

---

[90] VIOLA, Mario; TEFFÉ, Chiara S. de. Tratamento de dados pessoais na LGPD: Estudo sobre as bases legais dos artigos 7º e 11. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. Digital.

[91] VIOLA, Mario; TEFFÉ, Chiara S. de. Tratamento de dados pessoais na LGPD: Estudo sobre as bases legais dos artigos 7º e 11. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. Digital.

[92] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[93] VIOLA, Mario; TEFFÉ, Chiara S. de. Tratamento de dados pessoais na LGPD: Estudo sobre as bases legais dos artigos 7º e 11. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. Digital.

[94] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

3 DO CONSENTIMENTO AO TRATAMENTO DE DADOS IMPERCEPTÍVEIS

Observamos ao longo do presente trabalho a jornada percorrida pelo consentimento no campo da proteção de dados, a fim de garantir uma autonomia individual e garantir um maior controle do titular acerca de seus direitos de personalidade[95].

Muito embora o consentimento tenha se mostrado evolutivo[96], diversos autores ressaltam sua insuficiência para a tutela da privacidade e proteção dos dados pessoais dos cidadãos, muito em razão da ascensão do *Big Data* e proliferação de novas tecnologias de rastreamento e monitoramento dos usuários na internet[97].

Realizada a construção histórica do consentimento, a partir da linha evolutiva das leis de proteção de dados, o presente capítulo tem como objetivo investigar a insuficiência do consentimento no tratamento dos dados imperceptíveis do cidadão.

Para melhor compreender a dinâmica dos dados pessoais, podemos considerar os dados pessoais em dois grupos: os dados perceptíveis, os quais o usuário tem pleno conhecimento sobre sua autorização para uso, nesse caso, *e-mail, nome, telefone, endereço,* entre outros. Ademais, esses dados perceptíveis são comuns para o usuário ao se cadastrar para utilizar um serviço ou produto como cadastro em redes sociais, plataformas de compras online e afins.

Por outro lado, os dados imperceptíveis são aqueles que o usuário autoriza, a priori, consentindo para seu tratamento, mas sem a capacidade de compreender de que forma serão tratados. Esses dados podem ser os de *localização, navegação na internet, compras e pesquisas realizadas em ambiente virtual,* bem como *seus gostos e afinidades*.

Dessa forma, a autorização para o uso desses dados imperceptíveis do usuário se dá (ou deveria se dar) a partir da leitura das *"Políticas de Privacidade"* ou *"Termos de Uso dos Dados"*, e posterior consentimento do cidadão. Entretanto, diversos estudos apontam que esse

---

[95] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[96] BIONI, Bruno; LUCIANO, Maria. O consentimento como processo: Em busca do consentimento válido. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. E-book. Conforme os autores, na segunda geração de leis o consentimento era até então adjetivado apenas como *informado*, enquanto que nas últimas gerações passou a receber outras qualificadoras: *livre, inequívoca, específica* e *expressa*.

[97] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521

formato de autorização se mostra pouco eficiente, além de demonstrar que as *limitações cognitivas* podem dificultar a tomada de decisão para tal.

Portanto, nos tópicos a seguir buscaremos compreender essa dinâmica do tratamento dos dados imperceptíveis do usuário, bem como observar a (in)eficácia do termo de consentimento para a proteção destes dados pessoais.

3.1 DADOS PESSOAIS COMO UM ATIVO NA ECONOMIA DA INFORMAÇÃO

É notória a evolução da inteligência gerada pela ciência mercadológica, principalmente na área de bens de consumo e publicidade, sendo os dados pessoais do usuário um fator vital para a engrenagem da economia da informação[98].

Deste modo, é possível organizar tais dados de maneira escalável, criando um mercado cuja base de sustentação é a sua extração e comodificação, tratando o cidadão como um mero expectador das suas informações[99].

Para contextualizar essa prática, que é bastante comum na segmentação do marketing, Rita Peixoto Blum[100] apresenta alguns exemplos das formas de coleta de dados, extraídas do relatório da Comissão Federal de Comércio (*Federal Trade Comission – FTC)* dos EUA, divulgado em 2010.

> – se você pesquisa por produtos ou serviços online, anunciantes podem coletar e compartilhar informações sobre as suas atividades, inclusive sobre as suas pesquisas, os sites que você visitou, e o conteúdo que você viu;
>
> – se você participa de um site de relacionamento social (i.e. rede social) os aplicativos de empresa terceira provavelmente terão acesso às informações ou conteúdos que você ou seus amigos "postar" (publicar) no referido site;
>
> – se você usa aplicativos de localização no seu smartphone (i.e. telefone móvel com acesso à internet), diversas companhias podem ter acesso ao seu paradeiro de forma exata;
>
> – se você utiliza cartões de fidelidade com uma loja de doces ou preenche um cartão de garantia de produto, seu nome, endereço e informações sobre a sua compra talvez

[98] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[99] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[100] BLUM, Rita Peixoto F. **O Direito à Privacidade e à Proteção dos Dados do Consumidor**. São Paulo: Almedina, 2018. p. 130.

> sejam compartilhadas com corretores de dados (“data brokers”) e combinadas com outras informações.

Nesse sentido, pode-se observar que o consumidor tem a sua privacidade invadida sem ao menos saber por quem, quando e como. Muito embora o usuário tenha autorizado o tratamento de seus dados, seja por fazer parte de uma rede social, seja por efetuar o cadastro de uma plataforma de compras online, o tratamento dos dados desse usuário vai muito além da simples posse do nome, e-mail, telefone e endereço, por parte da empresa privada.

Ademais, é de suma importância destacar que dados e informações são coisas completamente distintas, enquanto que dado é o estado primitivo da informação, algo que não se acresce conhecimento. Entretanto, quando processado e organizado, extrai-se dali uma informação inteligível[101].

Para exemplificar o funcionamento dessa prática, podemos utilizar o exemplo do famoso caso da Target Corporation[102], uma empresa de varejo americana que explora os padrões de compras de seus clientes.

Na obra, *O Poder do Hábito*, Charles Duhigg nos mostra como a companhia, que faturava 44 bilhões de dólares em 2002, passou a faturar 67 bilhões de dólares em 2010, a partir da venda de produtos para mulheres grávidas.

De acordo com Duhigg, o banco de dados da Target conseguia ligar as informações — a partir da coleta de dados dos usuários que acessavam o site — aos números de clientes e de suas famílias, conseguindo identificar suas pesquisas no ambiente virtual do site, bem como suas compras. Com isso, o analista de dados da Target, Andrew Pole, acabou identificando um padrão de compras de mulheres grávidas, chegando a atingir 87% de chances de acerto.

Dessa forma, a companhia passou a enviar cupons com itens de bebês para a residência de seus clientes, cuja pesquisa no site ativara o sinal de possível gravidez na família. Em sua obra, Duhigg apresenta um relato acerca de um consumidor que recebeu o cupom com itens

---

[101] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[102] DUHIGG, Charles. **O Poder do Hábito: por que fazemos o que fazemos na vida e nos negócios**. Rio de Janeiro: Objetiva, 2012. p. 195-225.

para mulheres grávidas e ficou furioso, mas que no fim, acabou sendo surpreendido pela eficácia da mineração dos dados:

> "Minha filha recebeu isso pelo correio!" ele disse. "Ela ainda está no ensino médio, e vocês estão mandando para ela cupons de roupas de bebê e berços? Estão tentando incentivar minha filha a engravidar?"
>
> O gerente não fazia ideia do que o homem estava falando. Olhou para o folheto que fora enviado pelo correio. De fato, estava o endereço à filha do homem e continha propagandas de roupas para grávidas, móveis para berçário e fotos de criancinhas sorridentes olhando nos olhos das mães.
>
> O gerente se desculpou profundamente, e então telefonou, alguns dias depois, para se desculpar de novo.
>
> O pai estava meio atônito.
>
> "Tive uma conversa com a minha filha", ele disse. "Pelo jeito, estão acontecendo coisas nesta casa das quais eu não estava totalmente ciente". Ele respirou fundo. "Ela vai ter o filho em agosto. Eu lhe devo um pedido de desculpas".[103]

Com efeito, o tratamento desses dados do consumidor torna possível a publicidade comportamental, onde pretende-se personalizar, ainda que de forma parcial, a comunicação entre empresas e consumidor, a fim de adicionar um determinado fator, aumentando a possibilidade de êxito da indução ao consumo[104].

Na mesma linha, Joana Varon, diretora executiva da Coding Rights, exemplifica a construção de perfis de consumo a partir da mineração de dados dos usuários:

> Da mesma forma, nosso histórico de compras *on-line* diz bastante sobre poder aquisitivo e preferências pessoais. Por meio dessas informações, é possível embasar o direcionamento de propagandas compatíveis com o nosso gosto, tentando-nos a comprar algo que não precisamos, bem como cobrar preços mais altos ou limitar o acesso ao crédito para determinados perfis[105].

Ademais, os dados pessoais não são utilizados somente para fins comerciais, eles também são utilizados para fins políticos. Nesse aspecto, basta relembrar o escândalo da

---

[103] DUHIGG, Charles. **O Poder do Hábito: por que fazemos o que fazemos na vida e nos negócios**. Rio de Janeiro: Objetiva, 2012. p. 209.

[104] LINS, Bruna R.; QUINELATO, Pietra D. Redes sociais à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Social Media Law: O Direito nas Redes Sociais.** São Paulo: Thomson Reuters Brasil, 2021. p. 143–184.

[105] Entrevista II publicada no Panorama Setorial da Internet, Número 2, Junho 2019, Ano 11. Disponível em: https://cetic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf. Acessado em 19.03.2022.

Cambridge Analytica[106], que veio à tona em 2018 e contribuiu para a concretização da Lei Geral de Proteção de Dados no Brasil[107].

No caso da *Cambridge Analytica*, os dados pessoais de usuários do Facebook foram obtidos através de um teste denominado *"thisisyourdigitallife"*, onde centenas de milhares de usuários receberam uma quantia em dinheiro para responder um teste de personalidade e concordar em ter seus dados coletados para uso acadêmico. Entretanto, os dados, tanto dos usuários que realizaram o teste como os de seus amigos na rede social foram utilizados para a construção de perfis de possíveis eleitores.

Assim, em 2016 a empresa foi contratada pela campanha de Donald Trump que, de acordo com investigações, teria usado mais de 50 milhões de perfis individuais, combinando-os com listas eleitorais. Com isso, foi possível construir um algoritmo capaz de analisar perfis da rede social e enviar mensagens personalizadas para o eleitor.

Entretanto, as mensagens personalizadas não foram enviadas somente para possíveis eleitores de Donald Trump. De acordo com o autor Giuliano Da Empoli, foram testadas inúmeras mensagens para desestimular os eleitores democratas de irem às urnas, tendo como foco os eleitores de Hillary Clinton e Bernie Sanders, adversários políticos do então candidato Trump[108].

Com isso, podemos observar que os dados pessoais constituem um papel valioso tanto para o interesse comercial quanto para interesses políticos. No tópico a seguir, buscaremos compreender a forma que se dá a obtenção dos dados imperceptíveis dos usuários.

3.2 DA COLETA AO TRATAMENTO DE DADOS E A PUBLICIDADE DIRECIONADA

A coleta dos dados pessoais pode ser caracterizada de duas formas: a primeira, com a participação ativa do usuário na concessão de suas informações à empresa. Nesse caso, o

---

[106] GADWALLADR, Carole; GRAHAM-HARRISON, Emma. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* **The Guardian**, março, 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acessado em 19.03.2022.

[107] Entrevista de Danilo Doneda na série 2018: Uma conjunção astral, disponível em: https://www.observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/. Acessado em 20.03.2022.

[108] EMPOLI, Giuliano Da. **Os engenheiros do caos**. 1. ed. São Paulo: Vestígio, 2020. p. 153.

usuário poderá ter seus dados coletados a partir de transações comerciais, censo e registros públicos, bem como através de pesquisas de mercado e de estilo de vida. Dessa forma, o usuário participa ativamente para a coleta de seus dados[109].

Por outro lado, a segunda forma de coleta de dados pessoais se dá com a utilização de tecnologias de controle na internet, entre elas o uso dos *cookies* e *spyware*. Nesse formato de coleta, os dados são captados de forma imperceptível aos olhos do usuário médio. Como bem aponta Laura Schertel,

> "o ambiente virtual é propenso às violações da privacidade, de uma forma mais imperceptível e silenciosa que o ambiente físico. Isso porque o espaço físico possibilita a constatação mais nítida do nível de privacidade disponível e permite que a pessoa tome as decisões a fim de aumentar ou diminuir a sua privacidade, o que nem sempre é possível no espaço virtual, uma vez que não se sabe quais informações estão sendo capturadas, nem o momento em que esse controle é realizado"[110]

Para exemplificar as duas formas de captação dos dados do titular, podemos utilizar uma atividade cotidiana de muitos usuários: a simples pesquisa para compra de um livro em algum site de vendas online (*Amazon*, *Americanas*, *Submarino,* etc).

Assim, o usuário, ao realizar o cadastro em uma dessas plataformas, estará fornecendo seus dados como: *nome, e-mail, telefone, endereço,* entre outros, com o objetivo de finalizar o processo de compra do livro no site – assim caracteriza-se a primeira forma, onde o usuário participa ativamente da concessão de seus dados. Entretanto, logo que o usuário acessa o site, ele terá uma janela *pop-up* solicitando o seu consentimento para o uso de *cookies* a fim de melhorar sua experiência no site.

Vale ressaltar que para efetuar uma simples pesquisa, o usuário não precisa ter ou realizar um cadastro prévio na plataforma, entretanto, ao aceitar os "termos de consentimento" ele já terá seus dados de *navegação e pesquisas* capturados pelos *cookies,* ainda que não resolva efetuar a compra naquele site específico – aqui, portanto, temos a caracterização da segunda forma.

---

[109] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 96-99.

[110] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 101-102.

Dessa maneira, tanto o proprietário do site quanto empresas terceiras, tidas como "parceiras", terão acesso às informações referente a navegação do usuário nas páginas e das compras realizadas naquele ambiente, tudo capturado através dos famigerados *cookies* — autorizados pelo usuário no momento do consentimento ao acessar o site.

De acordo com a literatura de sistemas de informação, os *cookies* são pequenas quantidades de informações armazenadas pelos sites no computador do usuário, em alguns casos com informações sobre o próprio usuário, como identificação e senhas[111].

Entretanto, os *cookies* também podem ser usados para o rastreamento do usuário durante sua navegação na internet, uma vez que essa ferramenta serve como um marcador digital, memorizando todos os movimentos do usuário na internet. Além disso, *cookies* armazenados por um longo período podem e são utilizados para construir um retrato do comportamento do usuário, sem que o mesmo tenha conhecimento dessa invasão à sua privacidade[112].

Ademais, os *cookies* são classificados em *first-party cookies* e *third-party cookies*, e ambos são utilizados para fins de rastreamento do comportamento do usuário, porém, de modos distintos.

Os *first-party cookies* são os *cookies* armazenados no computador diretamente pelo site em que o usuário está visitando. Através desses *cookies* o site saberá, por exemplo, quais são as configurações de idioma selecionado pelo usuário, páginas visitadas, além de poder salvar as informações de login do usuário, para que o mesmo não necessite fazê-lo novamente quando retornar ao site.

Os *third-party cookies*, por outro lado, são os *cookies* de terceiros, ou seja, eles são criados por uma empresa parceira do proprietário do site e são utilizados para fins de

---

[111] RAINER JR, R. Kelly; CEGIELSKI, Casey G. **Introdução a Sistemas de Informação**. 5. ed. Rio de Janeiro: Elsevier, 2016. E-book.

[112] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 103.

publicidade online. Esses *cookies* são colocados no site através de um *script* ou *tag*, a exemplo das *tags* do Google[113] e o *pixel* do Facebook[114].

Os *cookies*, portanto, apresentam grande utilidade para o usuário, possibilitando a memorização de senhas e personalização de serviços. Entretanto, quando o computador passa a ser associado a um determinado usuário, este pode trazer riscos à privacidade[115], e, justamente, nesse sentido, que a opinião do Grupo de Trabalho do art. 29 sobre "*Cookie Consent Exemption"* dispôs que esses tipos de *cookies* devem obter um consentimento prévio do usuário[116].

No entanto, não são apenas os *cookies* os responsáveis pela captação dos dados e informações dos usuários. Com um mundo cada vez mais conectado, novos modelos de negócios surgiram, onde consumidores não pagam mais em dinheiro pelos bens de consumo, mas sim com seus dados pessoais em troca de publicidade direcionada[117].

Nesse negócio, considerado *plurilateral*, o consumidor torna-se um produto comercializável, uma vez que seus dados fazem parte da operação econômica. Nesse sentido, Bruno Bioni esclarece que a terminologia *zero-price advertisement business model* exemplifica bem esse modelo:

> "Os usuários não pagam uma quantia monetária (*zero-price*) pelo produto ou serviço. A contraprestação deriva do fornecimento de seus dados pessoais, o que possibilita o direcionamento de conteúdo publicitário, e cuja receita pagará, indiretamente, pelo bem de consumo (*advertisement business model*)[118].

---

[113] A *Tag* do Google Ads, de acordo com a própria Google, serve para configurar a origem do público-alvo que acessa o site, tornando possível alcança-los novamente com publicidade de remarketing. https://support.google.com/google-ads/answer/2476688?hl=pt-PT. Acessado em 29.03.2022.

[114] O *Pixel* do Facebook é outro *third-party cookie* e, como o próprio Facebook explica, é um trecho de código colocado no site, cuja função é medir a eficácia da publicidade por meio das ações realizadas pelo usuário. https://pt-br.facebook.com/business/help/742478679120153?id=1205376682832142. Acessado em 29.03.2022.

[115] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 223.

[116] Opinião 04/2012 do Grupo de Trabalho do Art. 29 sobre *"Cookie Consent Exemption"*, de 7 de junho de 2012. Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf. Acessado em 29.03.2022.

[117] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[118] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

Esse tipo de negócio pode ser ilustrado através do Facebook, onde o usuário, a princípio, não paga qualquer valor para realizar seu registro na plataforma. Entretanto, as informações obtidas através dos dados dos usuários e vendidas para anunciantes tornam a plataforma cada vez mais valiosa à medida que aumenta o número de usuários — e, consequentemente, mais dados e informações[119].

Aliás, uma constatação bastante interessante acerca do Facebook é que até meados de 2018 a página utilizava o slogan "*It's free and always will be"*, que em tradução livre significa "É gratuito e sempre será", que agora não faz mais parte da página inicial da rede social. Com a ajuda do site "*Way Back Machine*" podemos confirmar que a frase fazia parte da identidade do Facebook[120].

Outra forma de ilustrar essa prática são as próprias ferramentas disponibilizadas pelo Google, que entre elas, podemos citar o G-mail, Google Maps e Youtube, por exemplo. Todas estas são ferramentas, a priori, gratuitas. Entretanto, o usuário paga com seus dados e informações, que são repassadas para anunciantes que remuneram o Google através de investimento em publicidade por meio do Google Ads[121].

É nesse contexto que nasce a figura do *prosumer*, onde o usuário passa a ter uma participação ativa e não mais uma posição passiva no ciclo do consumo. Com suas informações nas redes sociais, pode-se criar e distribuir publicidade de forma segmentada, ou seja, ele não apenas consome (*consumption*), mas também produz o bem de consumo (*production*): *prosumer*[122].

Ademais, é somente através desse monitoramento por meio dos *cookies* que se torna possível realizar uma publicidade direcionada, cuja prática visa personalizar, ainda que de

---

[119] LINS, Bruna R.; QUINELATO, Pietra D. Redes sociais à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Social Media Law: O Direito nas Redes Sociais.** São Paulo: Thomson Reuters Brasil, 2021. p. 149-150.

[120] Para acessar uma imagem da página inicial do Facebook no ano de 2018, recorremos ao site *Way Back Machine*. Disponível em: https://web.archive.org/web/20180501001849/https://www.facebook.com/. Acessado em 30.03.2022.

[121] Inclusive, em fevereiro de 2022, a *Alphabet*, dona do Google, divulgou seus resultados para acionistas informando uma receita de 257 bilhões de dólares e lucro líquido de 76 bilhões, tendo como impulsionador destes valores a venda de publicidade. https://abc.xyz/investor/static/pdf/2021Q4_alphabet_earnings_release.pdf. p. 1-2. Acessado em 03.04.2022

[122] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

forma parcial, a comunicação entre anunciantes — que remuneram as empresas como Facebook e Google através do investimento em publicidade — e usuários[123].

Os dados dos consumidores possuem, portanto, grande relevância para a chamada economia da informação pessoal, onde grandes empresas tomam decisões baseadas em refinadas análises acerca da renda, preferências e comportamentos dos seus clientes[124].

Dessa forma, o modelo de marketing sofreu uma "customização", passando de um marketing de massa — em que o alvo era um consumidor médio, anônimo, que recebia todos os tipos de publicidade, sem qualquer distinção —, para um marketing individualizado, agora tendo como alvo um tipo de consumidor individualizado, podendo-se oferecer um produto específico e personalizado, além de poder atingi-lo por diversas vias[125], e quantas vezes forem necessárias através do *remarketing*.

Nesse sentido, os dados pessoais do consumidor servem como objeto para o marketing direto e publicidade direcionada, a fim de atingir as seguintes finalidades do mercado: i) previsibilidade e diminuição dos riscos, ii) interação com o consumidor, iii) diferenciação de produtos e iv) diferenciação de serviços[126].

O marketing direto está relacionado ao consumidor que já possui ou possuiu uma relação contratual com a empresa. Nesse caso, a partir do histórico de compras desse consumidor, seria possível direcionar anúncios publicitários condizentes ao seu padrão de consumo[127], tornando o investimento em publicidade muito menor para a empresa, uma vez que ela já possui informações mais precisas acerca consumidor. Ademais, de acordo com autores como Bruno

---

[123] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[124] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 84.

[125] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 87-88.

[126] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p. 89.

[127] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

Bioni[128], Mario Viola e Chiara de Teffé[129], para o marketing direto aplica-se a base legal do legítimo interesse, sendo inclusive apontado na *General Data Protection Regulation - GDPR*[130].

Por outro lado, a publicidade direcionada subdivide-se em publicidade contextual, segmentada e comportamental. A publicidade contextual está relacionada com a temática de um determinado ambiente, ou seja, focada no aspecto subjetivo, não importando se o conteúdo estará em um ambiente *offline* ou *online*, desde que a mensagem esteja de acordo com o contexto em que o consumidor está inserido[131]. Já na publicidade segmentada, o foco está no público-alvo do bem ofertado, ou seja, se o produto é destinado ao público feminino, com determinada idade, a abordagem será realizada em um ambiente em que essa audiência seja predominante. Por fim, a publicidade comportamental, em que o foco está nas preferências dos usuários, a partir de seus dados de navegação. Esse formato de publicidade permitiu uma personalização ainda maior entre compradores e vendedores, sendo, mais efetiva se comparada com as anteriores[132].

Para contextualizar a eficácia da publicidade direcionada, Joana Varon realizou diversos experimentos com propagandas no Facebook, onde foi possível alcançar usuárias com um grau de especificidade e então direcionar mensagens publicitárias customizadas[133]. Entre as mensagens publicitárias criadas pela equipe de Varon, podemos destacar uma em que mostra uma mulher com uma moto e um buquê de flores na bolsa — a fim de representar uma pessoa,

---

[128] BIONI, Bruno. Legítimo Interesse: Aspectos Gerais a Partir de uma Visão Obrigacional. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. E-book.

[129] VIOLA, Mario; TEFFÉ, Chiara S. de. Tratamento de dados pessoais na LGPD: Estudo sobre as bases legais dos artigos 7º e 11. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. Digital..

[130] O considerando 47 da GDPR aponta o marketing direto como uma das possíveis aplicações do legítimo interesse: "*The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest*". Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acessado em 05.04.2022.

[131] A título de exemplo, Bruno Bioni apresenta a seguinte passagem: "Por exemplo, há uma maior probabilidade de que leitores de revistas de carros tenham interesse na aquisição de tal bem, já que se subentende que quem está pesquisando sobre o assunto tende a ser um potencial comprador." BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[132] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[133] O experimento dirigido pela Joana Varon: "Você está vendo isso porque é uma...". https://chupadados.codingrights.org/gendered-targeted-ads/. Acessado em 06.04.2022.

do sexo feminino, que possui interesse em motos e que está em um relacionamento à distância. Dessa forma, com uma publicidade paga e direcionada, o experimento atingiu centenas de mulheres que, em seus comentários, afirmavam que a publicação havia "acertado em cheio".

O experimento apresenta diversos questionamentos acerca do nível de detalhes que se pode encontrar no Gerenciador de Anúncios do Facebook, que somente é possível em razão dos dados fornecidos pelos usuários — que usam a rede social "gratuitamente".

A publicidade comportamental, que é o meio de personalizar a mensagem com base no monitoramento das atividades *online* do consumidor, pode acarretar inúmeros riscos à personalidade, e tem como pressuposto de legitimidade o consentimento do usuário, que deve ser, portanto, informado, expresso, específico e anterior, nos moldes do sistema *opt-in*[134].

3.3 A INSUFICIÊNCIA DO CONSENTIMENTO NA PROTEÇÃO DE DADOS

Como pode-se perceber, o desenvolvimento tecnológico culminou em uma hiperconexão em vários aspectos da vida na sociedade, onde a capacidade do tratamento de dados tornou-se um diferencial produtivo e de competividade entre agentes econômicos[135]. Nesse cenário, o consumidor não mais paga diretamente pelo bem de consumo através de uma prestação pecuniária, mas sim com seus dados pessoais e informações para entrega de publicidade direcionada, em uma economia que tem como cerne a vigilância[136].

Se no início da década de 1980 a preocupação para o tratamento dos dados pessoais estava na vigilância ostensiva do Estado — o que nos leva a figura sólida do Grande Irmão, do romance de George Orwell[137] —, que como vimos em capítulo anterior, fez com que a Corte Constitucional Alemã se tornasse referência fundamental a partir de uma decisão no campo da

---

[134] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Editora Saraiva, 2014 p.225.

[135] HILÁRIO, Dânton.; GONÇALVES, Luís Felipe; VALASKI, Luís Henrique. Consentimento e legítimo interesse como hipóteses de tratamento de dados pessoais na Lei Geral de Proteção de dados: Paradoxos e convergências. **Revista da Comissão de Inovação e Gestão da OAB/PR**, [*s. l.*], v. III, p. 266–290, 2021.

[136] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[137] Como aponta Danilo Doneda, "Em primeiro lugar, foi o Estado que por primeiro se encontrou na posição de utilizar largamente informações pessoais", sob o argumento de tornar a administração pública mais eficiente através do conhecimento da população. DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 34-37.

proteção de dados[138], hoje, essa vigilância já desgastada, diluiu-se pela multiplicação de Pequenos Irmãos, em uma economia composta por diversos atores, cujo modelo de negócio é o de vigiar cidadãos-potenciais consumidores. Nesse sentido, a vigilância não é mais centralizada, mas sim descentralizada, através dos "*tiny brothers"*[139].

Outrossim, são os pequenos pedaços de informações agregados por atores de uma rede complexa — cujo objetivo é desenvolver um perfil mais preciso dos hábitos do consumidor — que tornam o fluxo informacional imprevisível, interminável e de difícil determinação, ou seja, algo completamente volátil. Em consequência disso, o titular dos dados deveria ter consciência a respeito de todos esses atores e de suas respectivas práticas quanto à mineração de dados, a fim de gerenciar as suas informações pessoais[140].

Neste sentido, imperioso destacar que o consentimento do titular dos dados pessoais é um ponto sensível no que tange à disciplina da proteção de dados, pois, é por meio dele que o direito civil pode estruturar, através da consideração da autonomia da vontade, a circulação e tratamento desses dados[141].

Ademais, o consentimento pode ser considerado como uma das principais bases legais para o tratamento de dados pessoais, uma vez que a LGPD tem o titular dos dados como centro gravitacional. Como bem aponta Bruno Bioni,

> "é uma carga principiológica que procura conformar, justamente, a ideia de que o titular dos dados pessoais deve ser empoderado com o *controle* de suas informações pessoais, e, sobretudo, na sua autonomia da vontade"[142].

Entretanto, esse consentimento é colocado em xeque quando visualizado o complexo fluxo informacional, onde existe uma série de atores envolvidos para operar os modelos de negócios baseados na publicidade direcionada. Os dados pessoais trafegam por inúmeros

---

[138] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 170.

[139] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book..

[140] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[141] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 310.

[142] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

"parceiros comerciais", presentes nas políticas de privacidade, que ao fim e ao cabo são quem viabilizam e monetizam os "negócios gratuitos"[143]. Assim, parcela significativa da literatura tem ressaltado as insuficiências do consentimento na tarefa de tutelar a privacidade e proteção dos dados pessoais dos cidadãos[144].

3.3.1 Da limitação cognitiva do usuário frente à complexidade do fluxo informacional

A primeira insuficiência enfrentada pelo consentimento está relacionada com o próprio titular dos dados e o processo cognitivo para a tomada de decisão. Nesse ponto, destaca Laura Schertel,

> "É que, sob tal ótica, esse indivíduo é guiado pela maximização de seus interesses em face dos custos e benefícios envolvidos em consentir, ou não, com os termos que lhe são apresentados. Assim, caso esteja munido de amplo conhecimento acerca do que é feito com seus dados pessoais, poderá sopesar os custos envolvidos para sua personalidade e contrapô-los diante dos benefícios trazidos, por exemplo, pela utilização de um serviço on-line".[145]

Nessa perspectiva, o usuário, após ler os termos de privacidade, por exemplo, poderá tomar uma decisão sobre o que consentir e o que não consentir na internet, tendo em consideração o seu melhor interesse.

No entanto, como já vimos, a economia informacional é composta por inúmeros atores, o que torna impossível — dada a racionalidade limitada do ser humano — absorver, memorizar e processar todas as informações relevantes para a tomada de decisão[146]. Evidentemente, não se trata de "infantilizar" o titular dos dados, como se fosse um incapaz de decidir por si mesmo, ou ignorar sua capacidade racional[147], mas sim de destacar a dificuldade de tomar uma decisão

---

[143] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[144] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, [*s. l.*], v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521.

[145] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, [*s. l.*], v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521.

[146] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[147] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, [*s. l.*], v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521.

coerente sem conseguir compreender quem são os diversos atores da rede, quais são e como são tratados seus dados, com base nas políticas de privacidade de cada um desses atores[148].

A fim de exemplificar essa dificuldade de racionalização do usuário, podemos utilizar o mercado de infoprodutos[149], que teve sua força impulsionada pelos impactos da pandemia desde o início de 2020[150]. Nesse caso, um usuário pode chegar até uma página de determinado produto, seja por meio de um anúncio[151], seja por meio de pesquisa, onde terá que informar seus dados para fazer o *download* "de forma gratuito"[152], ou então informar seus dados para efetuar uma compra.

Nesse sentido, o usuário que está informando seus dados para o *download* "gratuito", por exemplo, está fornecendo seus dados não apenas para o produtor que está lhe oferecendo o produto, mas sim para uma rede mais complexa de atores[153].

De igual modo, com um exemplo prático, é possível observar que em alguns casos, o usuário que efetua uma compra online também tem seus dados compartilhados com terceiros, sem dar seu consentimento para tanto. A fim de demonstrar essa prática, bastante comum no

---

[148] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[149] Infoprodutos são produtos digitais, criados e disponibilizados exclusivamente no meio digital, ou seja, eles precisam estar na internet. Estes produtos são desenvolvidos a partir do conhecimento prévio de seu produtor e contém informações com o objetivo de resolver um problema específico, agregando valor a vida do ser humano. São exemplos de infoprodutos: *e-books*, videoaulas, *audiobooks*, *membership* (site com área exclusiva para membros). COSTA, Ana C.; SILVA, Monique de A. O comportamento do consumidor de infoproduto. ***Research, Society and Development***, v. 10, n. 3, p. 1–6, 2021. Disponível em: https://doi.org/10.33448/rsd-v10i3.12874. Acessado em 08.04.2022.

[150] Procura por cursos online aumentam na pandemia. Disponível em https://ecommercedesucesso.com.br/cursos-online-pandemia. Acessado em 08.04.2022.

[151] Aqui, o usuário já está sendo impactado pela utilização de suas informações. Como vimos no experimento de Joana Varon, o anunciante possui um acervo de interesses e informações a fim de atingir um público específico, tudo com base nas informações "consentidas" pelo usuário para usar a rede social ou acessar sites na internet.

[152] Importante destacar que o gratuito está relacionado ao não pagamento pecuniário pelo produto, mas, que está sendo pago com seus dados pessoais, aqui informados de forma ativa pelo usuário.

[153] É dessa forma que o pixel do Facebook funciona, por exemplo. Para que o Gerenciador de Anúncios consiga direcionar os anúncios de forma eficaz para "mulheres que curtem motos e estão em um relacionamento à distância", como no experimento de Joana Varon, ele precisa captar as informações do usuário em sites visitados por este. Assim, ao efetuar o cadastro e fazer o *download*, o Facebook compreende, através de um evento denominado "Conversão", que aquele usuário possui interesse por aquele tipo de produto ou negócio. Disponível em: https://pt-br.facebook.com/business/help/742478679120153?id=1205376682832142. Acessado em 08.04.2022.

mercado de infoprodutos, acessamos o site de um produto digital disponível na Hotmart[154], denominado "Curso Escola Desginer de Unhas"[155], onde estão disponíveis diversos links para o usuário efetuar a compra do produto, que, quando clicados, redirecionam o usuário para a página de *checkout* da plataforma da Hotmart.

A primeira questão relevante do acesso à página é que ela não solicita o consentimento do usuário para o uso de cookies, que, em uma simples inspeção[156], é possível observar o uso de cookies primários e de terceiros (*first-party cookies* e *third-party cookies*), tais quais do Youtube, Facebook e da plataforma de chat Jivo.

Em um segundo momento, e ainda mais grave, o usuário que efetua a compra do produto, e, consequentemente, fornece dados que permitem sua imediata identificação — como nome e e-mail, por exemplo —, tem os mesmos divulgados pelo produtor do curso para terceiros totalmente estranhos à relação contratual entre empresa e comprador[157].

Essa prática é bastante comum no chamado "mercado de afiliados"[158], no qual tanto pessoas físicas quanto jurídicas podem se afiliar a um produto digital e realizar sua divulgação através de um link específico e receber uma comissão em razão da venda.

Entretanto, para tornar o custo com a publicidade direcionada mais baixo, a empresa que disponibiliza o curso divulga uma lista com os e-mails de todos os compradores, a fim de que os afiliados consigam criar os chamados "públicos semelhantes"[159] ou "público *lookalike*" no Gerenciador de Negócios do Facebook, e assim, alcançar entre os usuários da rede social,

---

[154] A Hotmart é uma das plataformas digitais mais conhecidas, que hoje conta com 26 milhões de usuários cadastrados entre produtores, vendedores afiliados e consumidores de conteúdo online em todo o mundo. Além do número de usuários, a startup brasileira criada em 2011 recebeu um investimento de 735 milhões de reais em 2021. Disponível em: https://veja.abril.com.br/blog/radar/com-26-milhoes-de-usuarios-no-mundo-a-hotmart-avanca-no-brasil/. Acessado em 08.04.2022.

[155] A página de vendas do produto está disponível em: https://unhasprofissionais.com/. Acessado em 08.04.2022.

[156] A inspeção pode ser realizada seguindo o passo a passo disponível em: https://www.thefastcode.com/pt-eur/wiki/Ver-os-Cookies. Acessado em 08.04.2022.

[157] A lista de e-mails dos consumidores que efetuaram a compra do produto está disponível em: https://drive.google.com/drive/folders/1TjAlI_Tto4UhTVZezYIXub0bEdD_qpGj. Acessado em 08.04.2022.

[158] Para saber mais sobre o mercado de afiliados, a Hotmart disponibilizou um artigo em seu site, disponível em: https://blog.hotmart.com/pt-br/o-que-e-um-programa-de-afiliados/. Acessado em 08.04.2022.

[159] Segundo o próprio Facebook, "o público semelhante é uma forma de os seus anúncios alcançarem novas pessoas que podem gostar da sua empresa por terem características parecidas com os clientes atuais". Disponível em: https://pt-br.facebook.com/business/help/164749007013531. Acessado em 08.04.2022.

potenciais consumidores que possuem gostos e interesses parecidos com os dos compradores. Em resumo, o consumidor tem seus dados vazados para pessoas estranhas, a fim de que suas informações sejam úteis para o aumento das vendas do mesmo produto adquirido.

Em uma leitura atenta da política de privacidade disposta na página do produto não é possível encontrar qualquer informação acerca do compartilhamento dos dados do usuário com terceiros com a finalidade de publicidade direcionada[160].

Não obstante, ainda que relevante a apresentação de informações acerca do tratamento de dados, estudos apontam que para a tomada de decisões sobre sua privacidade e seus dados, os usuários sequer leem regularmente as "políticas de privacidade" ou os "termos de uso de dados" que são apresentados nos sites, tornando tal medida inócua[161].

Em um estudo recente conduzido pela Universidade de Bochum, na Alemanha, constatou-se um aumento de 45% na adoção dos chamados avisos de *cookies* por parte dos sites no cenário pós-GDPR[162]. Em síntese, os avisos de *cookies* são banners em formato de *pop-up*[163] informando acerca da coleta de dados através dos *cookies*, geralmente indicando quais são os *cookies* presentes no site com um link redirecionando o usuário para a página de política de privacidade.

A pesquisa selecionou uma amostra aleatória de 1.000 (um mil) avisos de *cookies* de sites de um estudo anterior. Além disso, os pesquisadores escolherem oito variáveis para análise manual nos respectivos avisos, a fim de realizar três experimentos[164].

---

[160] Política de privacidade da página "Curso Escola Designer de Unhas", disponível em: https://unhasprofissionais.com/privacidade/. Acessado em 08.04.2022.

[161] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, [*s. l.*], v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521.

[162] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[163] *Pop-up* são janelas que abrem na tela do dispositivo com alguma informação, que pode variar entre promoção de produto, convite para se cadastrar na lista de e-mails do site, entre outras.

[164] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

No primeiro experimento observou-se que os avisos estavam alocados em mais de 91,8% das vezes no topo ou no final da plataforma, dificultando sua visualização, além de não bloquear o conteúdo da página, o que acarretava em uma baixa taxa de cliques.

O segundo experimento, de acordo com Bruno Bioni:

> "constatou que tal tecnologia não causava interação no usuário, porque: i) na grande maioria das vezes, não lhe franqueava qualquer tipo opção senão a aceitação do uso dos seus dados; ii) quando havia opções, essas eram limitadas a ele aceitar ou não o uso de cookies. Uma lógica binária que não lhe informava os vários usos possíveis com os seus dados; iii) quando havia várias opções (e.g., analytics, marketing110), os avisos dificultavam o exercício de uma escolha genuína de sua parte, sendo: iii.a) as opções pré-marcadas, de modo que, por padrão, o usuário autorizava o processamento de seus dados; iii.b) as opções em não aceitar o uso de cookies ou aceitá-los com restrições não eram destacadas com cores que as realçavam; iii.c) a aceitação do uso de cookies com restrições demandavam uma série de cliques, não sendo, muitas vezes, tais opções apresentadas na primeira tela da notificação."[165]

Por fim, o terceiro experimento tratou acerca da linguagem dos avisos, onde percebeu-se que os usuários não compreendem a linguagem aplicada, de forma que: a) o próprio termo "*cookies*" é técnico e seu significado não é tão difundido; e b) alguns entrevistados não compreendem as implicações de suas escolhas, acreditando, por exemplo, que a recusa desses *cookies* impediria o acesso ao site[166].

No mesmo sentido, tem-se outro experimento[167], chamado "*The Biggest Lie on the Internet: Igonoring the Privacy Policies and Terms of Service Policies of Social Networking Services*", conduzido em 2020 pelos pesquisadores Jonathan Obar, da York University, e Anne Oeldorf-Hirsch, da Universidade de Connecticut, onde o objetivo era analisar o comportamento do usuário quanto a leitura da política de privacidade e termos de serviços em uma rede social fictícia chamada "*NameDrop"*.

Para isso, os pesquisadores criaram uma política de privacidade, cuja leitura levaria, aproximadamente, 30 minutos, e um termo de serviços que demandaria 15 minutos de leitura.

---

[165] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[166] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[167] OBAR, Jonathan A.; OELDORF-HIRSCH, Anne. *The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services.* **Information, Communication & Society**, [*s. l.*], v. 23, n. 1, p. 128–147, 2020. Disponível em: https://doi.org/10.1080/1369118X.2018.1486870.

Ademais, os pesquisadores incluíram duas armadilhas nas cláusulas dos termos de serviços, entre elas:

> "2.3.1 Tipos de pagamento (cláusula de atribuição de filho) [...] Além de qualquer pagamento monetário que o usuário pode fazer para NameDrop, concordando com estes Termos de Serviço, e em troca do serviço, todos os usuários deste site concordam em ceder imediatamente seus filhos primogênitos para NameDrop Inc. Se o usuário ainda não tiver filhos, este contrato será executável até o ano de 2050. Todos os indivíduos atribuídos à NameDrop tornam-se automaticamente propriedade da NameDrop, Inc. Sem exceções"[168]

Diante disso, os pesquisadores chegaram aos resultados onde 74% dos participantes não leram nenhum dos dois documentos, optando por clicar rapidamente em participar da rede social. No que tange às armadilhas, 98% dos participantes não perceberam que, ao consentir com aqueles termos, eles estavam concordando em renunciar aos direitos de seu filho primogênito para participar da rede social[169].

Nessa perspectiva, o próprio consentimento individual é incapaz de corresponder à vontade real do titular dos dados, uma vez que esse sequer compreende os efeitos que a sua escolha poderá causar aos seus direitos de personalidade[170].

3.3.2 Da desigualdade entre as partes e a lógica do "*take it or leave it*"

A segunda insuficiência do consentimento está na desconsideração da assimetria de poderes na relação entre o titular dos dados e os agentes responsáveis pelo tratamento desses dados[171]. Como bem pontua Danilo Doneda:

---

[168] Tradução livre: "*2.3.1 Payment types (child assignment clause): In addition to any monetary payment that the user may make to NameDrop, by agreeing to these Terms of Service, and in exchange for service, all users of this site agree to immediately assign their first-born child to NameDrop, Inc. If the user does not yet have children, this agreement will be enforceable until the year 2050. All individuals assigned to NameDrop automatically become the property of NameDrop, Inc. No exceptions*". OBAR, Jonathan A.; OELDORF-HIRSCH, Anne. *The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services.* ***Information, Communication & Society***, v. 23, n. 1, p. 128–147, 2020. Disponível em: https://doi.org/10.1080/1369118X.2018.1486870. p. 12.

[169] OBAR, Jonathan A.; OELDORF-HIRSCH, Anne. *The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services.* ***Information, Communication & Society***, v. 23, n. 1, p. 128–147, 2020. Disponível em: https://doi.org/10.1080/1369118X.2018.1486870. p. 02.

[170] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521

[171] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521.

> "O confronto com situações reais revela que, em tais situações, a alternativa a não revelação dos dados pessoais pelo seu titular costuma ser uma — por vezes, brutal — renúncia a determinados bens ou serviços. A disparidade de meios e de poder entre a pessoa de quem é demandado o consentimento para utilização dos dados pessoais em contemplação da realização de um contrato e aquele que os pede faz com que a verdadeira opção que lhe reste seja, tantas vezes, a de "tudo ou nada, "pegar ou largar".[172]

Nesse sentido, pode-se citar o cadastro e utilização das redes sociais, aplicativos e até mesmo a condição de realizar o download de um produto anunciado como gratuito através de publicidade direcionada — caso do exemplo do mercado de infoprodutos citado anteriormente —, mas que ao fim e ao cabo, o não consentir resulta na negativa de desfrutar de tal serviço ou produto.

Esse tipo de negócio está baseado em uma lógica binária "*take it or leave it"*, consentir ou não consentir, sem outras opções[173]. De igual maneira, essa problemática foi abordada no artigo "*The crisis of consent: How stronger legal protection may lead to weaker consent in data protection*", em que os autores identificaram a falta de uma escolha significativa para o titular dos dados:

> "embora os titulares dos dados sejam confrontados com um pedido de consentimento, muitas vezes há uma ausência significativa de escolha para eles. Em geral, os titulares dos dados buscam acessar (*e.g*, notícias, redes sociais, pesquisas) e, em troca do acesso aos serviços, "permitem" o tratamento de seus dados pessoais. Esses serviços online, em particular, gratuitos, geralmente oferecem pouco ou nenhum espaço para negociação, pois o uso dos dados pessoais é vital para o sucesso do seu modelo de negócios"[174].

Nessa lógica, percebe-se que mesmo estando exposto a tamanhos riscos, o usuário pode acabar consentindo com o tratamento de seus dados pessoais em troca de proveitos, tais como: conexão com amigos ou familiares através das redes sociais, acesso a informações e meios de comunicação em tempo real. Como aponta Laura Schertel, esse consentimento é, na grande

---

[172] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil 2021. p. 312.

[173] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521.

[174] Tradução livre: "*while data subjects are confronted with a consent request, there is often an absence of meaningful choice for them. In general, data subjects seek to access a service (e.g. news, social networking, search) and in exchange for accessing the service they 'allow' the processing of their personal data. These online services, in particular free services, usually provide little to no room for negotiation, because the use of the personal data is vital for the success of their business model*". SCHERMER, Bart W.; CUSTERS, Bart; VAN DER HOF, Simone. *The crisis of consent: How stronger legal protection may lead to weaker consent in data protection*. ***Ethics and Information Technology***, v. 16, n. 2, p. 171–182, 2014. Disponível em: https://doi.org/10.1007/s10676-014-9343-8. p.11-12. Acessado em 08.04.2022.

parte do tempo, meramente aparente, sendo questionável sua contribuição para a proteção dos dados pessoais[175].

Há, portanto, que se levar em consideração a existência de uma assimetria quanto ao poder de barganha entre as partes. Sobre isso, oportuno mencionar o entendimento de Tepedino e Teffé:

> "uma parte, geralmente grandes empresas e Estados, detém mais poder, recursos e melhores informações do que a outra, o cidadão comum, por vezes consumidor nas relações desenvolvidas. Esse cenário enseja diversos questionamentos acerca, por exemplo, da validade do consentimento do titular dos dados nos contratos celebrados, principalmente quando eles são de adesão. Tal assimetria informacional não se revela apenas no poder que o agente dispõe sobre os dados pessoais de terceiros, mas também nas novas modalidades de negócio, em que informações pessoais de seus usuários representam uma das bases centrais do sistema desenvolvido.
>
> A posição de destaque que o tratamento de dados tem em muitos produtos e serviços oferecidos ao público por empresas de tecnologia – as quais, por vezes, não exigem remuneração direta dos usuários, mas o preenchimento de cadastro, a criação de perfil e/ou o acesso aos contatos e mensagens trocadas – revela a importância fundamental dos dados na criação, desenvolvimento e manutenção de diversos modelos de negócio da Web 3.0.".[176]

Não obstante, a existência dessa assimetria foi tema de uma pesquisa empírica da Faculdade de Comunicação Annenberg, da Universidade da Pensilvânia[177]. Esse estudo refuta o discurso da indústria publicitária de que os consumidores estariam confortáveis e conscientes em conceder seus dados pessoais em troca dos serviços e produtos "gratuitos".

Em síntese, a pesquisa apresenta dados em que 84% das pessoas entrevistadas gostariam de ter controle sobre o que é feito com seus dados pessoais, bem como, 65% dos entrevistados reconhecem que possuem pouco controle sobre o que pode ser feito com suas informações pessoais — uma vez que são submetidos a lógica do *trade-off*, em que ocorre a troca dos dados pessoais para o acesso a determinados produtos e serviços. Assim, foi possível concluir que os

---

[175] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, [*s. l.*], v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521.

[176] TEPEDINO, Gustavo; TEFFÉ, Chiara S. de. O consentimento na circulação de dados pessoais. **Revista Brasileira de Direito Civil**, v. 25, n. 03, p. 83–116, 2020. Disponível em: https://doi.org/10.33242/rbdc.2020.03.005. p. 89-90.

[177] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

consumidores estão *resignados*[178] com essa dinâmica, desejando um maior controle do uso de seus dados pessoais, porém reconhecendo, ao mesmo tempo, que têm pouca gerência sobre tal situação[179].

Por derradeiro, forçoso observar que esse é o cenário em que o consentimento é uma mera ficção, tendo em vista que o usuário carece de efetiva autonomia para decidir como e quando se proteger de possíveis perigos e danos à sua personalidade, conforme apontam Schertel e Fonseca citando Spiros Simitis[180].

3.3.3 Da impossibilidade do gerenciamento individual dos riscos durante a coleta dos dados pessoais

Como pode se observar ao longo desse trabalho, é a partir dos dados pessoais que são extraídas informações relevantes que formarão a representação virtual do indivíduo na sociedade. Assim, uma terceira insuficiência do consentimento está no fato da impossibilidade de se oferecerem respostas aos desafios decorrentes da "massificação da produção, coleta, armazenamento, tratamento e compartilhamento de dados pessoais"[181].

Dessa forma, o tratamento dos dados pessoais não pode ser visto como algo estático, com sua utilidade exaurida no momento em que alcançada sua finalidade pela qual foram coletados. Pelo contrário, através de novas tecnologias — como as que se utilizam de *Big Data*, A.I e algoritmos — é possível se obter novas informações acerca daqueles dados que foram coletados para outra finalidade[182]. Para tanto, toma-se de exemplo o caso da Cambridge

---

[178] Segundo o autor, essa resignação significa que as pessoas estariam acatando algo que consideram indesejável, mas que é, ao mesmo tempo, inevitável. BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[179] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book

[180] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, [*s. l.*], v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521.

[181] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, [*s. l.*], v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521.

[182] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, [*s. l.*], v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521.

Analytica, que usou informações a partir dos dados coletados em um teste de personalidade para afetar o regime democrático, conforme já mencionado anteriormente.

Sobre esse ponto, referem Laura Schertel e Gabriel Fonseca que:

> "o fluxo desses dados perpassa por uma complexa rede de atores que os utilizam por meio de práticas e de operações com fins diversos. É impossível que o titular de dados tenha conhecimento prévio de todos esses elementos não só por limitações de cognição, mas também por questões estruturais. É dizer: seja pela escala em que a informação é processada, seja pela enorme capacidade de agregação da informação pelas novas tecnologias, é improvável que o indivíduo, no momento da coleta, gerencie plenamente algo que ocorrerá no futuro e que envolve inúmeras incertezas acerca de como todas as informações e dados acerca de um indivíduo serão agregados, cruzados ou utilizados"[183].

Nessa perspectiva, se torna impossível que o usuário tenha um conhecimento prévio acerca de como seus dados serão tratados e usados, não só por limitação cognitiva, mas também por problemas estruturais impostas pela economia informacional[184], quais sejam: problema da escala, problema da agregação e problema de avaliação de danos.

O problema da escala consiste na dificuldade que o usuário tem em gerenciar sua privacidade no emaranhado de sites que visita[185], ou seja, ainda que a empresa apresente uma política de privacidade transparente e de fácil compreensão, o problema está na impossibilidade de o usuário manter um controle sobre o que e onde consentiu.

Por sua vez, o problema da agregação está relacionado ao que chamamos de mineração de dados. Nesse sentido, ainda que o usuário tenha o mínimo de cuidado com a sua privacidade,

---

[183] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, [*s. l.*], v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521.

[184] SOLOVE, Daniel J. *Introduction: Privacy self-management and the consent dilemma.* **Harvard Law Review**, v. 126, n. 7, p. 1880–1903, 2013. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018. p. 1888-1889. Acessado em 11.04.2022.

[185] De acordo com o autor, só nos EUA o usuário médio visita quase uma centena de sites por mês e faz negócios online e offline com inúmeras empresas. Ademais, é bem provável que esse número tenha se multiplicado com o passar dos anos e aumentado consideravelmente durante a pandemia da COVID-19. SOLOVE, Daniel J. Introduction: *Privacy self-management and the consent dilemma.* **Harvard Law Review**, v. 126, n. 7, p. 1880–1903, 2013. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018. p. 1888. Acessado em 11.04.2022.

ao compartilhar seus dados com inúmeras empresas e diversos sites, a combinação desses dados dispersos pela rede podem revelar fatos sensíveis sobre a pessoa[186].

Por derradeiro, o problema de avaliar danos possui relação com a análise custo-benefício. Nesse caso, o problema está no fato de que as pessoas geralmente favorecem benefícios imediatos, mesmo quando podem sofrer um prejuízo no futuro[187].

[186] SOLOVE, Daniel J. *Introduction: Privacy self-management and the consent dilemma.* ***Harvard Law Review***, v. 126, n. 7, p. 1880–1903, 2013. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018. p. 1889-1890. Acessado em 11.04.2022.

[187] SOLOVE, Daniel J. *Introduction: Privacy self-management and the consent dilemma.* ***Harvard Law Review***, v. 126, n. 7, p. 1880–1903, 2013. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018. p. 1891. Acessado em 11.04.2022.

4 DA INSUFICIÊNCIA DO TERMO DE CONSENTIMENTO À ADOÇÃO DE NOVAS ALTERNATIVAS

Ao longo do trabalho observarmos o progresso geracional das leis de proteção de dados e como o consentimento obteve uma gradual adjetivação como sendo inequívoco, expresso, informado, específico ou livre[188]. Nesse sentido também é possível observar o surgimento das "políticas de privacidade" e "termos de uso" como uma resposta regulatória, a fim de colher esse consentimento para legitimar o tratamento de dados do usuário.

Contudo, diversos são os apontamentos no sentido da insuficiência desse consentimento, que, na maior parte do tempo, é meramente aparente, uma vez que há uma limitação cognitiva do usuário, desigualdade entre as partes, e, quando não esses dois problemas, a impossibilidade do gerenciamento dos riscos durante a coleta de dados pessoais.

Nessa perspectiva buscaremos apresentar algumas alternativas a fim de reduzir essa debilitada regulação por meio da adjetivação do consentimento, que, até o momento mostra-se artificial[189].

4.1 A POSSÍVEL ADOÇÃO DA PRIVACY ENHANCING TECHNOLOGIES

Há muito, diversos autores já mencionam as ferramentas tecnológicas que visam facilitar as configurações de privacidade, denominadas "*Privacy Enhancing Tecnologies*" – PETs, que dão concretude à metodologia "*Privacy by Design*"[190].

Essa é a ideia de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviço, tornando primordial a inclusão de tecnologias que facilitem o controle e a proteção das informações pessoais por parte do usuário. Em outras palavras, as PETs apresentam-se como uma possível solução para resolver ou diminuir as assimetrias entre as

---

[188] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[189] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[190] HILÁRIO, Dânton.; GONÇALVES, Luís Felipe; VALASKI, Luís Henrique. Consentimento e legítimo interesse como hipóteses de tratamento de dados pessoais na Lei Geral de Proteção de dados: Paradoxos e convergências. **Revista da Comissão de Inovação e Gestão da OAB/PR**, [*s. l.*], v. III, p. 266–290, 2021.

partes, uma vez que seriam capazes de empoderar os cidadãos com um melhor controle sobre seus dados[191].

Nesse contexto, a *Plataform for Privacy Preferences*/P3P — Plataforma para Preferência de Privacidades poderia ser um mecanismo capacitador, conforme ressalta Bruno Bioni:

> "Desenvolvida e recomendada desde os idos de 2002 pela W3C205, o usuário poderia, por intermédio de seu navegador, configurar as suas mais variadas preferências de privacidade, incluindo, por exemplo, quais tipos de dados pessoais poderiam ser coletados (geolocacionais, sensíveis ou não sensíveis etc.) e, até mesmo, se ele assentiria o seu compartilhamento com terceiros. Portanto, o próprio browser procederia a uma análise automatizada das políticas de privacidade das aplicações acessadas, verificando-se a sua (in)compatibilidade com as preferências de privacidade pré-configuradas".[192]

Em síntese, a P3P tornaria possível a configuração manual das preferências de privacidade do usuário através do navegador, de modo que o mesmo pudesse delimitar o tratamento de seus dados sem a necessidade de leitura de cada política de privacidade presente em cada site. Dessa forma afastar-se-ia a lógica do "tudo" ou "nada" por uma autorização "granular" do usuário no que tange à utilização de seus dados pessoais[193].

Contudo, a ferramenta P3P mostrou-se também inexecutável, pois, para tanto, seria necessária a adoção da ferramenta por parte dos navegadores, além de tornar todas as políticas de privacidade em um formato legível com a leitura automatizada dos termos[194].

Não obstante a negativa de utilização da ferramenta P3P, outra tecnologia que merece destaque no que tange à proteção de dados pessoais é o *Google Dashboard*, que funciona como

---

[191] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[192] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[193] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

[194] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019. p. E-book.

uma espécie de "central de gerenciamento" para o usuário, e busca esclarecer, de forma acessível e concentrada, o modo como a empresa utiliza esses dados pessoais armazenados[195].

Ademais, essa alternativa do *Google Dashborad* possibilita que o usuário faça o download de seus dados, observe quais são os serviços do Google que estão sendo usados — e, consequentemente, tratando seus dados —, bem como permite a exclusão de um serviço específico como Youtube, G-mail, Google Fotos, Agenda, Google Maps, Google Drive e tantos outros[196].

Nessa perspectiva, o *Google Dashboard* se mostra uma ferramenta bastante útil tanto para usuários que possuem algum conhecimento técnico como para usuários que não possuem conhecimento alguma sobre como seus dados são tratados na internet.

4.2 VISUAL LAW PARA UMA FÁCIL COMPREENSÃO DAS POLÍTICAS DE PRIVACIDADE

A limitação cognitiva é uma das grandes problemáticas, que torna o consentimento insuficiente para o tratamento de dados pessoais, uma vez que, como observado no tópico 3.3.1, muitos usuários sequer leem as "políticas de privacidade" ou "termos de serviços/uso dos sites".

Nesta senda, a aplicação de técnicas de *visual law* poderia ser considerada como uma alternativa para essa dificuldade do usuário em compreender os documentos e termos jurídicos presentes nas páginas de "políticas de privacidade" e "termos de uso" dos sites.

Isso porque a aplicação do *visual law* busca ampliar o conforto cognitivo do usuário e a sensação de familiaridade e pertencimento com a informação[197] através do uso de recursos como figuras, imagens, formas, tabelas e tantos outros. Nesse ponto, vale ressaltar os dados de um estudo citado por Danielle Serafino e Paula Cardoso:

---

[195] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, [*s. l.*], v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521.

[196] Qualquer usuário que possui um serviço do Google pode acessar o "*Google Dashboard*". Disponível em: https://myaccount.google.com/dashboard. Acessado em 12.04.2022.

[197] PRESGRAVE, Ana Beatriz. **Visual Law: o design em prol do aprimoramento da advocacia**. Brasília: OAB Editora, 2021. p. 36.

> "A utilização de imagens pode ser um grande diferencial, já que temos estudos que indicam que:
>
> - Nosso cérebro é capaz de interpretar imagens captadas pelos olhos em apenas 13 milissegundos;
> - Apresentações com recursos visuais são até 43% mais persuasivas;
> - Nosso cérebro processa imagens 60 mil vezes mais rápido que os textos;
> - Documentos com símbolos são até 95% mais bem compreendidos"[198]

A título de exemplo, pode-se citar a página de "Políticas de Privacidade e Termos de Uso" do site do escritório de advocacia "Nelson Wilians Advogados"[199], em que o "aviso de privacidade" utiliza o recurso de tabelas a fim de demonstrar ao usuário os termos e conceitos presentes no documento, com o objetivo de facilitar a interpretação do mesmo.

Além disso é possível observar a utilização de recursos a fim de tornar o design da página mais atraente e acessível para a leitura, o que, em síntese, compõe o que Serafino e Cardoso chamam de "um bom design":

> "temos sete passos principais que auxiliam na identificação de um bom design:
>
> 1. **Layout**: está relacionado com a disposição de imagens e textos nos documentos. É o layout que delimitará o espaço para cada coisa dentro do documento e definirá a hierarquia da informação, dando maior ou menor destaque para cada parte específica, de acordo com a ideia que desejamos transmitir para o usuário;
> 2. **Grid**: são as réguas utilizadas para montar um documento. Sua principal função é deixar, dentro de uma estrutura, todas as informações bem organizadas e harmonizadas;
> 3. **Espaço** negativo: sua função é dar respiro visual e oferecer espaço entre os conteúdos para melhorar o entendimento do documento;
> 4. **Fonte**: também é uma mensagem e é o ponto de contato estético que o seu usuário terá com o documento. Ela deve facilitar a leitura do documento e, se você for usar mais de uma fonte, saiba combiná-las;
> 5. **Cores**: devem ser usadas com intenção, porque elas têm efeitos psicológicos nos leitores. Utilize-as de acordo com o sentimento que você pretende despertar ou de acordo com a identidade visual da marca que você representa;
> 6. **Contraste**: comanda a atenção, uma vez que ele direciona o leitor para o ponto destacado. Ele pode ser feito de diversas maneiras, seja pelo tamanho da fonte, pelo destaque com cor, pela troca de fonte ou pelo negrito, por exemplo;

---

[198] SERAFINO, Danielle L.; CARDOSO, Paula. Legal Design e Visual Law na Prática. **Legal Inovationa: o futuro do Direito e o Direito do futuro**. São Paulo: Thomson Reuters Brasil, 2022. p. 81–92.

[199] A página de "Política de Privacidade e Termos de Uso" está disponível em: https://nwadv.com.br/politicas-de-privacidade/. Acessado em 12.04.2022.

> 7. **Consistência**: quando utilizamos um documento que tem um padrão, é importante que ele tenha consistência para reforçar um elemento ou mensagem. Dentro do Visual Law, este recurso é muito utilizado na padronização ou no reforço de ícones".[200]

Nesse sentido, levando em consideração que os usuários não leem as "políticas de privacidade" nem os "termos de uso" e, quando o fazem, acabam por não os entender ou levam um tempo significativo para tanto[201], a aplicação de técnicas de *visual law* tendem a melhorar a comunicação jurídica, auxiliando na compreensão do conteúdo pretendido, sem que este perca sua complexidade e profundidade[202].

[200] SERAFINO, Danielle L.; CARDOSO, Paula. Legal Design e Visual Law na Prática. **Legal Inovationa: o futuro do Direito e o Direito do futuro**. São Paulo: Thomson Reuters Brasil, 2022. p. 81–92.

[201] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, [*s. l.*], v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521.

[202] PRESGRAVE, Ana Beatriz. **Visual Law: o design em prol do aprimoramento da advocacia**. Brasília: OAB Editora, 2021. p. 41.

5 CONSIDERAÇÕES FINAIS

O presente trabalho teve por objetivo analisar a insuficiência do consentimento para a proteção dos dados pessoais, levando em consideração tanto os dados pessoais que são informados pelo usuário de forma ativa quanto aos dados imperceptíveis, que são usados na economia informacional sem que o usuário tenha conhecimento.

Na parte inicial do trabalho foi possível observar a construção histórica a respeito do direito à privacidade, que teve seu início de discussão a partir da segunda metade do século XIX. Neste ponto, evidenciou-se que o desenvolvimento tecnológico permitiu a coleta e tratamento dos dados pessoais de forma mais elevada, trazendo, portanto, a necessidade de discussão da tutela dos titulares dos dados pessoais.

Consequentemente, desenvolveu-se na Europa a disciplina da proteção de dados, onde diversas leis foram criadas a fim de regular a matéria. É nesse contexto também que surgiram os principais princípios orientadores do tema, tais quais: princípio da finalidade, publicidade, qualidade, livre acesso, segurança física e lógica, bem como o do consentimento.

Com efeito, verificou-se o contexto brasileiro na discussão sobre a proteção de dados pessoais, onde se concluiu que o tema já possuía uma regulamentação com a vigência do Código de Defesa do Consumidor (Lei 8.078/1990).

Ademais, outras leis que tratamento da matéria surgiram em nosso ordenamento jurídico, as quais também merecem indicação: A Lei 12.414/2011 (Lei do Cadastro Positivo), Lei 12.527/2011 (Lei de Acesso à Informação Pública), Lei 12.965/2014 (Marco Civil da Internet) e, por fim, a Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), que é a primeira lei específica sobre a disciplina no Brasil.

Na segunda parte do trabalho desenvolveu-se o estudo acerca do tratamento de dados pessoais e como esse processo está relacionado ao desconhecimento do cidadão que utiliza a internet, tornando, portanto, o consentimento em uma mera ficção.

Nesse sentido, o estudo empenhou-se em demonstrar como os dados pessoais do usuário são importantes no contexto da economia informacional, onde o usuário deixa de ser um simples consumidor e passa a ser, de certa forma, um produto oferecido pelas empresas para terceiros realizarem publicidade direcionada.

É nesse contexto que a coleta e o tratamento de dados pessoais recebem grande atenção, tanto pelas empresas quanto pelos legisladores — estes últimos que buscam, de alguma forma, tornar essa assimetria em uma balança equilibrada. Entretanto, observa-se que o desenvolvimento tecnológico torna esse equilíbrio entre empresa e cidadão cada vez mais difícil de se alcançar, uma vez que a própria engrenagem da economia informacional tem os dados como combustível. Nesse sentido, o uso de ferramentas como os *cookies* se faz necessário, ainda que coloquem em risco a privacidade dos usuários em um modelo de negócio "*take it or leave it*", em que não há outro caminho senão aceitar o tratamento de dados.

Ademais, o consentimento do usuário passou a ter uma grande importância nesse aspecto, recebendo cada vez mais adjetivação a partir de sua concepção, o que o tornou em regra geral para o tratamento de dados. Dessa forma, para que o tratamento dos dados do usuário seja legítimo e lícito, ele precisa ser consentido de forma livre, expressa, informada e para uma determinada finalidade.

Uma vez que os dados são o combustível da economia da informação e que o consentimento do usuário é tido como necessário para um tratamento legítimo e lícito, o trabalho buscou investigar se, de fato, esse consentimento é suficiente para que tal processo ocorra.

Nesse contexto, evidenciou-se que os usuários tem seus dados obtidos de duas formas: i) de forma ativa, quando ele próprio informa seus dados para uma empresa a fim de efetivar uma transação comercial ou se cadastrar para fazer parte de uma rede social, por exemplo, e, ii) de forma imperceptível, quando esses dados são obtidos através de ferramentas e tecnologias desconhecidas por parte do usuário, porém, "consentidas", uma vez que este autorizou o tratamento ao clicar em "li e aceito os termos".

Não obstante, esse consentimento mostrou-se insuficiente para o tratamento de dados pessoais. Primeiro, porque o usuário possui uma limitação cognitiva para a tomada de decisão sobre aceitar ou não aceitar o tratamento de dados; segundo, porque a desigualdade entre as partes torna o consentimento a única possibilidade, onde a sua não aceitação acarreta em duras consequências para o usuário, e, terceiro, pela impossibilidade de o usuário gerenciar os riscos da coleta dos dados frente a tantos lugares que solicitam o seu consentimento.

A limitação cognitiva está relacionada a difícil compreensão do usuário em consentir com algo que não sabe como funciona. Observou-se, através de pesquisas empíricas que grande

parte dos usuários consentem sem ao menos ler as “políticas de privacidade” dos sites, e, quando o fazem, não compreendem os termos jurídicos presentes no documento.

A assimetria entre as partes é o segundo problema que torna o consentimento em uma mera ficção, pois, viu-se que grande parte dos usuários são submetidos a um modelo de negócio em que a aceitação do tratamento de dados é a única opção, em uma lógica de “*take it or leave it*”.

Por fim, a terceira problemática diz respeito a impossibilidade de o usuário ter um controle sobre seus dados compartilhados, uma vez que autoriza por diversas vezes em inúmeros locais. Observou-se que com o avanço tecnológico, atualmente existem ferramentas capazes de juntar pedaços de dados do usuário espalhados pela internet a fim de construir um retrato do mesmo.

Ao final desse trabalho foram apresentadas duas possíveis alternativas com o objetivo de mitigar as problemáticas apresentadas na segunda parte do estudo. A primeira alternativa trata-se das PETs, onde foram demonstradas duas ferramentas que buscam empoderar o cidadão na proteção de seus dados pessoais. A segunda alternativa diz respeito a aplicação de técnicas de *visual law* a fim de facilitar o entendimento do usuário acerca dos termos presentes nas “políticas de privacidade” dos sites, tornando a leitura mais fácil e atraente, haja vista que esse é um dos grandes problemas para a eficácia do consentimento.

REFERÊNCIAS BIBLIOGRÁFICAS

BIONI, Bruno. Legítimo Interesse: Aspectos Gerais a Partir de uma Visão Obrigacional. **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021. *E-book*.

BIONI, Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021.

BIONI, Bruno.; LUCIANO, Maria. O consentimento como processo: Em busca do consentimento válido. **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021. *E-book.*

BLUM, Rita Peixoto Ferreira. **O Direito à Privacidade e à Proteção dos Dados do Consumidor**. São Paulo: Almedina, 2018. *E-book*.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD)**, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

BRASIL, Presidência da República. **Medida Provisória nº 954, de abril de 2020**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm

BRASIL, Supremo Tribunal Federal. **ADI nº 6387. Rel. Min. Rosa Weber, Plenário, j. 06 e 07.05.2020**. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf

COSTA, Ana Costa; SILVA, Monique de Almeida. O comportamento do consumidor de infoproduto. **Research, Society and Development**, v. 10, n. 3, p. e0310312874, 2021. Disponível em: https://doi.org/10.33448/rsd-v10i3.12874

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91–108, 2011. Disponível em: http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021. *E-book.*

DUHIGG, Charles. **O Poder do Hábito: por que fazemos o que fazemos na vida e nos**

negócios. Rio de Janeiro: Objetiva, 2012.

EMPOLI, Giuliano Da. **Os engenheiros do caos**. 1. ed. São Paulo: Vestígio, 2020.

FRAZÃO, Ana. Objetivos e Alcance da Lei Geral de Proteção de Dados. **Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019. p. 99–129.

GADWALLADR, Carole.; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian**, 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-face book-influence-us-election

HEW, EUA. Records, Computers and the Rights of Citizens. **Report of the Secretary's Advisory Committee on Automated Personal Data Systems**, 1973. Disponível em: https://aspe.hhs.gov/reports/records-computers-rights-citizens

HILÁRIO, Dânton; GONÇALVES, Luís Felipe; VALASKI, Luís Henrique. Consentimento e legítimo interesse como hipóteses de tratamento de dados pessoais na Lei Geral de Proteção de dados: Paradoxos e convergências. **Revista da Comissão de Inovação e Gestão da OAB/PR**, v. III, p. 266–290, 2021.

LINS, Bruna Rego; QUINELATO, Pietra Daneluzzi. Redes sociais à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Social Media Law: O Direito nas Redes Sociais.** São Paulo: Thomson Reuters Brasil, 2021. p. 143–184.

MARTINS, Leonardo. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Fundación Konrad-Adenauer, 2005.

MAYER-SCHÖNBERGER, Viktor. Generational Development of Data Protection in Europe. Technology and Privacy: The New Landscape. London: The MIT Press, 1997. p. 219–242. Disponível em: https://doi.org/10.7551/mitpress/6682.003.0010

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

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**. São Paulo: Revista dos Tribunais, 2018. v. 120, p. 469–483. *E-book*.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, v. 6, n. 2, p. 507–533, 2020. Disponível em: https://doi.org/10.21783/rei.v6i2.521

MENKE, Fabiano. A possibilidade de cumulação de bases legais nas operações de tratamento de dados pessoais. **Proteção de Dados: Temas Controvertidos**. Indaiatuba, SP: Editora Foco, 2021a. p. 279–293.

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Revista Jurídica Luso-Brasileira**, n. 1, p. 781–809, 2019. Disponível em: https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf

MENKE, Fabiano. As origens alemãs e o significado da autodeterminação informativa. **Migalhas**, 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/335735/as-origens-alemas-e-o-significado-da-autodeterminacao-informativa

MENKE, Fabiano. Spiros Simitis e a primeira lei de proteção de dados do mundo, **Migalhas**, 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/355182/spiros-simitis-e-a-primeira-lei-de-protecao-de-dados-do-mundo.

MORAIS, José Luis Bolzan de; NETO, Elias Jacob de Menezes. A Insuficiência do Marco Civil da Internet na Proteção das Comunicações Privadas Armazenadas e do Fluxo de Dados a Partir do Paradgma da Surveillance. **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 417–439.

OBAR, Jonathan A.; OELDORF-HIRSCH, Anne. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. **Information, Communication & Society**, v. 23, n. 1, p. 128–147, 2020. Disponível em: https://doi.org/10.1080/1369118X.2018.1486870

PAESANI, Liliana Minardi. Garantia fundamental do não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei. **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 518–526.

PANORAMA SETORIAL DA INTERNET, NÚMERO 2, JUNHO 2019, ANO 11. Disponível em: https://cetic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-

xi_n_2_privacidade_e_dados_pessoais.pdf.

PRESGRAVE, Ana Beatriz. **Visual Law: o design em prol do aprimoramento da advocacia**. Brasília: OAB Ed, 2021.

RAINER JR, Rainer Kelly; CEGIELSKI, Casey G. **Introdução a Sistemas de Informação**. 5. ed. Rio de Janeiro: Elsevier, 2016.

RENZETTI, Bruno Polonio; ALMEIDA, Luís Felipe Rasmus de; BANHOS, Tiago Paes de Andrade. Implicações da Lei do Cadastro Positivo para a Proteção de Dados Pessoais no Brasil: As Dificuldades do Sistema Opt-Out. **A Lei Geral de Proteção de Dados Brasileira: Uma Análise Setorial (Volume I)**. 1. ed. São Paulo: Almedina, 2021. p. 130–171.

SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O direito fundamental à proteção de dados. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, *E-book*.

SCHERMER, Bart W.; CUSTERS, Bart; VAN DER HOF, Simone. *The crisis of consent: How stronger legal protection may lead to weaker consent in data protection*. **Ethics and Information Technology**, v. 16, n. 2, p. 171–182, 2014. Disponível em: https://doi.org/10.1007/s10676-014-9343-8

SCHREIBER, Anderson. **Direitos da personalidade: revista e atualizada**. 3. ed. São Paulo: Atlas, 2014. *E-book*.

SERAFINO, Danielle Lima; CARDOSO, Paula. Legal Design e Visual Law na Prática. **Legal Inovation: O Futuro do Direito e o Direito do Futuro**. São Paulo: Thomson Reuters Brasil, 2022. p. 81–92.

SIMITIS, Spiros. *Revisiting Sensitive Data*. **Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, Strasbourg, nov. 1999. p. 1–11. Disponível em: https://rm.coe.int/09000016806845af

SOLOVE, Daniel J. *Introduction: Privacy self-management and the consent dilemma*. **Harvard Law Review**, v. 126, n. 7, p. 1880–1903, 2013. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018

TEPEDINO, Gustavo; SPADACCINI DE TEFFÉ, Chiara. O consentimento na circulação de dados pessoais. **Revista Brasileira de Direito Civil**, v. 25, n. 03, p. 83–116, 2020. Disponível

em: https://doi.org/10.33242/rbdc.2020.03.005

VIOLA, Mario.; SPADACCINI DE TEFFÉ, Chiara. Tratamento de dados pessoais na LGPD: Estudo sobre as bases legais dos artigos 7º e 11. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. Digital.

WARREN, Samuel D.; BRANDEIS, Louis D. *The right to privacy*. **Harvard Law Review**, v. 4, n. 5, p. 193–220, 1890. Disponível em: https://www.jstor.org/stable/1321160