



**FACULDADE BAIANA DE DIREITO**

**CURSO DE GRADUAÇÃO EM DIREITO**

**MARIA EDUARDA CAVALCANTE FERREIRA ANDRADE**

**CONSENTIMENTO NO MUNDO VIRTUAL: COMO OS *DARK PATTERNS* INFLUENCIAM PARA QUE ELE NÃO SEJA LIVRE, INFORMADO E INEQUÍVOCO**

Salvador

2022

**MARIA EDUARDA CAVALCANTE FERREIRA ANDRADE**

**CONSENTIMENTO NO MUNDO VIRTUAL: COMO OS *DARK PATTERNS* INFLUENCIAM PARA QUE ELE NÃO SEJA LIVRE, INFORMADO E INEQUÍVOCO**

Monografia apresentada ao curso de graduação em Direito, Faculdade Baiana de Direito, como requisito parcial para obtenção do grau de bacharel em Direito.

Orientador: Prof. Diogo Guanabara

Salvador

2022

**TERMO DE APROVAÇÃO**

**MARIA EDUARDA CAVALCANTE FERREIRA ANDRADE**

**CONSENTIMENTO NO MUNDO VIRTUAL: COMO OS *DARK PATTERNS* INFLUENCIAM PARA QUE ELE NÃO SEJA LIVRE, INFORMADO E INEQUÍVOCO**

Monografia aprovada como requisito parcial para obtenção do grau de bacharel em Direito, Faculdade Baiana de Direito, pela seguinte banca examinadora:

Nome: \_\_\_\_\_

Titulação e instituição: \_\_\_\_\_

Nome: \_\_\_\_\_

Titulação e instituição: \_\_\_\_\_

Nome: \_\_\_\_\_

Titulação e instituição: \_\_\_\_\_

Salvador, \_\_\_\_/\_\_\_\_/\_\_\_\_

Aos meus pais, que nunca me deixaram desistir dos meus sonhos.

## **AGRADECIMENTOS**

Por mais clichê que seja, eu gostaria de iniciar agradecendo a Deus, a Nossa Senhora, Santa Barbara e Santo Antônio, pois a minha fé, durante os diversos momentos difíceis foi meu alicerce.

Meus pais, Sandra e Juca também foram peças fundamentais para que eu chegasse até aqui, eles sempre zelaram pela minha educação, investiram o possível e o impossível para que eu percorresse caminho o caminho que eu desejava seguir, vocês são a minha força e a minha inspiração. Obrigada por serem o meu suporte, pelo incentivo e por acreditarem em mim, mais até do que eu mesma. Gostaria de agradecer aos meus irmãos Daniel, Luiza, Paula e Pedro, que em algum momento foram inspirações para mim. Por fim, não poderia deixar de citar meu tio Herbert, que é um exemplo de advogado e me incentivou a pensar como tal, desde nova. Tio Neo, Elber e meu avô Antônio Palmeira, que me incentivaram minha carreira jurídica e a minha dinda, Izabel, que foi quem me fez sonhar com a carreira no direito. Mamá, Cacá e Dindo, obrigada por todo o amor e suporte de sempre. Ainda aqui dedico um agradecimento ao meu namorado, Ícaro, que foi fundamental durante todo meu processo, me dando suporte e me ouvindo.

Gostaria de agradecer à Faculdade Baiana de Direito por ter me acolhido e me oferecido diversas possibilidades, ao meu orientador, professor Diogo Guanabara, que tanto me ajudou nesse processo. Sou grata a cada uma das entidades que pude passar durante a minha jornada na universidade, sobretudo à Alfa, Atlética e Equipe de Negociação, lugares onde fiz muitos amigos, que certamente levarei para a vida.

Aos meus amigos que, durante o curso, deixaram tudo mais leve. Obrigada aos Furões, sobretudo à Mari, a Cacá que foram minhas companheiras desde que entrei. Agradeço também ao Cerveja no Impulso, um dos grupos mais fantástico que tenho a honra de fazer parte, sobretudo à Nanda, que por diversas vezes chorou comigo pelos corredores da baiana e depois rimos no café. Impossível não citar Vic e Juli, que foram presentes da minha graduação. Por fim, preciso agradecer às minhas amigas da vida, que, como sempre estiveram do meu lado, feito nunca.

Por último e não menos importante, deixo meus agradecimentos para as minhas chefinhas, Dra Bia e Dra Gabi, que nos últimos anos me ensinaram e me inspiraram no tipo de profissional que almejo ser, buscando sempre a excelência. Obrigada.

## RESUMO

O presente estudo tem o intuito de fazer análise do consentimento, previsto na Lei Geral de Proteção de dados, em conjunto com os *dark patterns*, ou padrões obscuros, usados nas plataformas digitais. Na Lei Geral de Proteção de dados, o instituto do consentimento possuirá requisitos de validade, que nem sempre são respeitados pelos controladores no universo digital, de modo que os padrões obscuros são empregados como forma de induzir o titular a fornecer o consentimento, sem que de fato essa seja sua vontade. Assim, o presente trabalho buscou analisar a coleta de consentimento através do uso de *dark patterns*, bem como auxiliar na identificação deste. Para melhor compreensão do tema, foi utilizado o método hipotético dedutivo, com o uso de legislações pertinentes, pesquisas bibliográficas e ilustração de casos concretos, onde os referidos padrões são empregados.

Palavras-chave: Consentimento. Dados. Padrões. Escuros. Digital.

## LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
DP	<i>Dark patterns</i>
GDPR	General Data Protection
LGPD	Lei Geral de Proteção de Dados
MP	Medida Provisória



## LISTA DE FIGURAS

Figura 1	Tela 1 de Cadastro de Conta Google	59
Figura 2	Tela 2 de Cadastro da Conta Google	60
Figura 3	Privacidade e Termos	61
Figura 4	Aceite de Termos	62
Figura 5	Sugestões de Privacidade	64
Figura 6	Minha atividade	65
Figura 7	Personalização de Anúncios	66
Figura 8	Informações sobre o Titular	67
Figura 9	Desativar Personalização	68
Figura 10	Tela de Acesso à Conta	70
Figura 11	Tela de Gerenciamento 1	70
Figura 12	Tela de Gerenciamento 2	71
Figura 13	Confirmação 1 de Cancelamento	71
Figura 14	Confirmação 2 de Cancelamento	72
Figura 15	Confirmação 3 de Cancelamento	72
Figura 16	Informação de Cancelamento	73
Figura 17	E-mail de Cancelamento	74
Figura 18	Confirmação de Cookies	75
Figura 19	Confirmação de Cookies 2	76

<b>1 INTRODUÇÃO .....</b>	<b>12</b>
<b>2 A LEI GERAL DE PROTEÇÃO DE DADOS E A SOCIEDADE</b>	
<b>MOVIDA A DADOS.....</b>	<b>16</b>
<b>2.1 AVANÇOS TECNOLÓGICOS E OS DADOS.....</b>	<b>16</b>
<b>2.2 A NOVA FORMAÇÃO ECONÔMICA E OS DADOS PESSOAIS.....</b>	<b>17</b>
<b>2.3 A PROTEÇÃO DE DADOS COMO DIREITO FUNDAMENTAL.....</b>	<b>20</b>
<b>2.4 A LEI GERAL DE PROTEÇÃO DE DADOS.....</b>	<b>21</b>
<b>2.4.1 CONCEITOS DA LEI GERAL DE PROTEÇÃO DE DADOS.....</b>	<b>24</b>
2.4.1.1 Artigo 5º, conceitos da Lei.....	24
2.4.1.2 Princípios, fundamentos e bases legais.....	25
<b>2.5 O DIREITO À PRIVACIDADE E A LEI DE PROTEÇÃO DE DADOS.....</b>	<b>27</b>
<b>3 O PAPEL DO CONSENTIMENTO NO TRATAMENTO DE DADOS.....</b>	<b>29</b>
<b>3.1 CONCEITO.....</b>	<b>29</b>
<b>3.2 REQUISITOS DO CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS.....</b>	<b>30</b>
<b>3.2.1 MANIFESTAÇÃO LIVRE.....</b>	<b>30</b>
<b>3.2.2 CONSENTIMENTO INFORMADO.....</b>	<b>31</b>
<b>3.2.3 CONSENTIMENTO INEQUÍVOCO.....</b>	<b>32</b>
<b>3.2.4 CONSENTIMENTO PARA UMA FINALIDADE DETERMINADA.....</b>	<b>32</b>
<b>3.2.5 FORMA DE COLETA.....</b>	<b>32</b>
<b>3.3 OUTROS ASPECTOS RELACIONADOS AO CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS.....</b>	<b>33</b>
<b>3.3.1 CONSENTIMENTO E AUTODETERMINAÇÃO INFORMATIVA.....</b>	<b>34</b>
<b>3.3.2 CONSENTIMENTO E TRANSPARÊNCIA.....</b>	<b>35</b>
<b>3.3.3 CONSENTIMENTO E DIREITOS DO TITULAR.....</b>	<b>35</b>
<b>3.4 VÁLIDADE DO CONSENTIMENTO NO MUNDO DIGITAL.....</b>	<b>37</b>
<b>3.4.1 POLÍTICA DE PRIVACIDADE E CONSENTIMENTO.....</b>	<b>39</b>
<b>4 DARK PATTERNS OU PADRÕES OSCUROS.....</b>	<b>42</b>
<b>4.1 CONCEITOS.....</b>	<b>42</b>

<b>4.1.1 NUDGES E <i>DARK PATTERNS</i>.....</b>	<b>43</b>
4.2 LEGISLAÇÃO E OS <i>DARK PATTERNS</i> .....	45
4.3 CLASSIFICAÇÃO DOS <i>DARK PATTERNS</i> .....	47
<b>4.3.1 CLASSIFICAÇÃO SEGUNDO BRIGNULL.....</b>	<b>48</b>
4.3.1.1 Pergunta ou Trick Question.....	48
4.3.1.2 Esgueirar-se ou Senak Into The Basket .....	48
4.3.1.3 Barata de Motel ou Roach Motel.....	48
4.3.1.4 Zuckering de Privacidade .....	48
4.3.1.5 Prevenção de Comparação de Preço .....	48
4.3.1.6 Desvio .....	48
4.3.1.7 Despesas Ocultas.....	49
4.3.1.8 Isca e Troca.....	49
4.3.1.9 Anúncios Disfarçados.....	49
4.3.1.10 Confirmar Vergonha .....	49
4.3.1.11 Continuidade Disfarçada.....	49
4.3.1.12 Spam de Amigos.....	49
<b>4.3.2 CLASSIFICAÇÃO DE ACORDO COM A TAXONOMIA DE BRIGNULL.....</b>	<b>49</b>
4.3.2.1 Irritante.....	50
4.3.2.2 Obstrução.....	50
4.3.2.3 Sorrateira.....	50
4.3.2.4 Interferência de Interfaces .....	51
4.3.2.5 Ação Forçada.....	51
<b>4.3.3 CLASSIFICAÇÃO DO EUROPEAN DATA PROTECTION BOARD.....</b>	<b>52</b>
4.3.3.1 Sobrecarga.....	52
4.3.3.2 Ignorar.....	52
4.3.3.3 Agitação.....	52
4.3.3.4 Impedir.....	53
4.3.3.5 Inconstância .....	53
4.3.3.6 Deixado no escuro.....	53
4.4 USER XPERIENCE.....	53

4.5 PRIVACY BY DESIGN.....	55
<b>5 CONSENTIMENTO,DARK PATTTERNS E USER XPERIENCE.....</b>	<b>56</b>
5.1 ANÁLISE TEÓRICA DOS INSTITUTOS.....	56
5.2 ANÁLISE PRÁTICA DOS <i>DARK PATTERNS</i> .....	58
<b>5.2.1 GOOGLE.....</b>	<b>58</b>
<b>5.2.2 AMAZON PRIME.....</b>	<b>69</b>
<b>5.2.3 COLETA DE CONSENTIMENTO PARA COOKIES.....</b>	<b>75</b>
<b>6 CONCLUSÃO.....</b>	<b>78</b>

## REFÊRENCIAS

## 1 INTRODUÇÃO

Os avanços tecnológicos e facilidades promovidos pelo mundo digital revolucionaram não só as formas de comunicação que evoluíram em níveis inimagináveis ao longo dos anos, *mas também a economia*. Tais avanços promoveram a migração de diversos comportamentos do cotidiano para o mundo digital, como fazer consultas médicas, compras, comunicação, exercer atividade laboral e muitos outros

Informação e dados pessoais movem a economia da chamada sociedade da informação, onde muitas coisas aparentemente são de graça, mas o preço vem através de informações que o titular considera simples. Dessa forma, quem detém mais dados, além de possuir poder, possui maior vantagem competitiva.

Conseqüentemente, quanto mais informações os controladores possuem a respeito de diversos titulares, maior o seu poder de influência e assim, eles usarão de todos os artifícios possíveis para maximizar a coleta de informações.

Nesse panorama, muitos países se organizaram internamente para regular o tratamento de dados, não só no mundo digital, mas principalmente nele. Em 14 de agosto de 2018, o Brasil aprova a sua própria regulamentação, a Lei 13.709, conhecida como Lei Geral de Proteção de Dados, que possuiria um *vacatio legis* de 2 anos para que houvesse tempo hábil de adequação, entrando em vigor dois anos depois, em 14 de agosto de 2020. Esse diploma normativo trará a figura do titular como protagonista de suas disposições. Dessa forma, ele deve ter seus direitos salvaguardados e seus dados como informações importantes, necessitam ser tratadas em consonância com as normas. Essa legislação vai impor não só as regras para ocorrerem as operações com dados, mas também princípios que devem ser seguidos durante todo o tratamento e as hipóteses legais para as operações com dados.

Dentre as muitas disposições dessa lei, há para o tratamento de dados a necessidade de adequação à uma base legal, dentre as dispostas no ordenamento, sendo uma delas o consentimento, já conhecido e utilizado amplamente no direito civil, mas

possuindo aqui requisitos específicos de validade. O ato de consentir aqui exprime a vontade de uma das partes em aderir a determinada coisa, que para ser válido precisa seguir alguns requisitos. O primeiro deles é que seja o titular seja informado de todos os aspectos que se relacionam ao tratamento de dados. Ademais, ele precisa ser produzido de maneira inequívoca e livre, sendo direcionado para uma finalidade determinada, de forma que seja fornecido expressamente pelo titular ou que o controlador possua meios de provar que aquela concordância ocorreu.

Ocorre que nem sempre o controlador vai coletar esse aceite de forma válida, no sentido que, ao longo dos anos, novas formas de induzir ao consentimento foram criadas. Assim surgem os chamados *dark patterns*, traduzidos como Padrões Escuros ou Obscuros, que virão através do layout nas páginas digitais e irão induzir o titular a tomar uma decisão que, se soubesse de todo o contexto, poderia lhe levar a agir de forma diferente. Ainda, irão promover no titular a falsa sensação de que ele possui poderes sobre seus dados. Ou seja, em muitos desses casos há o tratamento de informações pessoais com base em um consentimento falacioso, que irá ceifar diretamente o direito de autodeterminação informativa do titular. A Autodeterminação informativa é a possibilidade dele decidir o que é melhor para si e com o que deseja consentir, não havendo aqui adequação à lei, por existir um consentimento viciado. Isso se agrava quando se percebe que os dados coletados dessa forma são utilizados para fins comerciais, objetivando auferir lucro e, que em muitos casos o titular nem tem noção como e do quanto suas informações estão sendo usadas.

Ao analisar o cenário internacional, observa-se que diversos países já se posicionaram, mesmo que de forma mínima a respeito do tema, impondo regras ou trazendo guias para o tratamento de dados com base em consentimento. Apesar disso, no Brasil ainda não há regulamentação e ainda existem poucos estudos sobre o tema, favorecendo a coleta de dados a partir dos *dark patterns* no ambiente virtual. Assim sendo, é imprescindível que o legislador determine que as empresas se atenham à coleta de consentimento de maneira adequada e válida, a fim de evitar desconformidade com a Lei Geral de Proteção de Dados e assegurem os direitos do titular. Outrossim, é preciso olhar com criticidade para os padrões obscuros da

indústria, de forma que seja possível colocar limites a coleta de consentimento, possibilitando a autodeterminação informativa do titular de dados.

O objetivo do presente trabalho é discutir acerca do instituto do consentimento, fazendo uma análise de seus requisitos de validade. Ademais, busca-se explicar o que seriam os padrões obscuros e como eles influenciam na coleta de consentimento, de maneira que o tornam viciado. Dessa forma irá contribuir com o universo teórico dos institutos apresentados, objetivando fazer uma análise crítica a respeito do tema de modo que os vícios existentes possam em um futuro ser sanados. A importância social do estudo advém da necessidade da conscientização do cidadão quanto aos direitos que ele possui e alertá-lo que algumas condutas daquele que coleta seus dados são questionáveis. Olhando por outro prisma, o do controlador de dados, o trabalho é importante para preveni-lo a respeito de práticas que devem ser eliminadas no tratamento de dados pessoais.

A monografia em questão será baseada em pesquisas bibliográficas, jurisprudências e em dispositivos legais, principalmente analisando a Lei 13.708 de 14 de 2018, a Lei Geral de Proteção de Dados, legislações e diretrizes estrangeiras a respeito do tema. Haverá também o estudo e utilização de plataformas online para ilustrar como a situação se aplica na realidade. Dessa forma, ao final do trabalho será possível aplicar a pesquisa bibliográfica ao observado em um pequeno recorte do mundo digital.

A metodologia que será utilizada para desenvolver este trabalho, terá como base o método Hipotético-Dedutivo de Karl Popper, onde serão feitas premissas, constatações e análises, que que passarão pelo procedimento do falseamento para averiguar sua veracidade. As premissas a serem falseadas são: (i) a lei geral de proteção de dados oferece ao titular todo um arcabouço de proteção relacionado ao tratamento de seus dados (ii) a lei geral de proteção de dados trouxe diretrizes que possibilitam uma coleta válida de consentimento no mundo virtual (iii) os padrões obscuros não influenciam na coleta de consentimento. Assim, usaremos as premissas para entender o uso de consentimento no mundo digital, delimitar quais devem ser os seus limites e observar a influência que isso tem na autodeterminação informativa do titular. Através da utilização desse método, busca-se comprovar as questões

relacionados ao uso indevido de padrões obscuros para assegurar a coleta de consentimento em plataformas virtuais.

Para guiar o trabalho serão utilizadas questões orientadoras, que estarão relacionadas com o tema proposto, para que ao fim, seja possível chegar a uma conclusão a respeito da questão. Junto a isso, serão utilizadas pesquisas qualitativas, objetivando a interpretação do objeto.

Nesse sentido, inicialmente, busca-se trazer ao leitor o panorama em que a questão está inserida: uma sociedade que com o advento da tecnologia foi ficando cada vez mais especializada em dados, de modo que o titular se tornou 100% monitorado em sua vida digital. Nesse cenário surgem as discussões a respeito do direito à privacidade de dados e da proteção de dados como direito fundamental e a necessidade de uma proteção maior à essas informações, que vem através da Lei Geral de Proteção de Dados. Há ainda explanação a respeito desse instituto, seus principais conceitos, princípios e bases legais.

Por conseguinte, o próximo capítulo vai focar no instituto do consentimento, analisando os requisitos impostos pela lei, trazendo uma análise teórica sobre ele e fazendo um paralelo com outros aspectos previstos no diploma legislativo.

O capítulo em sequência vai versar sobre os padrões obscuros, sua definição, como eles são utilizados para coletar o consentimento viciado, suas classificações. Serão traçadas também as relações desses padrões com algumas estratégias de marketing. e como podem evitados, através de estratégias de marketing.

Em diante, o capítulo 5 irá ilustrar a relação dos Padrões Obscuros com todos outros temas abordados durante o presente estudo. Além disso, será exemplificado como são empregados os padrões obscuros através de análise de algumas plataformas online.

Por fim, o último capítulo irá abordar as conclusões advindas deste estudo.



## **2 A LEI GERAL DE PROTEÇÃO DE DADOS E A SOCIEDADE MOVIDA À DADOS**

### **2.1 AVANÇOS TECNOLÓGICOS E OS DADOS**

De maneira inicial, urge trazer à baila o contexto de toda a questão: o mundo digital. De acordo com Silva, os últimos anos do século XX se mostraram fundamentais para o desenvolvimento da informação e comunicação, ampliando o acesso de muitos à essas tecnologias, de maneira jamais imaginada. Como nunca, as pessoas puderam ter contato crescente com dados através da internet, utilizando um fluxo contínuo deles, trazendo novas possibilidades ao cotidiano (SILVA, 2010,p.1). Esse mundo, conhecido como ciberespaço, é formado por um fluxo de informações e de mensagens transmitidas entre computadores (ALMEIDA E LUGATI, 2020 p.1).

Ao tratar dos avanços tecnológicos no mundo digital, ao longo dos últimos anos, é evidente que as informações pessoais, os dados, têm se destacado nesse cenário. A respeito disso, Pinheiro afirma que a reunião de informações estruturadas, passou a garantir maior poder, concentrado nas mãos de poucos. (PINHEIRO, 2018, p. 205).

A digitalização de experiências e relações sociais tem sido um processo constante que ocorre, principalmente, por conta do aprimoramento tecnológico que existe e das tecnologias cada vez mais ágeis, surgidas a cada dia, somados ao grande potencial de armazenamento e difusão de informações. (COSTA e OLIVEIRA, 2019, p.3). Pode-se dizer, que as ações no mundo virtual constantemente geram dados, que serão transferidos para algum lugar. É inegável que esse conhecimento gerado através disso produz facilidades e alternativas de consumo, mas também é praticamente impossível os titulares controlarem seus próprios dados. (CARVALHO, 2019, p. 95).

Com protagonismo dos dados, há a datificação dos atos humanos como reflexo, que ocorre através da codificação de muitos aspectos da vida social. O que nunca havia sido quantificado passou a ser transferido para os ambientes da web, produzindo uma verdadeira indústria baseada em dados. (DIJCK, 2014, p.2).E, no contexto de uso

exacerbado da tecnologia da informação, que gera intenso e volumoso fluxo de dados, o usuário não ocasionalmente encontra-se em posição de desnorteamto. Vê-se perdido no emaranhado de redes, conexões, dados e termos de compromisso, cuja cadeia informativa, por vezes, é pouco conhecida. (MENDONÇA, 2019, p.2).

## 2.2 A NOVA FORMAÇÃO ECONÔMICA E OS DADOS PESSOAIS

O tratamento de informações resultou em uma nova forma de economia. Prass descreve que o uso de dados no mundo digital consiste em coletar os “rastros” de navegação do usuário da Internet, como detalhes sobre preferências informadas em redes sociais, o que gera um subsídio valioso para a formação de perfis do usuário. (PRASS, 2018, p.1). Assim, o fornecimento de alguns dados, que podem parecer irrelevantes, do ponto de vista do titular, ou nem serem diretamente referenciados a ele, ao serem cruzados e organizados, podem resultar em dados bastante específicos sobre determinada pessoa, assegurando até informações de caráter sensível. (VIOLLA E TEFFÉ, 2019, p. 195).

O tratamento dessas informações de forma exagerada se reflete em uma mutação do capitalismo, conhecida como capitalismo de vigilância, onde há a transformação de dados cedidos gratuitamente em matéria prima para um produto altamente lucrativo (MENA, 2019, p.1). Nesse sentido, Bruno Bioni afirma que a coleta de dados faz com que exista um sistema de informação, que permite a estruturação de dados e de maneira organizada pode produzir conhecimento que pode ser revertido a uma tomada de decisão, como no caso de uma ação publicitária (BIONI, 2019, p. 57). Para isso, as empresas de tecnologia irão extrair essas informações e refiná-las, de modo que se tornem dados de predição de comportamento, capazes de prever os próximos passos do usuário antes até dele mesmo (MENA, 2019, p.1).

Esse processo está diretamente ligado ao nascimento de novas formas econômicas. O controle de dados oferece aos controladores um grande poder. As velhas formas de pensar sobre a concorrência, concebidas na era do petróleo, parecem desatualizadas em relação ao que veio a ser chamado de “economia de dados” (THE ECONOMIST, 2017, p.1). A economia movida a dados surge em um cenário em que

a informação se tornou preponderante para a produtividade e poder, levando em consideração o incremento de novas tecnologias. (SANTOS, 2019, p. 5). Nesse cenário, é inegável que os dados pessoais são ativos de valor imensurável (FERRAZ E SIROTHEAU, 2021, p.1).

Ao pensar sobre a necessidade de proteção de dados, entende-se que uso destes foi e ainda, é algo que não preocupa o titular. Muitas informações sobre o usuário podem ser auferidas através das plataformas digitais. Ao interagir com o conteúdo publicado, com os demais usuários, realizando publicações, check-ins, likes e afins, o usuário possibilita a coleta de uma gama de informações pessoais, sociais e até íntimas. Uma vez coletados, essas informações possuem grande valor no mercado.(D'URSO e D'URSO, 2021, p.2).

As grandes empresas como Google, Facebook e Twitter, ao analisar os dados e metadados coletados conseguem observar até impressões, sintomas dos comportamentos ou humores reais das pessoas. (DIJCK, 2017, p. 42). Essa análise pode ser usada de forma nociva, como no caso em que o Facebook se viu envolvido, no ano de 2018, onde dados pessoais de mais de 50 milhões de pessoas foram utilizados sem o consentimento delas pela empresa americana Cambridge Analytics para fazer propaganda política. A empresa teria tido acesso ao volume de dados ao lançar um aplicativo de teste psicológico na rede social. Aqueles usuários do Facebook que participaram do teste acabaram por entregar à Cambridge Analytics não apenas suas informações, mas os dados referentes a todos os amigos do perfil. (CRIDDLE, 2018, p.1).

Outro caso muito famoso de análise desenfreada de dados no capitalismo de vigilância ocorreu em 2012, quando o Target, rede de supermercados americano, descobriu através de suas análises a gravidez de uma adolescente e enviou cupons à sua residência, antes mesmo que ela pudesse contar a notícia aos seus familiares.

À época do caso, eles atribuíam pontuações a cada comprador, vinculado ao nome ou cartão de crédito, que armazenava o histórico de compras e, ao cruzar os dados de compra com comportamento padrão de determinado grupo de pessoas. Assim, foi possível inferir que havia a possibilidade de gravidez e até o trimestre em que a

grávida se encontra, o que gerava cupons de desconto para determinados itens, e eram enviados ao titular (HILL, 2012, p. 1-2).

Observando a recorrência dessas práticas o Conselho de Consumo Norueguês em um de seus relatórios, retrata que no universo digital, os serviços costumam acumular dados pessoais para uso e análise, para assim obterem receita. Isso acontece por meio do compartilhamento de informações que, além de possibilitar a personalização do serviço, facilita o desenvolvimento de publicidade direcionada. Dessa maneira, considera-se que o usuário acaba pagando pelo serviço através de seus dados. (FORBRUKERRADET 2018, p.5)

Como consequência do uso desenfreado de dados pessoais e dessa troca constante, há o que Leetaru vai chamar de Estado Distópico de Vigilância, onde tudo é gratuito, mas o preço disso é a privacidade do titular. Ele entende que nesse universo as empresas perseguem suas vítimas inocentes, extraindo o máximo de lucro de qualquer fragmento de privacidade do usuário, ao utilizar os seus dados (LEETARU, 2018, p.1). Para além disso, existem outros malefícios nesse uso, como consequências sociais de isolamento do usuário em suas próprias preferências e ainda a possibilidade de adentrar o caminho da violação de direitos, com um tratamento realizado fora do propósito inicialmente comunicado ao titular (SEBASTIÃO, 2020 p.111)

Em contraponto ao discutido, Prass afirma que o aproveitamento de detalhes sobre o usuário não é sempre nocivo. Assim é preciso avaliar se há uso positivo de dados, como no caso do Waze, aplicativo de trânsito, onde os dados são utilizados para propor o trajeto com menos congestionamento, que é maximizada devido ao fornecimento da localização em tempo real dos dispositivos que estão no interior dos automóveis. (PRASS, 2018, p.1).

É inegável que o mundo digital em muito acrescentou e trouxe facilidade para a vida de todos aqueles que estão inseridos nele. Os serviços oferecidos, em muitos casos possuem um modelo de negócios que é bastante baseado em dados, oferecendo um valor central ao consumidor (um sistema de buscas, uma plataforma de vendas online, uma plataforma de transporte compartilhado, uma plataforma de vídeos etc.), somado

a isso, têm-se a conveniência de personalizar a experiência de cada usuário, com base em seus hábitos, individualizando assim o relacionamento das marcas com os consumidores (TANAKA, 2019, p. 18).

Apesar disso, fazendo uma análise de acordo com um paradigma protetivo, que reconhece a posição de vulnerabilidade de determinados grupos, devem ser dedicadas normas especiais para tutelá-los na exata medida de suas fraquezas. Dessa maneira, devemos assumir que o titular de dados, em meio ao mercado informacional, deve ser considerado em estado de vulnerabilidade. Diante disso, devem ser emitidas normas protetivas, para assegurar um tratamento correto para eles (BIONI, 2019, p. 220).

### 2.3 PROTEÇÃO DE DADOS COMO DIREITO FUNDAMENTAL

Apesar dos avanços tecnológicos possuírem pontos positivos e negativos, é preciso que se reflita a respeito dos problemas jurídicos decorrentes da massificação do uso da internet. Dessa forma, é necessário que exista estudo crítico a respeito dos direitos humanos fundamentais à privacidade e à proteção aos dados pessoais. (BOFF e FORTES, 2014, p. 111).

A existência dos direitos fundamentais sobreveio da necessidade de definições das relações entre indivíduos e estruturas de poder, especialmente com relação ao Estado. Os direitos fundamentais delimitam o poder do Estado e, ao mesmo tempo, exigem que os este adote medidas positivas garantindo um ambiente que permita que todas as pessoas gozem de seus direitos. (SANTIAGO e SOUZA, 2021, p. 106). Ainda sobre o tema, há a ideia de que os direitos fundamentais são considerados como valores inerentes ao ser humano, a exemplo da liberdade e dignidade, sendo constitucionalmente assegurados (CONJUR, 2022, p.2).

Wolfgang entende que assim como ocorre com os direitos fundamentais em geral, no caso do direito fundamental à proteção de dados pessoais há uma dupla dimensão subjetiva e objetiva, desempenhando múltiplas funções na ordem jurídico constitucional. Sob a condição de direitos subjetivos, como um direito amplo, o direito de proteger dados pessoais é decodificado em um conjunto de posições subjetivas

defensivas (negativas) heterogêneas, mas também carrega os benefícios condicionais do direito, e seu objetivo é para o estado para fornecer fatos ou ações tomadas por interesses normativos. (WOLFGANG, 2021, p. 3).

Nesse sentido, o ordenamento brasileiro já reconhece o direito à proteção de dados como um direito fundamental. Inicialmente, essa ideia foi discutida na esfera jurídica, trazida pela Ministra Rosa Weber em seu relatório e em seu voto do julgamento da Medida Provisória nº 954, de 17/4/2020, pelo Supremo Tribunal Federal. A MP trata do compartilhamento de dados de clientes de empresas de telefonia móvel com o Instituto Brasileiro de Geografia e Estatística. Nesse caso, a ministra afirma que há uma inconstitucionalidade material, por afronta ao direito fundamental à proteção de dados. Esse direito decorre da conjugação das cláusulas fundamentais assecuratórias da dignidade da pessoa humana, da inviolabilidade da intimidade, da vida privada, da imagem e da honra, bem como do sigilo dos dados (WEBER, 2020, p. 5).

Posteriormente, em fevereiro de 2022 a Emenda Constitucional 115, de fevereiro deste ano, promulgada pela Câmara dos Deputados e Senado federal instituiu esse direito como fundamental. De acordo com o texto legislativo, adiciona-se ao artigo 5º, LXXIX, que é assegurado, o direito à proteção dos dados pessoais, inclusive nos meios digitais, nos termos da Lei. Outrossim, foi adicionada como uma das competências da União “organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei” e, por fim, foi acrescida como competência privativa da União Legislativa sobre proteção e tratamento de dados pessoais (BRASIL, 2022).

## 2.4 A LEI GERAL DE PROTEÇÃO DE DADOS

Junto com as transformações trazidas pelos avanços tecnológicos, as preocupações a respeito do direito à privacidade não poderiam ser tratadas apenas no âmbito privado e individual. Dessa forma, a ideia de que para que houvesse sua superação, bastaria sua abstenção, foi superada. Agora essa temática avança rumo ao reconhecimento de que as ameaças aos dados pessoais partem tanto de instituições

públicas quanto privadas, de modo a ensejar um novo olhar para o tema. (FLÔRES E SILVA, p. 4, 2020).

Ao ter em mente o enorme processamento de dados, que veio com a tecnologia, percebeu-se que a proteção da intimidade e privacidade não era o bastante, sendo necessária também a proteção dos dados pessoais. Isso porque os dados pessoais dizem muito a respeito do seu titular, podendo ser considerados uma extensão de sua personalidade, devendo assim ser protegidos. Vale salientar que, com a ideia de trazer um ordenamento para isso, não há o proibicionismo quanto ao seu uso, mas o incentivo à inovação e o desenvolvimento junto com as garantias de segurança necessárias para o titular, através do estabelecimento de regras para o uso adequado e leal desses dados. (FERRAZ E SIROTHEAU, 2021, p.1). Assim, a iniciativa irá trazer a necessidade do titular como participante do processo, bem como de ter direitos, ao reconhecer que ele se encontra em uma posição(hiper)vulnerável. (ALMEIDA E LUGATI *apud* BIONI, 2020 p.1).

Salienta-se que, apesar da necessidade de uma lei específica para a temática, antes delas existiam diplomas normativos que tocavam na questão. Lugati e Almeida trazem o Código de Proteção do Consumidor, de 1990, que em seu artigo 43 aborda a proteção assegurada ao titular frente a bancos de dados e cadastros. Esse artigo exige que o cadastro seja claro, objetivo e verdadeiro, com linguagem facilmente compreendida. Ademais, é preciso também que o consumidor seja comunicado sobre a abertura de cadastros, ficha, registro e dados pessoais e de consumo (ALMEIDA E LUGATI, 2020, p. 10). Para além disso, a Constituição Federal de 1988 garante o direito à vida privada e intimidade. Nesse sentido, o Marco Civil da Internet, a Lei 12.965 de abril de 2014, determina princípios, garantias, direitos e deveres para o uso da internet no Brasil. Em seu artigo 3º, III o referido diploma assegura a proteção de dados pessoais como um de seus princípios. Há também na lei alguns direitos como o não fornecimento de dados pessoais à terceiros, de informações claras sobre o tratamento, e a necessidade de coleta expressa de consentimento para tratar e alguns outros, restritos apenas à internet (BRASIL, 2014).

Levando o contexto da necessidade de aprofundamento de proteção de dados, em 14 de agosto de 2018 foi sancionada pelo então presidente Michel Temer 35a Lei nº 13.709/2018, também denominada Lei Geral de Proteção de Dados Pessoais, que entrou em vigor em agosto de 2020 (FINKELSTEIN e FINKELSTEIN, 2019, p. 11). Embora o País já tivesse algumas leis que tratavam com parcimônia da proteção de dados, as disposições da LGPD trouxeram novas e relevantes regras legais sobre o assunto (MOLICONE, 2020, p.1).

Essa não vai se resumir apenas ao sistema europeu isso, visto que é muito comum assumir que ela está fortemente atrelada ao General Data Protection Regulation. Seu caráter global é amplamente verificável, possuindo também gêneros oriundos dos Estados Unidos (BIONI, p. 32, 2020).

Sobre a Lei Geral de Proteção de Dados, Peck afirma que é um marco legal que gerou grande impacto, não só nas instituições privadas, mas também no universo público. Isso porque o diploma se refere à dados pessoais do indivíduo em qualquer relação que envolve o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja a operação realizada por pessoa natural, seja por pessoa jurídica. (PINHEIRO, 2018, p. 11). A contribuição da Lei é marcante, tendo em vista que não vai versar apenas sobre o tratamento de dados pessoais coletados, como também arrola direitos ao titular no ambiente digital e fora dele. (MENDONÇA, 2019, p.1).

Segundo a 13.709 de 14 de Agosto de 2018, o objetivo desta é proteger os direitos fundamentais da liberdade e da privacidade e o livre desenvolvimento da personalidade da pessoa natural. Dessa forma, ela irá dispor sobre o tratamento de dados pessoais, em qualquer meio, realizador por pessoa natural ou jurídica. (BRASIL, 2018). Nesse sentido, a LGPD é uma regulamentação que tratará consigo direitos, obrigações e princípios relacionados ao uso de dados, um dos ativos mais valiosos da sociedade digital, que são usados como base de dados relacionados às pessoas. (PINHEIRO, 2019, p. 11).



## 2.4.1. CONCEITOS DA LEI GERAL DE PROTEÇÃO DE DADOS

### 2.4.1.1. Artigo 5º, conceitos da Lei.

Ao falar sobre a Lei 13.709 é importante que sejam esclarecidos alguns conceitos trazidos por ela em seu artigo 5º:

Inicialmente é importante tornar cristalino o conceito de dado pessoal que é uma informação relacionada a pessoa natural identificada ou identificável. Esse dado pessoal se torna sensível quando tem relação com origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (BRASIL, 2018).

O dado pessoal sensível vai ser objeto de proteção recrudescida, por haver potencial de lesividade da informação, já que se refere a informações relacionadas ao íntimo da pessoa e pode ensejar discriminações abusivas (ABILIO, FRAZÃO e OLIVEIRA, 2019, p. 680).

Há ainda o dado anonimizado, que é aquele em que o titular não pode ser identificado, sendo fundamental que sejam utilizados meios técnicos razoáveis e disponíveis no momento do tratamento (BRASIL, 2018).

O tratamento, por sua vez, é trazido como toda operação que acontece envolvendo dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018)..

Ainda de acordo com o diploma legislativo, titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. (BRASIL, 2018).

Por fim, é relevante citar que a Lei traz duas figuras de agente de tratamento, que serão aqueles que tratam os dados. O primeiro deles é controlador, que é a pessoa jurídica ou natural, podendo ser direito público ou privado que irá decidir como ocorrerá o tratamento de dados. Ademais, o Operador, que é uma pessoa natural ou

jurídica, de direito público ou privado, é aquele que tratará os dados pessoais em nome do controlador. (BRASIL, 2018).

Em todos os tratamentos de dados, parte dessas figuras ou termos estarão presentes, o que faz com que seja necessário o entendimento destes em determinadas situações.

#### 2.4.1.2. Princípios, Fundamentos e Bases Legais

Dentre as muitas novidades trazidas pela inovação do diploma de proteção de dados, é importante destacar os princípios, que deverão ser respeitados durante o tratamento de dados de pessoas físicas. (PESTANA, 2020, p.1).

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (BRASIL, 2018)

Patrícia Peck traz em sua obra que as atividades de tratamento legítimo, com dados pessoais, devem estar orientadas pelos princípios citados anteriormente (PINHEIRO, 2019, p.25), o que na prática significa que, inobstante um tratamento de dados estar de acordo com outros requisitos legais, como finalidade legítima e estar em consonância com as bases legais do artigo 7º, impõe-se que os princípios sejam devidamente respeitados (LEAL, 2021, p.1).

O diploma normativo em tela, trará também alguns fundamentos, que devem ser seguidos durante qualquer operação de tratamento de dados pessoais. São eles: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

Ainda com o objetivo de obedecer aos cuidados trazidos pela legislação para o tratamento de dados, fica estabelecido que qualquer pessoa que trate dados seja ela natural ou jurídica, de direito público ou privado, inclusive na atividade realizada nos meios digitais, deverá ter uma base legal para fundamentar os tratamentos de dados pessoais que realizar. (VIOLA e TEFFÉ, 2019, p. 195).

As bases legais consistem em hipóteses normativas que possibilitam que o controlador ou operador de dados tratem os dados pessoais. Dessa maneira, para que seja possível o tratamento de dados, deverá ocorrer o encaixe do mesmo em uma

pelo menos uma das hipóteses legais, sendo ele assim, considerado legítimo e lícito. Ainda há a possibilidade de cumular as bases. (VIOLA e TEFFÉ, 2020, p. 38).

A Lei Geral de Proteção de Dados traz como bases legais: consentimento; o cumprimento de obrigação legal ou regulatória; pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; realização de estudos por órgãos de pesquisas; execução contratual ou procedimentos preliminares ligados a isso; exercício regular de direito em processos; proteção da vida ou incolumidade física; tutela da saúde; legítimo interesse; proteção do crédito. As referidas hipóteses estão elencadas nos artigos 7º e 11º (BRASIL, 2018).

## 2.5 O DIREITO À PRIVACIDADE E A LEI GERAL DE PROTEÇÃO DE DADOS

O direito à privacidade tem recebido atenção e relevância nas controvérsias atuais considerando o estado da sociedade moderna, em que há um acesso significativo às redes sociais e meios de comunicação. Nesses termos, a lei vem, ao longo dos anos, se adaptando às demandas sociais, de forma a proteger o referido direito da personalidade considerado como um direito humano fundamental (CUNHA, 2020, p.1).

Esse direito, está previsto no artigo 5º, inciso X da Constituição Federal de 1988, sendo uma de suas cláusulas pétreas (BRASIL, 1988). De igual maneira, o direito à privacidade vem na Lei Geral de Proteção de dados como um de seus princípios, previsto no artigo 2º I, sendo um dos objetivos da referida lei proteger esse direito fundamental (BRASIL, 2018). Para além disso, o direito à proteção dos dados pessoais, por outro lado, também encontra salvaguarda parcial e indireta mediante a previsão da ação de habeas data (art. 5.º, LXXII, da CF), ação constitucional, com status de direito-garantia fundamental autônomo (WOLFGANG, 2021, p.2) e em 2022 foi considerado um direito fundamental.

Desta forma, o direito à privacidade não irá se confundir com o direito à proteção dos dados pessoais, já que este é somente um dos fundamentos que disciplinam a

proteção dos dados pessoais (CUNHA, 2020, p.9). Pode-se assim afirmar que os referidos direitos devem ser usados para promover a personalidade humana, privilegiando-se escolhas e decisões individuais. (BESSA, 2021, p.4).

### **3 O PAPEL DO CONSENTIMENTO NO TRATAMENTO DE DADOS**

#### **3.1 CONCEITO**

Inicialmente para ilustrar o que seria o consentimento, no direito civil, é relevante trazer o entendimento de Chaves e Rosernvald, no que diz respeito ao tema, eles explicam que os atos jurídicos, compreendidos em sentido amplo, são atinentes aos atos decorrentes da vontade humana. Mais adiante, completam que essa vontade deve ser exteriorizada no sentido de aderir a efeitos jurídicos concretos previstos na norma jurídica (ato jurídico *stricto sensu*) ou pode ser dirigida à criação de concretos efeitos jurídicos (negócio jurídico) (CHAVES e ROSERNVALD, 2015 p.501).

O consentimento é fundamental para a formação de qualquer negócio, por meio dele, é possível admitir o concurso da vontade, que é um elemento que atribui a voluntariedade e a liberdade (VASCONCELOS, 2020. p.6). Assim, mediante a uniformidade de opinião, duas ou mais expressões volitivas irão se destinar à produção de efeitos legalmente permitidos e desejados pelas partes. (ROMAN, 2020, p.56). Há a existência desse instituto como elemento central da estratégia de supervisão de privacidade de informações, mesmo sabendo que existem dúvidas a respeito da racionalidade e poder de negociação do titular no controle de seus dados. (DONEDA, 2019, p. 401).

Nas operações de operações de tratamento, a pessoa natural se encontra em uma situação de vulnerabilidade frente às empresas e organizações no que diz respeito à privacidade, dessa maneira, o consentimento se faz extremamente relevante na relação jurídica entre as partes. (MORAIS, 2020, p.2). Isso porque ele vai conferir à essa pessoa a possibilidade de modificar sua própria esfera jurídica, com base na expressão de sua vontade. (DONEDA, 2019, p. 401).

Antes da Lei Geral de Proteção de Dados, o Marco Civil da Internet já havia firmado o entendimento de que cabia ao cidadão o direito de não ter seus dados fornecidos a terceiros, salvo nos casos em que houvesse consentimento para tal. Além disso, o consentimento deveria ser coletado de maneira expressa para o uso, armazenamento

e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais (BRASIL, 2014).

Para efeitos de proteção de dados, o Consentimento é uma das bases legais que permitem o tratamento, possuindo um papel importante, mas sem excluir a possibilidade de utilização de outros fundamentos legais mais adequados à situação. É uma espécie de permissão do indivíduo para a realização do tratamento de seus dados, que se usada corretamente possibilita o controle do titular sobre as operações de tratamento, caso isso não ocorra inexistente controle e não há utilização adequada, perdendo o seu valor. (WORKIN PARTY 29, 2011, p. 2 e p.10).

Na perspectiva de Doneda, o consentimento se faz fundamental para o tratamento, apesar de ser um ponto complexo da disciplina. Ele irá justificar isso afirmando que, por meio deste, o direito civil terá a oportunidade de estruturar uma disciplina que ajuste os efeitos desse consentimento à natureza dos interesses em questão. Isso poderá ser feito a partir da consideração da autonomia da vontade, da circulação de dados e dos direitos fundamentais (DONEDA, 2019, p. 398)

### 3.2 REQUISITOS DO CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados traz que este deve ser uma **manifestação livre, informada e inequívoca** pelo qual o titular concorda com o tratamento de seus dados pessoais **para uma finalidade determinada** (BRASIL, 2018). Sua obtenção é antes do início do tratamento de dados é uma condição essencial para legitimá-lo (WORKING PARTY 29º , 2011, p.9).

#### 3.2.1. Manifestação livre

Sobre a manifestação, Leques entende que livre é aquela que expressa a genuína vontade do seu titular (sem qualquer tipo de vício de vontade — erro, fraude ou coação). (LEQUES, 2019, p.1). Outrossim, é necessário que exista a liberdade de escolha quanto aos dados que deseja fornecer e deve haver a possibilidade de retirada do consentimento, a qualquer tempo (ROMAN, 2020, p. 60). Nesse sentido a

Comissão Europeia de Proteção de Dados em sua Diretiva sobre consentimento ainda afirma que, nos casos em que o titular não possui a escolha real, se sentir compelido a consentir ou sofrerá consequências por sua recusa, esse consentimento não será considerado válido (EUROPEAN DATA PROTECTION BOARD, 2020, p. 7).

### **3.2.2. Consentimento informado**

No que tange a necessidade dele ser informado, isso significa que o titular do dado pessoal deve possuir ao seu dispor as informações que são necessárias para avaliar a forma como ocorrerá o tratamento, sendo determinante para a expressão do consentimento (VIOLA e TEFFÉ, 2019, p. 9).

A respeito das informações prestadas, considera-se que devem conter quais dados são coletados, se há uso compartilhado e para quem, quais as finalidades do tratamento, informações a respeito de medidas de segurança adotadas, informações sobre o controlador e operador, quais os direitos do usuário e como eles podem ser exercidos. Para além disso, essas informações precisam ser específicas, detalhadas e acessíveis. (CUSTERS, 2016, p.2). Caso isso não ocorra, o controle do usuário torna-se ilusório e será uma base inválida para o tratamento (EUROPEAN DATA PROTECTION BOARD, 2020, p. 15). Aqui vão se destacar os princípios da transparência, adequação e finalidade para restringir tanto a generalidade na utilização dos dados quanto tratamentos opacos (VIOLA e TEFFÉ, 2019, p. 9). Não obstante, as informações devem possuir profundidade, já que a forma como ela é fornecida influencia na qualidade do consentimento, bem como a sua acessibilidade e disponibilidade (WORKING PARTY 29º, 2019, p. 20).

O European Data Protection Board recomenda que o consentimento deve ser claro, distinguível de outros assuntos e fornecido de forma inteligível e de fácil acesso. Esse requisito significa essencialmente que as informações relevantes para a tomada de decisões informadas sobre consentir ou não, não podem ser ocultadas nos termos e condições gerais. (EUROPEAN DATA PROTECTION BOARD, 2020, p.16).



### **3.2.3. Consentimento inequívoco**

Ao exigir que o consentimento seja inequívoco, entende-se que a manifestação deve ocorrer através de um ato positivo do usuário, não bastando a aceitação passiva. Dessa maneira, o silêncio do titular não implica em anuência. (ROMAN, 2020, p. 61). O ato declarativo deve mostrar de maneira óbvia que o titular consentiu, através de mecanismos disponibilizados pelo controlador (EUROPEAN DATA PROTECTION BOARD, 2020, p. 19).

### **3.2.4. Consentimento para uma finalidade determinada**

A coleta de dados deve ser sempre vinculada a uma ou mais finalidades específicas, que devem ser informadas na respectiva política de privacidade para que o titular tenha noção do que será feito com suas informações pessoais (ROMAN, 2020, p. 61). A necessidade dessa especificação advém da garantia de controle e transparência para o titular (WORKING PARTY 29, 2011, p.34).

Deve-se ter em mente que o titular dos dados autoriza o tratamento não para finalidades universais e ilimitadas, mas sim compatíveis com o contexto em que aqueles dados serão utilizados. Disso decorre a ideia de que o tratamento de dados deve ser pautado por objetivos legítimos e específicos, amplamente divulgados aos usuários para que possam esclarecimentos suficientes para sustentar a sua tomada de decisão quanto à autorização de uso de dados. (MENDONÇA, 2019, p.3).

Qualquer modificação dos termos inicialmente informados dará ensejo à obrigação de notificar previamente o titular a respeito, que poderá revogar seu consentimento, caso não esteja de acordo com a alteração (conforme parágrafo 6º do artigo 8º e parágrafo 2º do artigo 9º, ambos da Lei 13.709/2018). (LEQUES, 2019, p.1). A revogação irá ensejar a finalização do tratamento (BRASIL, 2018).

### **3.2.5. Forma de coleta**

O consentimento deve ser fornecido de maneira escrita ou por outro meio que demonstre a manifestação de vontade do titular, devendo, nos casos em que for escrito estar destacado das demais cláusulas (BRASIL, 2018).

A coleta pode ocorrer em documento autônomo, pode fazer parte do instrumento ou pode ser coletado de maneira oral. É fundamental que nessa coleta exista menção à finalidade específica e havendo expressa responsabilidade quanto à segurança dos dados armazenados, pois de acordo com o diploma legal, controlador e operador são responsáveis solidariamente por eventual dano causado ao titular (MORAIS, 2020, p.2) No entanto, tal instrumento não se constitui como única forma de coleta deste. Por exemplo, no contexto digital ou online, um titular de dados pode emitir a declaração exigida preenchendo um formulário eletrônico, enviando um e-mail, carregando um documento digitalizado com sua assinatura do ou usando um Assinatura Eletrônica. Em teoria, o uso de declarações orais também pode ser suficientemente para obter um consentimento explícito válido, no entanto, pode ser difícil provar para o controlador que todas as condições para um consentimento explícito válido foram atendidas quando a declaração foi registrada (EUROPEAN DATA PROTECTION BOARD, 2020, p. 21).

É importante observar que o controlador tem para si o ônus de provar que o consentimento foi obtido de acordo com os dispositivos previstos em Lei (MOLICONE, 2020, p.1).

Ademais existe firmada em outros ordenamentos jurídicos a ideia de granularidade do consentimento, nos cenários em que o serviço pode envolver múltiplas operações de tratamento para mais de uma finalidade. Nesses casos, os titulares dos dados devem ser livres para escolher qual finalidade aceitam, em vez de terem que consentir com um conjunto de finalidades de tratamento. Essa fragmentação para a obtenção do consentimento vai se relacionar diretamente com uma ideia de que ele precisa ser específico. (EUROPEAN DATA PROTECTION BOARD, 2020, p.12) .

### 3.3 OUTROS ASPECTOS RELACIONADOS AO CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS

Da mesma maneira que ocorre em outros diplomas legislativos, o instituto do consentimento vai dialogar com outros aspectos da norma de proteção de dados, não só no Brasil, mas no mundo. Nesse sentido, ele será exercido através da

autodeterminação informativa, precisando de transparência e vai dialogar diretamente com os direitos do titular.

### **3.3.1. Consentimento e autodeterminação informativa**

O direito à autodeterminação informativa está tutelado na Lei Geral de Proteção de Dados em seu artigo 2º, II, trazido como um dos fundamentos da lei. Ele consiste na faculdade que todos possuem de exercer, de algum modo, controle sobre seus dados pessoais e garantindo, em algumas circunstâncias a decisão sobre o tratamento de seus dados. (BESSA, 2020, p.1). Assim, o referido direito vai se expressar sobre o controle do titular durante toda a operação de tratamento (CNIL, 2017, p. 9), havendo determinação expressa e prevista em lei de que esse controle deve existir (STABEN, 2012, p. 5).

Nesse diapasão, a autodeterminação informativa reflete um direito humano básico, relacionado inclusive ao acesso à informação que deve ser fornecido pelo provedor do serviço (YOON, e YOON, 2019, p.2).

Ao fazer um paralelo entre este instituto e o consentimento, pode-se afirmar que há relação entre os dois, na medida em que a autonomia do titular dos dados é tanto uma condição prévia como uma consequência do consentimento: confere ao titular dos dados influência sobre o tratamento dos dados. (WORKING PARTY 29, 2011 p. 9). No que tange à Lei Geral de Proteção de Dados Pessoais, ao mesmo tempo que esta reconhece a importância do tratamento de dados para desenvolvimento econômico e tecnológico, ela vai buscar conferir instrumentos para que o titular tenha certo controle e autonomia em relação ao que é feito com seus dados, através da autodeterminação informativa (BESSA 2021, P.3).

Ocorre que, apesar da relação dos institutos é fundamental, para que se torne efetiva, que a autodeterminação informativa do titular seja vista como um princípio que vai além de uma simples forma de obter um consentimento efetivo do titular. As tecnologias devem exercer o papel de empoderar o titular de dados, que se encontra em posição de muita vulnerabilidade, ao contrário do que se costuma afirmar e, diante disso, se poderá falar em uma autodeterminação informativa (LUGATI e ALMEIDA, 2020, p. 29).

### **3.3.2. Consentimento e o princípio da transparência**

De acordo com a Lei Geral de Proteção Dados, a transparência, um de seus princípios previsto no artigo 6º, VI, deve ser observado no tratamento de dados pessoais. O referido diploma normativo conceitua esse instituto como a garantia de serem fornecidas ao titular de informações claras, precisas e facilmente acessíveis, sobre a realização do tratamento e os respectivos agentes de tratamento, devendo ser observados, obviamente, os segredos comerciais e industriais. (BRASIL, 2018). A ênfase assegurada a esse princípio deseja destacar a importância da fluidez das informações que devem ser fornecidas ao titular. Isso porque ele, junto com seus dados constituem os elementos mais importantes inerentes ao tratamento de dados (PESTANA, 2020, p.6) .

Nesse sentido, a Lei determina em seu artigo 9º que, nas hipóteses em que o consentimento é requerido, caso as informações oferecidas ao titular possuam conteúdo enganoso, abusivo ou não tenham sido apresentados com transparência, de maneira clara e inequívoca, o consentimento será considerado nulo (BRASIL, 2018).

Ou seja, independentemente da existência de base legal e do cumprimento dos demais requisitos estabelecidos pela Lei, é impositivo que o titular possuía pleno conhecimento de todas as operações que ocorrem com seus dados pessoais, sob pena do controlador incorrer em infração à Lei 13.709/18. Conclui-se assim que é de suma importância que o controlador direcione atenção e recursos para a confecção de documentos referentes ao tratamento de dados que pretendem realizar, de forma que seja traduzido ao titular, de maneira compreensível, o motivo pelo qual há o tratamento e as condições que estão envolvidas ali. (LEAL, 2021, p.6).

### **3.3.3. Consentimento e direitos do titular**

A Lei Geral de Proteção de dados além de determinar como deve ser o tratamento de dados pessoais e alguns outros aspectos, vai trazer em seu artigo 18 alguns direitos que devem ser tutelados ao titular de dados. Vejamos:

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência

**VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;**

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

**VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;**

**IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.**

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

**§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.**

Dessa maneira, ao analisar o referido diploma fica evidente que o legislador assegurou ao titular alguns direitos relacionados ao consentimento. Inicialmente, pode-se inferir que nos casos em que há tratamento de acordo com a base legal do consentimento, poderá haver por parte do titular o pedido de exclusão de seus dados da base legal, ressalvados os casos previstos no artigo 16 da mesma lei. Ademais, há também a possibilidade do titular saber quais as consequências que haverá do não aceite em fornecer o consentimento ao controlador.

Para além disso, há a possibilidade da revogação do consentimento fornecido, não devendo existir procedimento oneroso para tanto, passando a produzir efeitos dali em diante (LEQUES, 2019, p3). Nos casos em que consentimento é obtido em meio eletrônico, por meio de apenas um clique do mouse, deslizar o dedo ou pressionar uma tecla, os titulares dos dados devem, na prática, poder retirar essa permissão com

a mesma facilidade que concederam (EUROPEAN DATA PROTECTION BOARD, 2020 p. 23).

Ao fim do tratamento, com a retirada do consentimento, todas as operações de dados que foram baseadas nele e ocorreram antes da retirada permanecem lícitas, no entanto, recomenda-se que o controlador interrompa as próximas atividades de tratamento (EUROPEAN DATA PROTECTION BOARD, 2020, p. 24). A exceção a isso acontece nos casos em que houver pedido expresso de eliminação pelo titular de dados (LEQUES, 2019, p.3).

Finalmente, é importante trazer que a pessoa interessada possuirá o direito de se opor ao tratamento de dados, com base em uma das hipóteses de renúncia de consentimento, caso não houver cumprimento das disposições legais (MOLICONE, 2020, p.10).

Ainda é possível, nos casos em que o tratamento esteja pautado no consentimento, que o titular solicite cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento. (BRASIL, 2018).

### 3.4 VALIDADE DO CONSENTIMENTO NO MUNDO DIGITAL

A problemática envolvendo o consentimento perpassa por muitas questões, a principal delas diz respeito a sua validade. De fato, o consentimento colhido em redes sociais ou em sites da internet, estão de acordo com todos os requisitos legais? Nem sempre.

No contexto digital, muitos serviços precisam de dados pessoais para funcionar, portanto, os titulares dos dados recebem várias solicitações de consentimento que precisam de respostas por meio de cliques e furtos todos os dias. Isso pode resultar em um certo grau de fadiga do clique: quando encontrado muitas vezes, o efeito de aviso real dos mecanismos de consentimento nem sempre é efetivo (EUROPEAN DATA PROTECTION BOARD, 2020, p.19).

Há na doutrina quem defenda a ideia de que o consentimento deveria ter um prazo de validade. Custers acredita que dada as rápidas mudanças dos fenômenos digitais e análises de dados, não é razoável que o consentimento geral para o tratamento seja fornecido *ad eternum*, já que este pode facilmente se tornar desatualizado, não refletindo mais as vontades do usuário. É importante salientar que isso não deve ocorrer, visto que o consentimento para a operação deve incluir o tratamento real. Ocorre que hoje, muitos sites e mídias sociais podem notificar o usuário sobre a mudança de políticas, mudanças e expansão de operações de tratamento, mas nem sempre irão renovar esse consentimento (CUSTERS, p.3, 2016)

A Lei Geral de Proteção de Dados, em seu artigo 8º vai considerar nulo o consentimento genérico e vedar o tratamento de dados baseado no vício de consentimento. Dito isto, é questionável a validade de um consentimento fornecido por um usuário através de um clique sem que esse indivíduo tenha de fato ciência sobre os termos e sobre o que acontece com seus dados offline (SOUZA e SANTIAGO, 2021, p. 117). Isso porque não basta a simples adesão a um “aceito” ou “concordo” em qualquer termo online para que a coleta seja válida, o que é muito comum que aconteça. É necessário que ele seja livre, informado e inequívoco, diante da vedação de generalidade (KHOURI, 2021, p. 2)

Ainda nesse sentido, o Grupo de Trabalho em Proteção de Dados da Europa, conhecido como Working Party 29, emitiu em um de seus pareceres a ideia de que o consentimento só pode ser válido se o titular puder exercer uma escolha real e se não houver risco de engano, coerção ou consequências negativas. Nos casos em que a negativa do titular o prejudicarem, não haverá consentimento livre. (WORKING PARTY 29º, 2011, p. 31).

Ao exemplificar o que seria uma coleta de consentimento inválida o Conselho de Proteção de Dados Europeu traz a seguinte situação: o titular, ao baixar o um aplicativo em seu dispositivo de celular se depara com o pedido de consentimento para uso do acelerômetro do telefone. Esse acesso não é necessário para que o aplicativo funcione, mas é útil para o controlador que deseja saber mais sobre os movimentos e níveis de atividade de seus usuários. Ao retirar a sua permissão para

tratamento desses dados, o titular percebe que o aplicativo agora funciona apenas de forma limitada, ainda que a função desabilitada não tenha influência direta. Nesse caso há um exemplo de prejuízo ao usuário, o que significa que este consentimento nunca foi obtido de maneira válida, devendo o controlador excluir todos os dados pessoais tratados anteriormente sobre os movimentos do usuário, coletados dessa forma (EUROPEAN DATA PROTECTION BOARD, 2020, p. 13).

Ainda buscando pacificar o tema, a Comissão Nacional de Informática e Liberdades da França em 2019 determinou que o consentimento só é válido se a pessoa possuir a possibilidade de exercer sua escolha, sem sofrer grandes penalidades caso não o forneça ou resolva retirá-lo. Foi decidido também que a pessoa pode dar o seu consentimento de forma específica e independente para cada finalidade distinta ou até de forma integral, devendo as duas opções estarem disponíveis e assim, a aceitação global não seria um método válido, por não oferecer opções individuais. Ademais, as informações devem ser completas, visíveis e destacadas no momento da obtenção do consentimento. Uma simples referência às condições gerais de uso não é suficiente. (CNIL, 2019).

Mediante o exposto, insta trazer que parte da doutrina entende que por vezes, mesmo que haja respeito ao que é preconizado pela lei reguladora, o consentimento obtido será fictício. Isso porque o ato de consentir parte do pressuposto de que o titular vai ter controle sobre o tratamento, o que não é verdade do ponto de vista técnico, configurando-se assim o chamado mito do consentimento (NÓBREGA, 2020, p. 4).

#### **3.4.1. Políticas de privacidade e o consentimento**

A política de privacidade é um documento que toda empresa, que possua tratamento de dados online ou não deve possuir. Através dela, um site ou aplicativo vai explicar as diretrizes sobre um tratamento de dados (BORTOLOZO, 2021, p.1).

Por meio desse documento o usuário será informado quais os dados serão coletados, como isso vai ocorrer, ela também vai dispor a respeito do armazenamento das informações. Em alguns casos essa política vai explicar quais dados são captados a



partir da ferramenta de cookies<sup>1</sup>, em outros casos, isso pode ser explicado em política à parte sobre o tema. O foco da política de privacidade é a proteção não só do cliente, mas também do empreendimento, ao evitar lides e em questões de marketing, com o objetivo aumentar o grau de confiança nas relações com o titular (SEBASTIÃO, 2020 p.112)

Ocorre que na maioria esmagadora dos casos, apesar de conceder a permissão para o tratamento de dados, o usuário na realidade não sabe do que se trata, muito por conta da forma que os sites ou aplicativos ofertam a leitura dos contratos ou termos de permissão, bem como a insistência persuasiva das políticas de privacidade (NÓBREGA, 2020 p. 3).

O procedimento de aceite dos Termos de Uso e Políticas de Privacidade vai influenciar ou até mesmo coagir o usuário ao acessar um site de seu interesse e este possuirá quase ou nenhuma possibilidade de alterar a redação ou efeitos de qualquer das cláusulas dispostas no documento. Obviamente, resta-lhe apenas aceitar os termos propostos ou rejeitá-los e, assim, ter seu acesso à informação, conteúdos, produtos, serviços etc., limitado ou até mesmo impedido (NÓBREGA, 2020 p.3).

Para além disso, as referidas políticas podem contar com cláusulas que não estão em conformidade com o que o ordenamento jurídico preceitua, podendo ser chamadas de cláusulas abusivas. De modo geral, elas são definidas pela violação de direitos ou excessiva desvantagem entre as partes, sendo formulada com base na desigualdade do ganho com a relação. Ademais, a cláusula abusiva também pode ter como objetivo se aproveitar da boa-fé do usuário, como ocorre nos contratos de adesão, que utilizam da necessidade ou falta de instrução do titular oferecendo algo que é supostamente vantajoso em primeiro momento, compelindo-o a aderir ao serviço através do aceite de documento com excesso de termos técnicos, que cede

---

<sup>1</sup> 1“Cookies são pedaços de código que dão a um site uma espécie de memória de curto prazo, permitindo que ele se lembre de pequenos pedaços de navegação” BARREDA, 2021, p.1. Para saber mais a respeito consulte: **Você deve aceitar o uso de cookies na Internet? É melhor pensar duas vezes. Em** <https://www.cnnbrasil.com.br/tecnologia/voce-deve-aceitar-o-uso-de-cookies-na-internet-e-melhor-voce-pensar-duas-vezes/>

acesso ilimitado aos dados pessoais, sem respeito aos seus direitos (SEBASTIÃO, 2020 p.114).

De maneira geral, as políticas de privacidade para coleta de consentimento são longas, difíceis de ler e vagas, o que faz com que o titular de dados não as leia e, na prática, o problema da assimetria da informação não está sendo resolvido. (BORGESIU, 2016, p. 6). Ao solicitar o consentimento, os controladores devem garantir que usem uma linguagem clara e simples em todos os casos. Isso significa que uma mensagem deve ser facilmente compreensível para uma pessoa comum e não apenas para advogados. (ALMEIDA e LUGATI, 2020, p. 25). Ou seja, os controladores não podem usar políticas de privacidade longas e difíceis de entender ou declarações cheias de jargões legais (EUROPENA DATA PROTECTION BOARD, 2020, p. 16). Nesse diapasão é evidente que da forma como ainda ocorre, os cliques no “eu aceito” ao final no texto nem sempre irão refletir claramente a real manifestação de vontade do titular, tendo em vista que nem sempre a leitura é realizada. (ALMEIDA e LUGATI, 2020, p. 25).

Assim, conclui-se que no ambiente online, levando em consideração a opacidade das políticas de privacidade, muitas vezes é mais difícil para os indivíduos conhecer seus direitos e dar consentimento informado. Isso ainda pode ser agravado pelo fato de que, em alguns casos, não é mesmo esclarecido o que constituiria consentimento livre, específico e informado para o tratamento de dados (WORKING PARTY 29, 2011, p. 3 *apud* Europa).

## 4 DARK PATTERNS

Os dark patterns, que ao longo dos anos se tornaram uma forma de coletar o consentimento do titular, estão cada vez mais presentes no mundo virtual. Nesse sentido, o presente capítulo almeja versar a respeito deles, suas classificações e legislações atinentes ao tema.

### 4.1 CONCEITO

Os *Dark Patterns*, que podem ser traduzidos como padrões escuros, obscuros ou ocultos, ainda não têm definição exata ou sequer foram objeto da Legislação de Proteção de Dados no Brasil, sendo apenas abordados pela doutrina.

Esses padrões consistem em mecanismos virtuais presentes em plataformas digitais que induzem o usuários a tomarem decisões não intencionais, que podem ser prejudiciais ao tratamento de seus dados (EUROPEAN DATA PROTECTION BOARD, 2022, p.2). Dessa maneira, designer e parceiros de negócios começaram a desenvolver interfaces enganosas a fim de manipular o usuário. (JAISWAL, 2018, p.1).

Harry Brignull, criador do conceito, as define como uma interface de usuário cuidadosamente elaborada para induzir o titular a fazer coisas que não faria em outra situação, como comprar seguro ou inscrever-se para compras recorrentes. Mais adiante, ele adiciona que é comum que se relacione um design ruim a questões negativas como preguiça ou desleixo, sem que haja algo por trás disso, entretanto isso ocorre de maneira intencional, sem erros. Há nessa ferramenta conhecimentos sólidos de psicologia humana, que serão sobrepostos aos interesses do usuário (BRIGNULL, 2013, p. 2).

Os padrões escuros têm a intenção de influenciar o comportamento dos usuários, de modo que podem prejudicar sua capacidade de proteger efetivamente seus dados pessoais e a possibilidade de fazer escolhas conscientes. (EUROPEAN DATA PROTECTION BOARD, 2022, p.2). É importante destacar que aqui o design vai possuir escolhas profissionais na escolha da interface usada para interagir com o

titular. Além de serem prejudiciais à privacidade do usuário, essas táticas precisam fornecer algum benefício ao provedor de serviço, para que assim sejam classificadas. Isso porque que o titular, desinformado sobre as escolhas de privacidade e sobre como vai ocorrer o tratamento de dados, vai ser induzido a um compartilhamento irrestrito de dados, fomentando uma cultura de divulgação irrestrita e inconsciente de dados pessoais (JAROVSKY, 2022, p. 9-10).

Os artifícios de design usados para o emprego desses padrões são os mais diversos, mas os que ganham destaque são: **configurações padrão**, onde o padrão é sempre o maior compartilhamento de dados possível, que nem sempre são alteradas pelo titular; **escolha de design astuto**, onde o compartilhamento de dados pessoais e o uso de publicidade direcionada são apresentados como exclusivamente benéficos e a desativação levaria à perda de funcionalidade para os usuários; **layout confuso** em que as opções de privacidade geralmente ficam ocultas ou exigem mais cliques para serem acessadas e por meio das ilusões de escolha, onde os serviços obscurecem o fato de que os usuários têm muito poucas opções reais e que o compartilhamento abrangente de dados é aceito apenas pelo uso do serviço (FORBRUKERRÅDET, 2018, p.1). Apesar disso, os padrões obscuros não se limitam a coleta de dados, eles podem afetar outras áreas como como finanças, emoções, atenção e assim por diante (JAROVSKY, 2022, p.4).

Ao abordar o tema, as autoridades norte-americanas e britânicas querem tornar a prática ilegal e multar empresas que a fizerem. Apesar disso, sabe-se que não vai ser fácil, afinal, o design é o reino da subjetividade. (GOMES, 2019, p.1). Nesse sentido, o European Data Protection Board adotou a posição de que as autoridades de proteção de dados são responsáveis por sancionar o uso de padrões obscuros se eles violarem os requisitos do General Data Protection Regulation, Lei de Proteção de Dados Europeia. (EUROPEAN DATA PROTECTION BOARD, 2022, p.1).

#### 4.1.1. NUDGES E DARK PATTERNS

Cumprir salientar que explicação do termo nudge, precisa ser abordada, tendo em vista que esta que é mais uma das muitas espécies de indução a um comportamento, que ao ser utilizada no mundo virtual pode ou não se tornar um Dark Pattern.

Um nudge, que pode ser traduzido de forma livre como um empurrão ou uma cutucada, é qualquer aspecto da arquitetura de escolha que tenha o potencial de alterar o comportamento das pessoas de maneira previsível. Apesar disso, não há proibição e nem altera significativamente seus incentivos econômicos (MATTOS, 2018, p.1 apud THALER AND SUNSTEIN). Esse conceito advém da economia comportamental e da psicologia e tem relação com o fato dos usuários serem levados a fazer determinadas escolhas a partir de um forte incentivo ao compartilhamento de informações, nesse caso (FORBRUKERRÅDET, 2018, p.6).

Apesar disso, nem todos os empurrões serão considerados padrões escuros, levando em consideração que para isso, ele precisará ser manipulador e malicioso. Não possuindo essas duas características atreladas, ele pode ser apenas considerado moralmente problemático ao tentar encorajar o usuário a seguir determinado curso (JAROVSKY, 2022, p.6). Entretanto, se o titular não possui conhecimento das consequências da coleta há assimetria de informação, onde o provedor possui vantagem sobre o usuário, apelando para preceitos psicológicos (FORBRUKERRÅDET, 2018, p. 6).

Esses empurrões podem ser mais úteis em situações em que os usuários enfrentam compensações e cenários incertos e subjetivos que envolvem a consideração de opções potencialmente conflitantes. Muitas decisões de segurança e privacidade se enquadram nessa categoria. Isso ocorre porque os usuários geralmente precisam pesar as considerações de privacidade e segurança em relação a outras prioridades (ACQUIST, *et al*, 2018, p. 27).

É possível ver a relação desse tipo de prática com os *Dark patterns* em caso recente, ocorrido em janeiro de 2022, onde distritos americanos de Washington, Columbia, Texas e Indiana moveram ações contra a Google, alegando que a empresa faz

promessas enganosas sobre a capacidade dos usuários de protegerem seus dados, desde 2015, ao menos. Para além disso, afirmam que a empresa implantou os referidos padrões escuros em seus produtos com objetivo de “cutucar” ou “empurrar” o titular a fornecer cada vez mais dados de localização, violando assim várias leis estaduais e proteção ao consumidor. Dessa forma, os procuradores buscam a partir dessa ação proibir o Google desse tipo de prática e multar a empresa (ZAKRZEWSKI, 2022, p.1)

Assim é evidente que os *dark patterns* em determinados momentos serão constituídos por esses empurrões, mas nem sempre o contrário irá ocorrer.

#### 4.2 LEGISLAÇÕES E OS *DARK PATTERNS*

Os esforços para legislar sobre o tema enfrentam um grande desafio: como definir padrões escuros. Os formuladores de políticas europeus e americanos geralmente concordam que interfaces de usuário enganosas devem ser proibidas, mas a linha tênue entre o marketing legítimo e legítimo e um padrão obscuro dificulta, já que não há resposta. Assim surge um desafio para a ampla regulamentação da tecnologia (MARTINEZ e DELSOL, 2022, p.2). Não obstante a isso, a infâmia dos padrões escuros levou a União Europeia e os oficiais de proteção de dados a especificamente destacar eles como exemplos de não conformidade com a General Data Protection Regulation em seus documentos consultivos (NOUWENS et al. 2019, p. 3).

Buscando regulamentar o tema, o Reino Unido trouxe em 2021 um Código de Design Adequado Para a Idade, conhecido como Código das Crianças (Age Appropriate Design Code). Esse Código estipula definições de alto nível de privacidade, devendo ser aplicado às configurações por padrão nos casos em que ele for uma criança (ou se suspeitar que seja). De acordo ele, existem disposições específicas de que geolocalização e criação de perfil devem estar desativadas por padrão (a menos que haja uma justificativa convincente para tais padrões hostis de privacidade) e, institui que os nudges, já citados previamente, junto com os *dark patterns* são proibidos para obter o consentimento de criança (LOMAS, 2021, p.2 *apud* ICO).

Nesse mesmo sentido, a Lei de Privacidade da Califórnia, conhecida como a California Privacy Rights Act, define os padrões obscuros como uma interface de usuário projetada ou manipulada com o efeito substancial de subverter ou prejudicar a autonomia do usuário, tomada de decisão ou escolha. Essa mesma lei proibiu o uso desse padrão na Califórnia. (CALIFÓRNIA, 2020). Em relação a isso, é válido destacar que esta é a primeira legislação de proteção de dados que afirma expressamente que um acordo obtido através de padrões escuros não enseja em um consentimento válido. O CPRA traz avanços no sentido de privacidade porque a terminologia Padrões Escuros, que decorre de um design de interface, está sendo trazida para o ordenamento, com o intuito de auxiliar na identificação de práticas que afetam negativamente os direitos do titular. Ademais, o fato da Califórnia ser sede de grandes empresas de tecnologia, a legislação tem potencial de possuir um efeito global mais amplo (JAROVSKY, 2022, p.38). Previamente, ainda nos Estados Unidos, os senadores Mark Warner e Deb Fischer elaboraram um projeto de Lei chamado de Detour Act que tinha como objetivo impedir as grandes empresas de se utilizar dos *dark patterns*, mas que não obteve muito sucesso. Dentre as suas muitas disposições o referido projeto considerava ilegal que os sites projetassem, manipulassem, modificassem a interface do usuário com a finalidade de obscurecer, subverter ou prejudicar a autonomia do usuário, a tomada de decisões ou a escolha de obter consentimento ou dados do usuário. Para além disso, as empresas também seriam obrigadas a criar conselhos de revisão para realizar testes do envolvimento dos usuários (ESTADOS UNIDOS, 2019, p.2).

Apesar disso, em outubro de 2021, a Federal Trade Commission, dos Estados Unidos, emitiu uma declaração alertando sobre políticas de fiscalização dos *dark patterns*. Eles alertaram as empresas a respeito da implementação desses padrões, que enganam os consumidores e em resposta a insatisfação deles por conta dos danos causados, as fiscalizações deverão aumentar. A declaração de política da FTC avisa as empresas de que enfrentarão ações judiciais se o processo de inscrição não fornecer informações claras e iniciais, obter o consentimento informado dos consumidores e facilitar o cancelamento. (ESTADOS UNIDOS, 2021, p.1). Para além disso, decidiu-se que para o tratamento, as empresas devem seguir 3 requisitos

chave, são eles: divulgação de forma clara e visível todos os termos materiais do produto ou serviço; Obter o consentimento expresso do consumidor; Fornecer cancelamento fácil e simples para o consumidor. (ESTADOS UNIDOS, 2021, p.1)

Ainda com o objetivo de combater os *Dark patterns*, a lei de Privacidade do Colorado traz disposição que afirma que não é válido o consentimento obtido através dos padrões obscuros (COLORADO, 2021).

No Canadá, a Lei federal de Proteção de Informações Pessoais e Documentos Eletrônicos (“PIPEDA”) não vai dispor exatamente sobre os padrões obscuros, mas vai reger a coleta, uso e divulgação de dados pessoais de usuários de mídia social. A Lei canadense exige que as organizações obtenham consentimento e informem os indivíduos sobre o propósito de coletar, usar ou divulgar tais informações. (AHMAD E COROVIC, 2022, p. 2). Apesar da PIPEDA não fazer distinção entre adultos e jovens, o Office of the Privacy Commissioner of Canada tem consistentemente visto informações pessoais de jovens e crianças como sendo particularmente sensíveis e recomendou limitar ou evitar totalmente sua coleta, sempre que possível. (AHMAD e COROVIC, 2022, p. 2). Com o objetivo de salvaguardar o titular, em 2019, o CNIL, órgão francês de Proteção de Dados publicou uma nova diretriz a respeito do uso de cookies, que deveria começar a valer no mesmo ano (CNIL, 2019, p.1). Ocorre que em 2022, após algumas investigações, a Entidade acusou o Google e o Facebook de usar padrões escuros, de maneira que tornam a recusa do uso de cookies mais difíceis que sua aceitação, o que iria afetar a liberdade de consentimento. Assim, as duas empresas foram condenadas a multas de 60 milhões de euros, por não conformidade com a Lei Francesa (CNIL, 2022, p.1).

Por fim, em março de 2022, o Conselho de Proteção de dados Europeu, que já possuía uma guia de 2020 sobre consentimento, lançou um guia chamado de “*Dark patterns* na plataformas de mídias sociais: como reconhecê-los e evitá-los” (EUROPEAN DATA PROTECTION BOARD, 2022, p.1).



### 4.3 CLASSIFICAÇÃO DOS *DARK PATTERNS*

Apesar de ainda ser um tema inicial, com poucas legislações, já existem algumas classificações dos padrões obscuros, feitas por doutrinadores do tema, que podem auxiliar o titular a entender e conseqüentemente reconhecer esses padrões quando se encontrar diante deles e serão úteis para guiar a análise de padrões obscuros realizada por esse trabalho.

#### 4.3.1. CLASSIFICAÇÃO SEGUNDO BRIGNULL

Harry Brignull, que iniciou os estudos a respeito dos *Dark patterns*, adicionou algumas categorias de *Dark patterns*, de maneira sintética, de modo que ao longo dos anos, outros estudiosos desenvolveram outras classificações. Ele os classifica como:

##### 4.3.1.1. Pergunta de Truque ou *Trick Question*

Ocorre quando o usuário preenche um formulário com perguntas que o levam a responder coisas que não pretendia, de modo que a pergunta dá a entender algo, mas na verdade quer saber outra coisa, com fulcro na manipulação do usuário, isso normalmente ocorre nos registros de usuário (BRIGNULL, 2011, p.1)

##### 4.3.1.2. Esgueirar-Se Na Cesta ou *Sneak Into The Basket*

Acontece quando o usuário tenta comprar algo, mas em algum momento da jornada de compra o site insere um item adicional em sua cesta. (BRIGNULL, 2011, p.1).

##### 4.3.1.3. Barata De Motel ou *Roach Motel*

É o caso em que o controlador oferece facilidade para adquirir determinada coisa, mas impõe muitas dificuldades ao usuário para sair, como nos casos de uma assinatura premium (BRIGNULL, 2011, p.1).

##### 4.3.1.4. Zuckering de Privacidade

Evidente no caso em que o titular é levado a compartilhar mais informações do que pretendia, sendo o nome em homenagem ao CEO do Facebook à época, Mark Zuckerberg (BRIGNULL, 2011, p.1).

#### 4.3.1.5. Prevenção de Comparação de Preço

Ocorre quando O varejista torna difícil a comparação do preço de um item com outro o que dificulta a tomada de decisão informada (BRIGNULL, 2011, p.1).

#### 4.3.1.6. Desvio

O design é focado, de maneira proposital, a desviar a atenção de uma coisa para outra, de modo que o titular nem sempre têm noção de tudo o que está ocorrendo (BRIGNULL, 2011, p.2).

#### 4.3.1.7. Despesas Ocultas

Ao final do processo, o titular vai se deparar com cobranças inesperadas. É comum em sites de compras online, que durante todo o processo se silenciam sobre outras despesas que o consumidor vai ter e, ao final, depois que ele investiu tempo escolhendo, preenchendo seus dados, vai ser compelido a pagar (BRIGNULL, 2011, p.2).

#### 4.3.1.8. Isca e Troca

O titular se propõe a realizar determinada ação, mas algo diferente acontece, sem depender de sua vontade (BRIGNULL, 2011, p.2).

#### 4.3.1.9. Anúncios Disfarçados

São anúncios disfarçados de conteúdo ou navegação, para que o titular entre nele. (BRIGNULL, 2011, p.2).

#### 4.3.1.10. Confirmar Vergonha

Aqui a opção de recusa é feita de maneira que venha a culpar ou envergonhar o titular por não concordar com algo da plataforma (BRIGNULL, 2011, p.2).

#### 4.3.1.11. Continuidade Disfarçada

Ocorre quando o período de avaliação gratuita termina e o valor começa a ser creditado na conta do cliente sem aviso prévio (BRIGNULL, 2011, p.2).

#### 4.3.1.12. Spam de Amigos

O produto solicita permissões de e-mail ou mídia social do usuário, sob o pretexto de que será usado para um resultado desejável, como encontrar amigos. Apesar disso, ela irá a todos os contatos em uma mensagem que afirma ser enviada pelo titular (BRIGNULL, 2011, p.2).

#### **4.3.2. CLASSIFICAÇÃO DE ACORDO COM A TAXONOMIA DE BRIGNULL**

Em uma pesquisa a respeito dos Padrões Obscuros, GRAY, KOU, BATTLES, HOGGATT e TOOMBS criaram uma classificação de como esses padrões podem ser utilizados em desfavor do titular de dados. Essa categorização se baseia e se relaciona com a taxonomia de Brignull, mas busca articular motivadores estratégicos por meio de um processo acadêmico rigoroso de integração e refinamento, de modo que cria categorias onde a classificação anterior pode ser encaixada (GRAY, KOU, BATTLES, HOGGATT e TOOMBS, 2018, p.5)

##### 4.3.2.1. Irritante

A primeira categoria, chamada de irritante, é composta por um pequeno redirecionamento de funcionalidade, que pode persistir em uma ou mais interações. É uma manifestação intrusa, que interrompe a atividade do usuário. Os comportamentos irritantes podem incluir pop-ups que escurecem a interface, avisos de áudio que distraem o usuário ou outras ações atrapalham o foco. (GRAY, KOU, BATTLES, HOGGATT e TOOMBS, 2018, p.5)

##### 4.3.2.2. Obstrução

É definida como um impedimento do fluxo de uma tarefa, tornando a interação mais difícil que o necessário, é uma espécie de barreira à navegação. Um exemplo dessa obstrução são as barreiras que interrompem a funcionalidade incentivando que a pessoa pague a assinatura da plataforma. (GRAY, KOU, BATTLES, HOGGATT E TOOMBS, 2018,2020, p.5).

Aqui vai haver um subtipo chamado de moeda em que o usuário é compelido a converter uma moeda real em moeda virtual, de modo que ele é desconectado do

valor real, fazendo com que ele interaja com a moeda virtual de maneira diferente. . (GRAY, KOU, BATTLES, HOGGATT E TOOMBS, 2018, p.5).

Essa classificação vai se relacionar com os padrões "Roach Motel", "Prevenção da Comparação de Preço",

#### 4.3.2.3. Sorrateira

Acontece de maneira a tentar disfarçar ou atrasar a divulgação de informações que seriam relevantes ao usuário. É uma furtividade para fazer o usuário executar uma ação a qual ele iria se opor, se tivesse conhecimento. Esse padrão de *Dark patterns* pode incluir a adição de custos não esperados, mesmo depois do cancelamento. (GRAY, KOU, BATTLES, HOGGATT E TOOMBS, 2018, p. 6)

Ao relacionar com a taxonomia de Brignull veremos os seguintes padrões: "Padrão de Continuidade Forçada", de "Custos Ocultos", a "Adição de itens não escolhidos ao carrinho" e a "Isca e Troca" (GRAY, KOU, BATTLES, HOGGATT E TOOMBS, 2018, p. 6)

#### 4.3.2.4. Interferência de interface

Ocorre através da manipulação da interface que privilegia ações específicas sobre outras, confundindo o usuário ou limitando a descoberta de possibilidades de ação importantes. Essa interferência pode ser vista em ilusões visuais e interativas, se dividindo ainda em subtipos:

- informações ocultas: a ideia consiste em ocultar informações relevantes ao usuário. Isso pode ocorrer através de letras miúdas, textos descoloridos ou declaração de termos e condições de um produto. O objetivo aqui será disfarçar informações relevantes, para que pareçam irrelevantes. (GRAY, KOU, BATTLES, HOGGATT E TOOMBS, 2018, p. 7)
- pré-seleção: ocorre nos casos em que uma opção já é selecionada por padrão, antes mesmo da interação com o usuário. Desse modo, o controlador vai escolher opções contrárias ao interesse do titular, em benefício próprio, sendo muito provável que o usuário concorde por não saber das implicações de sua escolha. (GRAY, KOU, BATTLES, HOGGATT E TOOMBS, 2018, p.7)

- manipulação estética: é a manipulação da interface do usuário, de forma que vai ocasionar em distração ou convencimento do titular. (GRAY, KOU, BATTLES, HOGGATT E TOOMBS, 2018, p.7)

Na tipologia de Brignull esses padrões se relacionam com “Brincar com emoções”, “Hierarquia falsa”, Padrão de Anúncio disfarçado”, “Perguntas para Enganar”

#### 4.3.2.5. Ação forçada

A ação forçada é uma forma de exigir que o usuário execute uma ação específica, para que assim, alcance o que deseja. Pode ser uma etapa necessária para concluir um processo ou pode aparecer disfarçada como uma opção da qual o usuário se beneficia muito. Um exemplo comum é nos casos de sistemas de computador, em que o usuário é obrigado a atualizar para que consiga desligar. (GRAY, KOU, BATTLES, HOGGATT E TOOMBS, 2018, p. 8).

Essa classificação vai se relacionar com os padrões "Privacy Zuckering" e "Gamificação de Brignull" (GRAY, KOU, BATTLES, HOGGATT E TOOMBS, 2018, p. 8).

### 4.3.3. CLASSIFICAÇÃO EUROPEAN DATA PROTECTION

Outra classificação relevante de trazer à baila é a lançada pelo European Data Protection Board em 2022, ao publicar Diretrizes que ajudam o titular a reconhecer os padrões obscuros em plataformas de mídias sociais. (EUROPEAN DATA PROTECTION BOARD, 2022, p.1).

#### 4.3.3.1. Sobrecarga

Está evidente a sobrecarga nos casos em que usuários são confrontados com uma avalanche/grande quantidade de solicitações, informações, com objetivo de induzir ao compartilhamento de um número maior de dados ou permitir involuntariamente o tratamento de dados, que iria de encontro com as expectativas do titular. Nessa categoria, os três tipos de padrões obscuros que podem ser observados são: “solicitação contínua”, “labirinto de privacidade” e o “uso de muitas opções”. (EUROPEAN DATA PROTECTION BOARD, 2022, p.2).

#### 4.3.3.2. Ignorar

Acontece quando o sistema projeta a interface ou experiência do usuário de forma que os usuários esqueçam ou deixem de pensar em todos ou alguns dos aspectos de proteção de dados. Os padrões obscuros que estão inclusos nessa categoria são: “Aconchego enganoso” e “Olhe para lá” (EUROPEAN DATA PROTECTION BOARD, 2022, p.2).

#### 4.3.3.3. Agitação

Vai agir de modo a afetar as escolhas do usuário a partir de interações que apelam para o emocional ou através de interações visuais. Nessa categoria estão inseridos os padrões chamados de “direção emocional” e “oculto à vista de todos” (EUROPEAN DATA PROTECTION BOARD, 2022, p.2).

#### 4.3.3.4. Impedir

O impedimento ocorre através da obstrução ou bloqueio dos usuários em seu processo de se tornarem informados ou de gerenciar seus dados, o que torna as ações difíceis ou impossíveis de serem realizadas. Os tipos de padrões observadas aqui são “beco sem saída”, “mais longo que o necessário” e “informações enganosas”. (EUROPEAN DATA PROTECTION BOARD, 2022, p.2).

#### 4.3.3.5. Inconstância

Ocorre nos casos em que o design não é claro, dificultando a navegação do usuário pelas diferentes ferramentas de controle de proteção de dados e, por conseguinte, a sua compreensão da finalidade do tratamento de seus dados. Podem ser observados nessa categoria os padrões “sem hierarquia” e “descontextualizando” (EUROPEAN DATA PROTECTION BOARD, 2022, p.2).

#### 4.3.3.6. Deixado no escuro

Deixados no escuro ocorre quando uma interface é projetada de forma que oculta informações ou ferramentas de controle de proteção de dados ou nos casos em que deixa os usuários inseguros sobre como seus dados são tratados e que tipo de controle eles podem ter sobre o exercício de seus direitos. Pode ser observado na

referida categoria o padrão de “linguagem descontinuada”, “conflito de informação” e “informações ambíguas” (EUROPEAN DATA PROTECTION BOARD, 2022, p.2).

#### 4.4 USER EXPERIENCE

O Design é um ato persuasivo que cria uma mudança intencional no mundo e que, direta ou indiretamente, vai induzir a mudança comportamental ou social (GRAY *et al.*, 2016 p.2). Apesar disso, o design difere de manipulação, devendo apenas convencer, havendo não apenas uma diferença semântica, mas moral, podendo possuir abuso de poder, não sendo aceitável em nenhuma circunstância (BOWLES, 2022, p.2).

O UX Design, ou User Experience, traduzido de maneira livre para Design de Experiência ou Experiência de Usuário é uma forma de design. É realizado através de abordagem ou metodologia multidisciplinar composta por vários aspectos que isolados não conseguem entregar uma boa experiência. Essa experiência criada vai refletir nas percepções da interação entre o usuário e uma empresa e pode ser uma experiência positiva ou negativa (ALBUQUERQUE, 2020, p.2).

A ISO 9241-210:2019, que versa sobre Ergonomia da interação do Homem com Sistema vai definir o *user xperience* como as percepções e respostas do usuário, que resultam do uso de um produto ou serviço. Essas percepções e respostas incluem as emoções, crenças, preferências, percepções, conforto, comportamentos e realizações dos usuários que ocorrem antes, durante e após o uso. A referida experiência vai ser uma consequência da imagem, da marca, da apresentação, funcionalidade, desempenho do sistema, comportamento interativo e recursos assistivos de um sistema, produto ou serviço. Isso vai ser combinado o estado interno e físico do usuário, que resulta de experiências anteriores, atitudes, habilidades, habilidades e personalidade; e do contexto de uso (ISO 9241-210, 2019, p. 5).

Nesse sentido, Tanaka afirma que é uma área do conhecimento que analisa, planeja e projeta a jornada dos usuários ao utilizarem determinado produto ou serviço. Por conta disso, vai requerer um uma visão holística do que é projetado, buscando entender o contexto e os agentes. (TANAKA, 2019, p. 11).

É importante observar que o design tem poderes que podem influenciar nas escolhas do titular, de modo que elas nem sempre reflitam o que ele verdadeiramente deseja. (WALDMAN, 2019, p. 5). Assim são os padrões obscuros, são utilizados artifícios da Experiência do Design de modo que o usuário seja induzido a determinado comportamento (BROWNLEE, 2016, p.1). As plataformas podem usar de manipulação para manter o fluxo de dados, que alimentam seus poderes de negócio, resultando disso esses padrões obscuros (WALDMAN, 2019, p. 5).

Dessa maneira, no design com base em *dark patterns*, a interface será criada com base no que usuário irá buscar, tentando prever a necessidade e acomodar os seus desejos (FORBRUKERRADET, *apud* WOODROW HARTZOG, 2018, p. 6). Os efeitos desse design são que os indivíduos tendem a ser influenciados por uma variedade de vieses cognitivos, muitas vezes sem estarem cientes disso. Assim, tendem a escolher recompensas menores a curto prazo. (FORBRUKERRADET *apud* USABILITY GOV, 2018, p. 6).

#### 4.5 PRIVACY BY DESIGN

Privacy by Design, em tradução livre significa Privacidade pelo design. É um conceito que desenvolvido por Ann Cavoukian em 1990, que se relaciona com Tecnologias de Informação, Comunicação e sistemas de dados em redes de grande escala. Ele avança na visão de que a privacidade não deve ser assegurada apenas com a conformidade à marcos regulatórios, devendo ser um padrão da organização em seu modo de operar, tendo como objetivo garantir a privacidade (CAVOUKIAN, 2011, p.1).

Esse conceito é dividido ainda em 7 princípios: (i) a privacidade deve ser regra central; (ii) a ideia de que deve haver sempre proatividade e não reação; (iii) privacidade deve ser incorporada à concepção do projeto, (iv) bem como na usabilidade e em suas funcionalidades; (v) deve haver segurança de ponta a ponta, durante todo o seu ciclo de vida; (vi) a transparência é fundamental e; é necessário o respeito à privacidade do cliente do usuário (CAVOUKIAN, 2011, p.2).

Feita essa breve introdução, podemos afirmar que o “Privacy by Design” representa uma mudança no modo de garantir a privacidade e a proteção de direitos e liberdades dos indivíduos. Isso porque é pensado e incorporado às práticas de negócio



antecipadamente, ou seja, desde o momento inicial quando são concebidos os processos produtivos, procedimentos e mecanismos internos do processamento de dados pessoais por Controladores, Operadores e terceiros (ÓPICE BLUM, 2021 p. 19).

Essa ideia é trazida na lei geral de proteção de dados em seu artigo 46, complementado por seu § 2. Este dispositivo imputa aos agentes de tratamento o dever de adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. É reforçado que essas medidas devem ser observadas desde a fase de concepção do produto ou serviço, até a sua execução (BRASIL, 2018).

## **5 CONSENTIMENTO, *DARK PATTERNS* E USER XPERIENCE**

Os dark patterns, conforme visto anteriormente, estão cada vez mais presentes no mundo virtual. Desse modo, o capítulo em seguida objetiva ilustrar o emprego destes, através do *user xperience*, de forma que ocorre a coleta de consentimento.

### **5.1 ANÁLISE TEÓRICA DA OCORRÊNCIA DOS INSTITUTOS**

É evidente que os padrões obscuros não ocorrem apenas durante o tratamento, mas se iniciam no momento prévio à coleta de dados, através da interface do design, (JAROVSKY, 2022, p.33).

O uso das ferramentas de design se liga diretamente ao emprego desses padrões, de modo que o controlador irá induzir o titular ao fornecimento de um consentimento que, em muitos aspectos, é incompatível com a Lei Geral de Proteção de Dados. Nesse sentido, Leal traz que é evidente que o princípio da transparência se faz inestimável para conferir licitude ao tratamento de dados. Aborda também que a ausência de conduta transparente no tratamento de dados tem a capacidade de macular os atos posteriores, podendo caracterizar um vício de consentimento na medida em que os

padrões obscuros utilizados. Assim, com a utilização desses padrões é possível afirmar que, parece inverossímil admitir a caracterização de um consentimento livre, inequívoco e informado nos casos em que eles são utilizados (LEAL, 2021, p.2).

Os provedores de serviços online se tornaram cada vez mais sofisticados para enganar os usuários para que entreguem suas informações pessoais (BÖSCH, ERB, KARGL, KOPP e PFATTHEICH, 2016, p.1) e os padrões escuros podem destacar dicas para compartilhamento de dados em redes sociais enquanto ocultam os perigos de sua divulgação. (WALDMAN, 2019, p.6). A utilização de cookies pode ilustrar essa discussão, ao passo que o controlador ao explicar esse tratamento não permite que o titular compreenda os efeitos decorrentes de sua escolha (LEAL, 2021, p.2).

Sobre esses provedores, o relatório do Conselho de Consumo Norueguês traz que eles utilizam técnicas de design (como as já explicadas anteriormente) para induzir o usuário a determinadas opções. Por si só, isso não representa o problema, a questão é que o uso padrões obscuros através do design é sem dúvida uma tentativa antiética de empurrar os consumidores para escolhas que não os beneficiam, levando em consideração que essas táticas podem ser enganosas e manipuladoras (FORBRUKERRADET 2018, p.5). Disso surge o debate envolvendo o limite entre o desenvolvimento de um design persuasivo e a necessidade de transparência para que o consumidor consiga apresentar o seu consentimento de forma livre. (COUTO, 2021, p.2). Um desafio para a coleta adequada de consentimento são os extremos entre a falta de informação e o excesso dela, de forma técnica e sem contexto. É difícil sustentar que cookie banners e pop-ups de apps apresentam, em geral, informação suficiente para uma escolha consciente por parte do usuário. (SUNDFELD e FERNANDES, 2021, p.6)

Ao utilizar padrões obscuros, a vulnerabilidade do titular é explorada, dificultando a preservação de sua privacidade, em troca de facilidades oferecidas, impondo a cessão de dados para que o usuário conquiste determinada funcionalidade. Isso é observado nos casos em que há o uso de cookies, onde práticas ocultam os padrões de coleta de dados pessoais, de forma que comprometem a autonomia da vontade

do indivíduo e desafiam a conformidade às Leis de Proteção de Dados. (LEAL, 2021, p.1).

Apesar das ferramentas de marketing serem utilizadas em desfavor do titular, existem modelos alternativos de design que podem ser favoráveis ao titular. Sundfeld e Fernandes afirmam que uma alternativa ao “tudo ou nada” poderia ser a utilização de estratégias que possibilitem ao usuário uma visão inicial, por um padrão simples e de maneira agrupada em relação às finalidades para as quais as cookies estão sendo executadas. Assim seria dada ao titular a possibilidade de escolha e iria inserir a transparência no processo. Ademais, é necessário que a linguagem seja alterada, como forma de assegurar que o público-alvo irá compreender. Uma alternativa trazida seria oferecer ao usuário um conteúdo detalhado em relação a cada cookie executado, quais os dados e com quem são compartilhados. (SUNDFELD e FERNANDES, 2021, p.6). Aqui o papel do designer especialista em UX (“*user experience*” – experiência do usuário) é essencial para chegar a um consenso na discussão. Isso porque a experiência virtual do usuário é desenvolvida por ele, de modo que ele deverá focar em desenvolver soluções focadas na usabilidade e não em impulsionar os *dark patterns*. Dessa maneira, é possível proporcionar ao usuário sensação de felicidade e assegurando que ele seja capaz de responder de forma adequada aos estímulos. Assim, o UX designer também tem um escopo de atuação cada vez mais atrelado à proteção de dados, tendo em vista que irá desenvolver os mecanismos que irão levar o usuário a fornecer um consentimento válido, de acordo com os parâmetros exigidos legalmente pela LGPD (COUTO, 2021, p.2).

Ou seja, é possível utilizar a UX a favor da privacidade, desde que, aperfeiçoando a transparência de produtos e serviços, customizando experiências, facilitando a compreensão do usuário e, de fato, dar controle ao titular sobre como seus dados são tratados. (SUNDFELD e FERNANDES, 2021, p.6). Não bastam políticas com vocabulários rebuscados, devendo essa ideia ser premissa básica na fase de formulação dos sistemas, projetos, serviços ou produtos da empresa, sendo isso elaborado a partir do Privacy by Design. Devem ser adotadas salvaguardas que impliquem em elevação da proteção jurídica e da segurança da informação para os dados pessoais; possibilitem ao indivíduo um maior controle sobre seus dados e,

consequentemente, propiciam um ambiente de negócios mais seguro, ético e sustentável (ÓPICE BLUM, 2021, p.19). Somados estes elementos, a UX tem, enfim, papel chave em tornar o consentimento livre, informado e inequívoco, tal como exige a LGPD (SUNDFELD e FERNANDES, 2021, p.6).

## 5.2 ANÁLISE PRÁTICA DOS *DARK PATTERNS*

Serão relatados alguns padrões obscuros observados em alguns sites e replicados nas mais diversas plataformas. Eles serão mostrados a fins exemplificativos, com fulcro em explanar como as estratégias já abordadas anteriormente são aplicadas no mundo digital.

### 5.2.1. GOOGLE

A Google começou como um mecanismo de busca na internet, usando um algoritmo proprietário projetado para recuperar e ordenar os resultados da pesquisa, que fornece as fontes de dados mais relevantes e confiáveis possíveis. A missão declarada da empresa é "organizar as informações do mundo e torná-las universalmente acessíveis e úteis". Ao longo dos anos a ferramenta se tornou o maior buscador do mundo, posição que gerou críticas e preocupação com o poder que tem de influenciar o fluxo de informações online (TECHOPEDIA, 2020, p.1). Para além disso, nos últimos anos a empresa se expandiu atuando na área de e-mail, anúncios, plataforma de vídeos, plataforma de sistemas de apresentação e documentos, entre outras áreas.

A referida empresa é uma das plataformas que possui diversos mecanismos de Padrões Obscuros, em seus diversos serviços, existindo estudo do Conselho de Consumidor a respeito deste, que será citado mais adiante.

Para ilustrar como o processo ocorre aqui, foi criado um perfil na plataforma, a partir do navegador de um computador, utilizando o sistema Google Chrome, com objetivo de demonstrar algumas das etapas que acabam por induzir o titular ao compartilhamento de dados. Inicialmente ao acessar a página de cadastro são

coletados dados como nome e sobrenome, telefone, e-mail de recuperação, data de nascimento e gênero.

---

**Google**

## Criar sua Conta do Google

Nome  Sobrenome

Nome de usuário  @gmail.com

Você pode usar letras, números e pontos finais

Disponível: **mariapix436**


[Usar meu endereço de e-mail atual em vez disso](#)

Senha  Confirmar

Use oito ou mais caracteres com uma combinação de letras, números e símbolos

Mostrar senha

[Faça login em vez disso](#)



Uma única conta. Todo o Google trabalhando para você.

**Figura 1** – Tela 1 de Cadastro de Conta Google

Fonte:

<https://accounts.google.com/signup/v2/webcreateaccount?flowName=GlifWebSignIn&flowEntry=SignUp>

**Figura 2 – Tela 2 de Cadastro da Conta Google**

Fonte:

<https://accounts.google.com/signup/v2/webcreateaccount?flowName=GlifWebSignIn&flowEntry=SignUp>

Aqui há a possibilidade do usuário saber a finalidade específica para o tratamento desses dados, através do botão “Por que pedimos essas informações”, mas é possível observar também que ao longo do processo há a utilização de imagens lúdicas, que buscam passar algumas mensagens ao titular, usando assim o Padrão (classificado por Gray *et. Al*, 2018, p.7) como Manipulação Estética

Ao dar seguimento ao processo, depois de fornecer as informações consideradas obrigatórias, ele será direcionado a uma página que aborda de maneira resumida

algumas questões relacionadas à privacidade, possibilitando que o usuário acesse sua política de privacidade e termos de serviço em página anexa:


## Privacidade e Termos

Para criar uma Conta do Google, você precisa concordar com os [Termos de Serviço](#) abaixo.

Além disso, quando você cria uma conta, nós processamos seus dados pessoais conforme descrito na nossa [Política de Privacidade](#), incluindo:

### Os dados que processamos quando você usa o Google

- Quando você configura uma Conta do Google, nós armazenamos as informações fornecidas, como seu nome, endereço de e-mail e número de telefone.
- Quando você usa os serviços do Google para atividades como escrever uma mensagem no Gmail ou comentar em um vídeo do YouTube, nós armazenamos as informações que você cria.
- Quando você pesquisa um restaurante no Google Maps ou assiste a um vídeo no YouTube, por exemplo, nós processamos informações sobre essa atividade, incluindo informações como o vídeo que você assistiu, códigos de dispositivos, endereços IP, dados de cookies e o local.
- Também processamos os tipos de informação descritos acima quando você usa apps ou sites que usam serviços do Google como anúncios, o Google Analytics e a plataforma de vídeo do YouTube.



Você controla os dados que coletamos e a forma como eles são usados

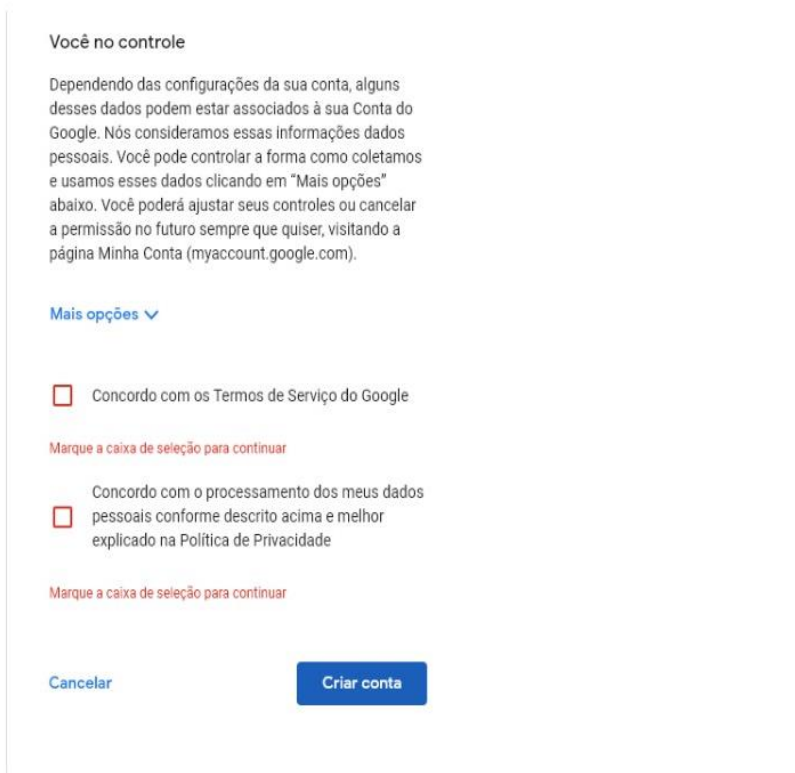
**Figura 3 – Privacidade e Termos**

Fonte:

<https://accounts.google.com/signup/v2/webcreateaccount?flowName=GlifWebSignIn&flowEntry=SignUp>

Será informado de maneira resumida e não muito clara ao titular sobre algumas etapas do processamento de dados. Ademais, a plataforma afirma que o titular possui controle sobre seus dados, mas impõe que o acesso deve ser realizado através de outro site, “My Account”, onde é possível que ele administre as informações pessoais dele, o que consiste no uso de mais um padrão escuro. Depois disso ele será obrigado a consentir com os dois termos, que foram resumidos e possuem alguns pontos a

respeito do tratamento ocultados do usuário, para que seja possível finalizar o cadastro:



The screenshot shows a web form for accepting terms. At the top, it says "Você no controle" (You in control) and explains that users can manage their data through their Google account settings. Below this is a link for "Mais opções" (More options). The main part of the form contains two checkboxes, both of which are unchecked. The first checkbox is labeled "Concordo com os Termos de Serviço do Google" (I agree with the Google Terms of Service). Below it is a red prompt: "Marque a caixa de seleção para continuar" (Check the selection box to continue). The second checkbox is labeled "Concordo com o processamento dos meus dados pessoais conforme descrito acima e melhor explicado na Política de Privacidade" (I agree with the processing of my personal data as described above and better explained in the Privacy Policy). Below it is another red prompt: "Marque a caixa de seleção para continuar" (Check the selection box to continue). At the bottom left is a "Cancelar" (Cancel) link, and at the bottom right is a blue "Criar conta" (Create account) button.

**Figura 4 – Aceite de Termos**

Fonte:

<https://accounts.google.com/signup/v2/webcreateaccount?flowName=GlifWebSignIn&flowEntry=SignUp>

É evidente no caso que a todo momento é passada a ideia ao titular de que ele possui o controle de seus dados. Apesar disso, é imposta a ele dificuldade maior que o necessário e até ocultas, de modo que pode impossibilitar que ele tenha o controle sobre suas informações, conforme será visto adiante.

Pode-se observar também o contraste dos botões azuis para aceitar e, neste caso, nenhuma opção de configurar a informação, para que se adeque ao desejo do titular. O conselho norueguês vai dizer que isso é um padrão que é para ajustar as



configurações fora do padrão, sendo assim design destinado a cutucar os usuários, tornando a escolha 'pretendida' mais saliente" (FORBRUKERRÅDET, 2018, p. 20).

Dessa forma, fica evidente que inicialmente o site vai utilizar-se de padrões obscuros para ocultar informações do titular. Analisando esse tratamento inicial, é possível reconhecer padrões explanados previamente, ao fornecer fragmentos de informação, que se resumem basicamente às ideias de que: "todos os dados criados durante a navegação na plataforma e em outros sites serão armazenados"; "que esses dados podem ser utilizados para o desenvolvimento de anúncio personalizado" e "para conduzir análises do sistema".

Apesar disso, em nenhum momento é deixado claro ao titular que esses dados serão unificados na base de dados, retidos por tempo indeterminado e utilizados para uma formação de perfil detalhada a respeito dele, que pode incluir informações como renda familiar, estado civil, gênero (mesmo que o titular tenha optado por não informar anteriormente), tipo de aparelho celular utilizado, interesses de compras, categoria de filme que interessa ao titular, status parental (se possui filhos ou não) e mais uma lista exaustiva de informações. Vale salientar que, apesar da plataforma explicar que essas informações são utilizadas para anúncios, não fica claro na página de cadastro como essas informações são tratadas para tal. Ademais, é informado que os dados de navegação podem ser usados por parceiros para anúncio, sem que fique claro quem são estes e as diretrizes para essas transferências. Essa é uma configuração padrão da plataforma, que só poderá ser desabilitada manualmente em um dos sites da Google e, ainda assim, para que isso ocorra, o titular precisa ser direcionado para, ao menos, 3 páginas diferentes.

Sobre isso o conselho do consumidor Norueguês afirma que Google vai trabalhar com configurações padrão pré-selecionadas para as opções menos favoráveis à privacidade. Além disso, haverá ocultação das configurações pré-selecionadas para que os usuários que simplesmente clicarem nos botões "Concordo" ou "Aceitar" e nunca vejam as configurações, tornando é difícil saber o que está pré-selecionado, representando assim o emprego dos Padrões Obscuros (FORBRUKERRÅDET, 2018, p. 18).

Depois que a conta é criada, o usuário poderá utilizar-se normalmente dos benefícios oferecidos pela empresa. Apesar disso, existem dois sites distintos, para fazer o controle da privacidade do usuário.

O primeiro deles é o chamado “my account”, que pode ser acessado através da busca por “Privacidade da minha conta” no buscador da plataforma e oferece um checkup de privacidade ao usuário, tendo como padrões o uso de alternativas que não são favoráveis ao titular. Esse checklist de privacidade oferece apenas 3 etapas: “Excluir automaticamente a Atividade na Web e de apps” Excluir automaticamente o Histórico do YouTube” e “Criar um plano para sua conta”. Desse modo, pode ser observado que apenas algumas das informações relacionadas à privacidade estão inseridas nesse site, havendo uma fragmentação da informação. Isso irá se relacionar com o padrão Inconstância (classificação DE EUROPEAN DATA PROTECTION BOARD, 2022, p. 2)



**Figura 5 – Sugestões de Privacidade**

Fonte: <https://myaccount.google.com/data-and-privacy>

A outra ferramenta utilizada pela plataforma para gerenciar consentimentos fornecidos pelo usuários no que tange à suas informações pessoais é o site “My Activity”, que é acessado quando este busca diretamente por ele na plataforma.

Excluir atividade por

Outra atividade

Controles de atividade

Conta do Google 

Ajuda e feedback



## Minha atividade no Google.

A atividade que você guarda permite melhorar os serviços do Google, oferecendo recursos como a redescoberta do que você pesquisou, leu e assistiu.

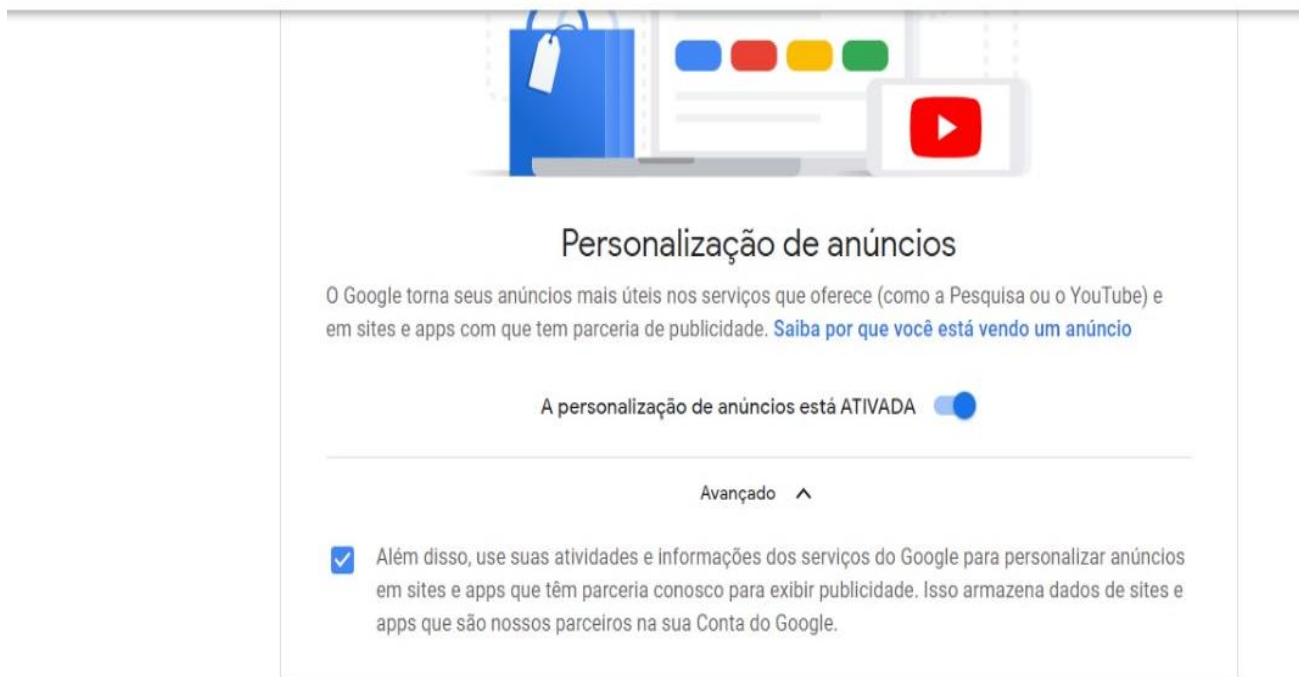
Você pode ver e excluir sua atividade usando os controles disponíveis nesta página.

Atividade na Web e de apps <input checked="" type="checkbox"/> Ativada >	Histórico de localização <input type="checkbox"/> Desativada >	Histórico do YouTube <input checked="" type="checkbox"/> Ativada >
-----------------------------------------------------------------------------	-------------------------------------------------------------------	-----------------------------------------------------------------------

**Figura 6 – Minha atividade**

Fonte: <https://myactivity.google.com/myactivity>

Ao acessar a o site, o usuário ainda precisar passar por mais de uma tela e menu de configurações para chegar até a personalização de anúncios. A informação fica escondida no menu lateral, de modo que ele precisará clicar na opção “outra atividade”, descer a tela e ir em busca de “Configurações de Anúncios no Google”, onde vai clicar e será redirecionado à outra página, onde pode ocorrer o gerenciamento de suas informações



**Figura 7 – Personalização de Anúncios**

Fonte: [https://adssettings.google.com/authenticated?hl=pt\\_BR](https://adssettings.google.com/authenticated?hl=pt_BR)

Há aqui a configuração padrão, que opta por disponibilizar os dados do usuário para a personalização de anúncios. O consentimento utilizado foi fornecido anteriormente, ao criar a conta, apesar disso, **não há para o titular a oportunidade inicial de não aceitar essa opção**, de modo que ele precisa ir em busca do referido site para optar que esse tratamento não ocorra.

Na mesma página é possível observar as informações do usuário coletadas pela plataforma, ao longo do tempo que ele a utiliza:

### Como seus anúncios são personalizados

Os anúncios são baseados nas informações pessoais que você adicionou à sua Conta do Google, em dados de anunciantes que têm parceria com o Google e na estimativa do Google dos seus interesses. Escolha qualquer fator para saber mais ou atualizar suas preferências. [Saiba como controlar os anúncios que você vê](#)



**Figura 8 – Informações Sobre o Titular**

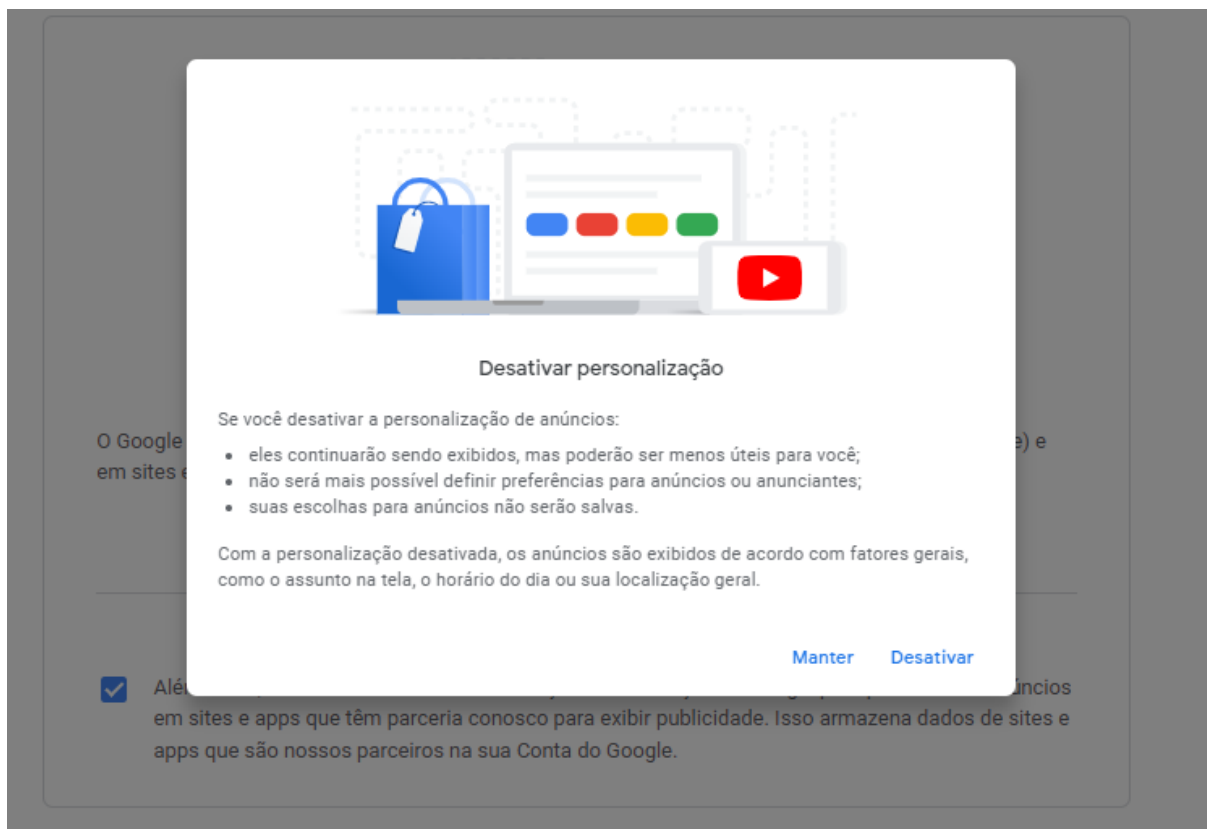
Fonte: <https://myactivity.google.com/myactivity>

Na conta utilizada para análise existiam 198 premissas a respeito do titular, sem que houvesse qualquer informação a respeito do tempo de retenção daqueles dados ou qualquer detalhamento a respeito do uso dessas informações para os anúncios personalizados, tampouco dos seus compartilhamentos.

Dessa forma, ao fazer a análise do processo de cadastro e dos tratamentos de dados para análise, ficam evidentes os seguintes padrões: há o desvio, visto na classificação de Brignull, que pode se relacionar com a interferência de Interface, utilizando informações ocultas (classificado por Gray et. Al, 2018, p. 7) e o Impedimento (classificado pelo Data Protection Board, 2022, p.2) . Isso porque o design é focado desviar a atenção ao impor a navegação por diversas páginas, que ficam ocultas, dessa forma, a plataforma irá dificultar o acesso do titular à formação de perfil que existe sobre ele. Para além disso, existem também o Zuckering de Privacidade (classificado por BRIGNULL, 2011, p.1)., tendo em vista que o usuário é induzido a

fornecer mais informações do que o necessário para o processo de navegação, que será utilizado para a produção de anúncios.

Ao fazer pela opção de desativar a configuração de anúncios personalizados, o usuário irá se deparar com mais um dos padrões escuros:



**Figura 9 – Desativar Personalização**

Fonte: <https://myactivity.google.com/myactivity>

No caso em tela, há mais uma vez o emprego do padrão de manipulação de interface, que vai, através dela, tentar induzir o titular a não revogar o seu consentimento.

Para além disso, insta salientar que ao desativar a opção de anúncios personalizado, através da revogação do consentimento não ocorrerá a exclusão dos dados. Para isso será imposto ao titular mais um desafio, visto que deverá ser feito através de outra aba do site, como forma de, mais uma vez, dificultar que o titular consiga exercer os seus direitos.

Por fim, no que tange ao serviço de localização oferecido pela empresa, uma investigação da Associated Press descobriu que muitos serviços do Google em dispositivos Android e iPhones armazenam dados de localização, mesmo que exista uma configuração de privacidade que diga que impedirá o Google de fazê-lo. Ocorre que apesar do usuário ter Histórico de Localização pausado, alguns aplicativos armazenam automaticamente dados de localização com carimbo de data/hora sem perguntar, isso ocorre de maneira automática ao acessar o google maps e para fornecer atualizações meteorológicas em telefones Android. Há ainda marcadores de localização, que irão salvar localizações recentes e para que cada uma dessas coletas seja desativada, o titular precisará realizar uma operação diferente (NAKASHIMA, 2018, p.3). Por conta disso, o Google sofre com uma ação nos distritos do Colorado, Virginia e Washington, acusado de se utilizar de padrões obscuros. Essa não é a única acusação que a empresa sofre, sendo sancionada em 2022 ao pagamento de multa no valor de 60 milhões de euros por emprego de *Dark patterns* na França (CNIL, 2022, p.1).

### 5.2.2. AMAZON PRIME

O Amazon Prime é um serviço de assinatura da varejista Amazon, que chegou ao Brasil em 2019, oferecendo uma série de benefícios para os membros. O programa apresenta como destaque o próprio promoções exclusivas na loja online e frete grátis, acesso ao seu serviço de streaming, o Prime Video, acesso ao serviço de música, o Prime Music e mais uma série de outros benefícios. ainda é possível testá-lo gratuitamente por alguns dias, antes de fazer a assinatura (SANTOS, 2021, p.2).

A análise inicial da plataforma da Amazon foi feita pelo Conselho de Consumo Norueguês, em estudo chamado “You can log out, but you can never leave”, direcionado a essa plataforma. Apesar disso, ele afirma que podem existir variações desses padrões a depender da localidade, dessa maneira, foi feito o estudo do cancelamento dos serviços da Amazon Prime no Brasil, para observar os padrões empregados aqui e classificar de acordo com os padrões supracitados. A análise foi feita através de um navegador WEB, usando o sistema do Google Chrome.

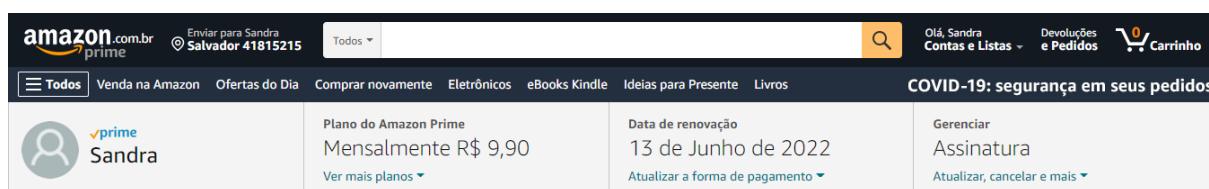
Inicialmente, para fazer o cancelamento o titular precisará entrar no site e acessar o canto superior direito, para ter acesso a sua conta, que o levará para a seguinte tela:



**Figura 10 – Tela de Acesso à Conta**

Fonte: [https://www.amazon.com.br/gp/primecentral?ref\\_=ya\\_d\\_c\\_prime](https://www.amazon.com.br/gp/primecentral?ref_=ya_d_c_prime)

Depois que isso é feito, ele deverá clicar em “Amazon Prime”, para acessar o seguinte menu:

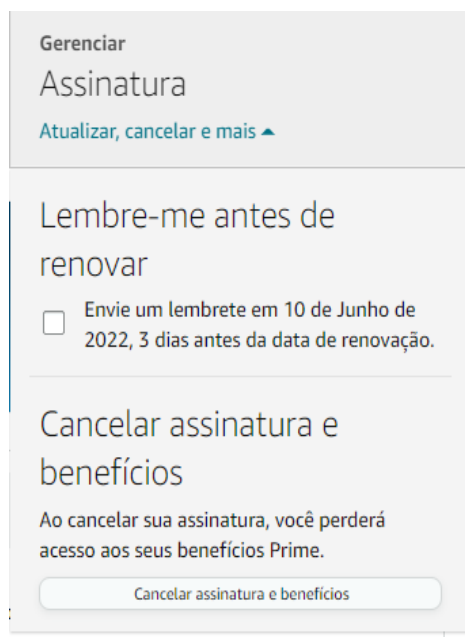


**Figura 11 – Gerenciamento de Assinatura 1**

Fonte: amazon.com.br

Por conseguinte, ele precisará clicar no canto superior esquerdo e será levado uma pequena página para gerenciar sua assinatura, onde aparecerá pela primeira vez a opção de cancelamento. Aqui já pode-se observar o primeiro padrão obscuro, que consiste em um redirecionamento sucessivo a diversas páginas, para que ele consiga ter acesso a opção de cancelamento.











**Figura 12 – Gerenciamento de Assinatura 2**

Fonte: amazon.com.br

Ao solicitar o cancelamento, o titular precisará passar pela tela que reforça os benefícios da assinatura que serão perdidos com o cancelamento, através de um layout bonito seguido da primeira tentativa explícita de impedir o cancelamento.

**Sandra, você ainda tem 20 dias para curtir os seus benefícios Prime até a próxima cobrança**

**Benefícios da sua assinatura Prime:**

<p><b>Entrega Prime</b></p>  <p>Frete <b>GRÁTIS</b> e rápido sem valor mínimo de compras em produtos elegíveis</p>	<p><b>Prime Video</b></p>  <p>Séries e filmes de sucesso, Amazon Originals premiados e muito mais</p>	<p><b>Amazon Music Prime</b></p>  <p>Mais de 2 milhões de músicas e podcasts sem anúncios</p>
<p><b>Prime Reading</b></p>  <p>Acesso a milhares de eBooks e revistas com o App Kindle</p>	<p><b>Prime Gaming</b></p>  <p>Acesso grátis a jogos, loots e uma assinatura Twitch a cada mês</p>	<p><b>Ofertas Prime</b></p>  <p>Ofertas exclusivas e acesso antecipado a ofertas selecionadas</p>


Lembre-me mais tarde      Continuar e cancelar      Manter minha assinatura

## Figura 13 – Confirmação 1 de Cancelamento

Fonte: amazon.com.br

Ao decidir seguir com o cancelamento, ele irá se deparar com mais uma tentativa de persuasão, que consiste no oferecimento de um plano anual, em que o cliente receberá 33% de desconto, devendo pagar o montante de R\$119,00.

### Sandra, antes de cancelar sua assinatura, considere mudar para o plano anual



Tenha todos os benefícios Prime por menos de R\$ 0,33/dia

Aproveite todos os benefícios do Amazon Prime com a facilidade dos pagamentos anuais. Será feito o reembolso de R\$ 6,14 para seu plano atual.

Economize até 33%

Mudar para o plano anual >

Ao clicar em Mudar para o plano anual, seu método de pagamento padrão ou outro método de pagamento disponível em nosso sistema será cobrado R\$ 119,00/ano. Sua assinatura Prime continuará até ser cancelada.

Lembre-me mais tarde

Cancelar assinatura

Manter minha assinatura


Mantenha meus benefícios e me lembre 3 dias antes da minha assinatura ser renovada

[Termos e condições da Amazon Prime](#)

## Figura 14 – Confirmação 2 de Cancelamento

Fonte: amazon.com.br

Ao clicar pela terceira vez no botão de “cancelar assinatura” o titular vai se deparar, mais uma vez com a necessidade de confirmar o cancelamento, como pode ser visto:



### Confirmar cancelamento da assinatura

Cancelar em 13 de Junho de 2022  
Seus benefícios continuarão até 13 de Junho de 2022. Após essa data, seu cartão não será cobrado.

Cancelar em 13 de Junho de 2022

Considere também:


Manter minha assinatura  
Você continuará aproveitando todos os benefícios do Amazon Prime.  
[Ver todos os benefícios do Amazon Prime.](#)

Manter minha assinatura

## Figura 15 – Confirmação 3 de Cancelamento

Fonte: amazon.com.br

Por fim, ao chegar nesse último passo, ele poderá ter a assinatura cancelada, mas ainda receberá em seu e-mail, como uma última tentativa de conversão desse cancelamento, dispondo das mesmas informações já fornecidas anteriormente.

 Sandra	Plano do Amazon Prime Mensalmente R\$ 9,90 <a href="#">Ver mais planos</a>	Assinatura terminando 13 de Junho de 2022 <a href="#">Altere a forma de pagamento</a>	Gerenciar Assinatura <a href="#">Atualizar, continuar e mais</a>
---------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------	------------------------------------------------------------------------

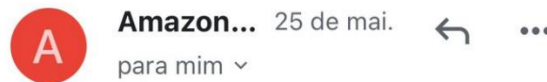
**⚠ Sua assinatura terminará em 13 de Junho de 2022**  
Nessa data, seus benefícios serão encerrados, e seu cartão não será cobrado.

**⚠ Sua assinatura Prime está próxima do fim**  
Sua assinatura Prime terminará em 13 de Junho de 2022 e você não terá mais acesso aos benefícios do Amazon Prime. [Continue com a assinatura](#)

## Figura 16 – Informação de Cancelamento

Fonte: amazon.com.br

Fonte:



Confirmação: sua assinatura do Amazon Prime não será renovada.



| Sua assinatura Prime |

Olá Sandra,

Confirmamos que você desativou a opção de renovação automática. Desta forma, ao final do período de sua assinatura, você não fará mais parte do Amazon Prime e não terá mais acesso aos benefícios Prime.

Gostaríamos de lembrá-lo que com sua assinatura Prime você tem [frete GRÁTIS](#) ilimitado em milhões de produtos elegíveis para o Amazon Prime, acesso a centenas de filmes e séries com o [Prime Video](#), dois milhões de músicas com o [Prime Music](#), centenas de eBooks e revistas com o [Prime Reading](#), conteúdo mensal de jogos com o [Prime Gaming](#), e acesso a ofertas exclusivas. Tudo em uma única assinatura.

Se desejar continuar aproveitando os benefícios Prime, use o botão abaixo para efetuar login e clique em Continuar assinatura na página Configurar sua assinatura Prime.

[Ver configurações assinatura](#)

amazon.com.br

Para mais informações sobre o Amazon Prime, por favor consulte os [Termos e Condições do Amazon Prime](#). Este e-mail foi enviado de um endereço de notificação que não está habilitado a receber mensagens. Por favor, não responda a esta mensagem.

## Figura 17 – E-mail de Cancelamento

Fonte: amazon.com.br via e-mail

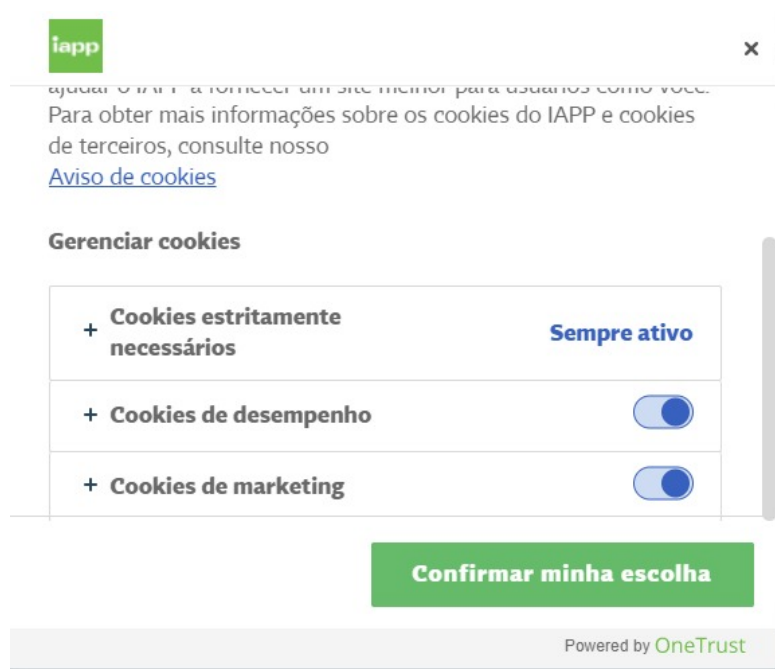
A respeito dessa análise, o Conselho de Consumo Norueguês, afirma que a Amazon parece fazer um grande esforço para desencorajar o usuário de cancelar a assinatura do Amazon Prime. Inicialmente o usuário precisa lembrar que possui uma assinatura, já que os pagamentos ocorrem de forma automática. O próximo obstáculo é realmente localizar a opção de cancelar a assinatura, que está escondida atrás de várias camadas do menu Amazon. O site impõe um número de cliques necessários para encontrar as configurações de cancelamento de inscrição tão alto que significa que há pouca chance de alguém iniciar o processo por engano. Apesar disso, a Amazon alerta o usuário durante todo o processo sobre as consequências do cancelamento da assinatura, ao mesmo tempo que implora ao usuário que mantenha sua assinatura

por meio de uma variedade de padrões sombrios a cada passo do processo. (FORBRUKERRÅDET, 2018, p. 18).

Ao longo desse exaustivo processo podem ser visto os seguintes padrões: de acordo com a classificação de Brignull há dark Pattern chamado de motel barato, pela dificuldade apresentada para o cancelamento, o desvio que ocorre com os sucessivos caminhos que são impostos pela plataforma até chegar ao cancelamento e a confirmação de vergonha, que tenta constranger o usuário a permanecer com sua assinatura ao se deparar com os benefícios que serão perdidos (classificação por BRIGNULL, 2011, p.1). Na classificação de Gray esses padrões se encaixam na categoria irritante; obstrução; a interferência de interface, através da manipulação estética e ação forçada (Gray, *et al*, 2018, p.2). Por fim ao, fazer a mesma análise de acordo com os padrões da European Data Protection board, podem ser evidenciados os padrões de agitação e impedimento (classificação EUROPEAN DATA PROTECTION BOARD, 2022, p.2).

### 5.3 COLETA DE CONSENTIMENTO PARA COOKIES

É comum que a coleta de consentimento, que ocorre para possibilitar o tratamento de dados referentes aos cookies de navegação, contenham os Padrões Obscuros, sendo habitual que não seja oferecido ao titular a possibilidade de recusar a coleta e a imposição de consentimento dos chamados cookies necessários, como se vê abaixo:



**Figura 18 – Confirmação de Cookies 1**

Fonte: <https://iapp.org/#>

De maneira semelhante, site utilizado pelo Governo Federal também se emprega padrão obscuro, ao não permitir inicialmente que o titular negue consentimento para a coleta de cookies.



## Figura 19 – Confirmação de Cookies 2

Fonte: <https://www.gov.br/pt-br>

Nos dois casos, o Padrão Escuro evidente é o descrito por Gray et.al como Interferência de Interface, onde há uma pré-seleção antes mesmo da interação com o usuário e a ação forçada, ao exigir que o usuário execute uma ação específica (classificação de Gray, *et al*, 2018, p.2).

Levando em consideração a não conformidade desta coleta com a LGPD, a Agência Nacional de Proteção de Dados elaborou em 13 de maio de 2022 uma nota de Recomendação para a adequação do Portal Gov.br às disposições da LGPD. Nela, a Equipe Técnica da Agência constata que são necessárias adequações às práticas de tratamento do portal, relacionado dois aspectos (BRASIL, 2022, p.1).

O primeiro aspecto observado pela ANPD se relaciona com o banner apresentado ao usuário assim que este acessa a página que, além de conter informações muito limitadas, contém apenas a opção “aceitar”. Essa prática irá contrariar a determinação da LGPD de que, para ser válido, o consentimento do titular deve ser livre, informado e inequívoco. Ademais, a política de cookies disponibilizada em outra página, depois que o usuário clica no link da página inicial, possui informações vagas e genéricas, que dificulta a compreensão do usuário. Para além disso, as finalidades de tratamento são apresentadas de forma de que não é possível que todas sejam identificadas (BRASIL, 2022, p.1).

Desse modo, é recomendado que seja instituído um botão para rejeitar o uso de cookies; que o sejam desativados os cookies baseados no consentimento por padrão; que seja disponibilizado um botão de fácil visualização; que permita rejeitar todos os cookies não necessários, que seja permitida a obtenção do consentimento específico de acordo com as categorias identificadas; que as bases legais sejam identificadas junto com a finalidade específica de cada tratamento (BRASIL, 2022, p.2)

## 6 CONCLUSÃO

O advento da tecnologia em muitos aspectos se mostra como algo positivo. Com as possibilidades oferecidas pelo mundo digital a economia e a sociedade obtiveram avanços inimagináveis, de modo que o mundo ficou totalmente conectado e as pessoas obtiveram a possibilidade de ficar mais próximas. É inegável que esses avanços trouxeram benefícios ao titular, não só em serviços utilizados em seu cotidiano, como em produtos, que puderam ser personalizados de acordo com o consumidor e, conforme abordado no segundo capítulo, é um dos muitos modelos de negócios baseado em dados.

A grande questão que advém disso é que à medida que a internet foi crescendo, foram surgindo grandes empresas, que se incumbiram de auferir lucros junto com esse crescimento, principalmente enquanto não existiam tantas regulações sobre o mundo digital. Os dados pessoais coletados na internet refletem a personalidade do titular, seus gostos, seus hábitos, preferências e até questões de caráter mais pessoal, como saúde, religião e afiliações políticas.

Ocorre que ao mesmo tempo que as inovações iam se materializando, o titular estava inserido nesse cenário e precisou aprender a viver no desconhecido enquanto ele ia surgindo, sem que ninguém lhe ensinasse como se comportar ali. Por conseguinte, esse usuário esteve sempre um passo atrás das Indústrias, que ao perceber que poderia se aproveitar de suas informações pessoais, fez de tudo para maximizar suas coletas e invadir a privacidade deste. O titular e seus dados estão no centro do modelo de negócio dessas companhias, sem que por vezes nem tenha noção, pois sem eles não há operações de tratamento e conseqüentemente, não há o que se falar em lucro.

Tão logo, muitos países cuidaram de incluir em seus ordenamentos jurídicos medidas que deveriam ser respeitadas pelos empresários inseridos no mundo virtual e, a cada Lei nova, mil e uma novas formas de contorno sobre ela vão surgir, afinal, o que importa no fim do dia é o lucro. Desse modo, a primeira coisa que se deve inferir nesse trabalho é que não bastam Leis, recomendações e guias sobre como o controlador



deve tratar os dados e sobre o direito dos titulares se aquele que está no centro não é ensinado a como se portar e quais as consequências de seus atos no mundo virtual. Esse fenômeno de criação de leis ocorreu no Brasil e foi discutido ainda no segundo capítulo. A Lei Geral de Proteção de Dados trouxe uma inovação jurídica sem igual ao apresentar diretrizes para o tratamento de dados pessoais, direitos do titular, princípios, fundamentos e outras coisas. Avanço maior ainda ocorre em 2022, quando o direito à proteção de dados é considerado como uma cláusula pétrea da Constituição Federal de 1988. Entretanto, mesmo com todas essas mudanças, o titular foi ensinado sobre como se portar ali e sobre os seus direitos. A lei por si só não é acessível a todos os titulares, na medida em que sua estrutura não é favorável ao entendimento do leigo, de modo que se deixa levar pelos artifícios digitais de quem a entende e sabe como driblá-la.

Mais adiante, o presente estudo discorre sobre as famigeradas hipóteses de tratamento de dados, conhecidas como bases legais. Elas funcionam quase que como um encaixe do fato à norma, assegurando fundamento para que o tratamento ocorra. Nesse cenário, vem a imagem do consentimento: uma das formas que o legislador encontrou de atribuir ao titular o poder de decidir sobre o tratamento de seus dados, sendo este mais uma das formas de consagrar a autodeterminação informativa, e isto é alvo de discussão do terceiro capítulo do presente trabalho.

Para o tratamento ocorrer com base no consentimento o Legislador vai impor critérios de validade a esse instituto, através de adjetivos que devem ser inerentes ao consentimento. Ele deve ser uma manifestação livre, informada, inequívoca, onde o titular irá aceitar o tratamento de seus dados para uma finalidade determinada, de acordo com 5º, XII da referida Lei. A forma de coleta aqui também será importante, já que a norma determina que é ônus do controlador provar que este foi adquirido. Observa-se que este instituto jurídico vai se relacionar com outros pontos da legislação, como a transparência que deve ser dada ao titular durante todo o tratamento, com a autodeterminação informativa e seus direitos, devendo este estar sempre em harmonia com o restante da lei para ser válido.

Nesse cenário aparecem as políticas de privacidade, que deveria ser uma forma do controlador se comunicar com o titular, conforme demonstrado no ainda no terceiro capítulo. Desta análise, conclui-se que este acaba por se tornar apenas mais um documento com escrita formal e distante de sua realidade, informando apenas o que é conveniente para ele. No mundo ideal essa política deveria ser uma forma de assegurar ao titular a sua autodeterminação informativa, vez que através dela, ele poderia decidir se, de fato, vai consentir com as operações de tratamento de seus dados, mas na realidade ocorre que em alguns casos o titular sequer irá e ler e se o fizer, em determinados casos não irá compreender.

Ainda como artifício das grandes empresas vão surgir os padrões escuros, analisados no quarto capítulo desta monografia. Eles serão como uma forma de ludibriar e induzir o usuário a determinado comportamento. Através do design e da ferramenta de experiência do usuário, este vai ser impulsionado em direção a realizar um comportamento favorável às Empresas que tratam dados. O conceito é estudado há 9 anos na doutrina mas, apenas nos últimos anos ele foi considerado como uma forma de inadequação às leis de proteção de dados em alguns ordenamentos jurídicos. Ao fazer a análise do uso desses padrões, é evidente que eles podem fazer com que o titular ofereça dados que não deseja ou adquira produtos sem perceber ou até que seja colocado em situações que o obrigam a fornecer dados, tudo isso em troca de algo que será benéfico apenas ao controlador. Conforme visto ainda no quarto capítulo desse estudo, existem algumas classificações para estes padrões, que retratam a forma como eles vão ser desenhados para se aproveitar do titular.

Por fim, no último capítulo, ao observar como esses padrões são empregados, fica evidente que as ferramentas de design são muito úteis e obtém êxito nesse processo, de modo que por vezes ele nem sabe para onde vão seus dados, quais são coletados e quem tem acesso. As gigantes da tecnologia, como o Google, Meta ou Amazon oferecem milhares de serviços, que coletam as mais diversas informações, sem que ele possua completo entendimento a respeito de todo o processo.

Ao fazer a análise em conjunto da situação, fica evidente que o instituto do consentimento, da maneira que é coletado e aceito se torna falacioso, tendo em vista

que o titular é lesado das mais diversas maneiras durante a sua coleta. O consentimento coletado no mundo virtual em muitos dos casos não ultrapassa o plano da validade, por não possuir uma vontade empregada genuinamente, de modo que não deve ser juridicamente aceito.

É contraproducente afirmar que este é dado de maneira livre, informada e inequívoco, bem como para uma finalidade determinada. Isso porque nem sempre o titular vai possuir a capacidade de compreender, de fato, tudo o que ocorre com suas informações, de modo que não vai oferecer essas informações por livre e espontânea vontade, ele será compelido a isso. Através desse estudo, pode-se concluir que a forma como os padrões obscuros são empregados, oferecem dificuldades de resistência ao titular, que é compelido a ter um comportamento direcionado pelo controlador.

Tão falacioso quanto o consentimento é o direito à privacidade no universo digital. Apesar do Legislador, por sua vez, assumir o seu papel de legislar a respeito do tema, isso não basta. Ao fazer a análise da lei, é evidente que esta é silente em muitos aspectos, mas essa análise irá se ater aos padrões escuros. Essa lacuna, que diz respeito a um tema que já era abordado na doutrina estrangeira à época da promulgação da Lei, em 2018, permite que o controlador possa reinar através da subjetividade de design e obtenha do titular tudo o que deseja. Desse modo, conclui-se que nem sempre o direito fundamental à proteção de dados poderá ser exercido pelo Titular.

Neste sentido, resta à Agência Nacional de Proteção de Dados o dever de atuar no sentido de proteger a privacidade do titular no mundo virtual. Cabe à ANPD o papel de agir de maneira mais protecionista, através de suas regulamentações e fiscalizações, de modo que a utilização de Padrões Escuros seja coibida. A Agência precisa assumir um papel mais imperativo com o controlador durante a coleta, no sentido que ele sinta a necessidade de se adequar devido aos possíveis impactos econômicos que o seu comportamento pode ensejar. Da mesma forma, cabe a esta o papel de ensino e conscientização do titular, que deve ter a mínima noção a respeito

de seus direitos, sobretudo à privacidade e proteção de dados e do impacto do compartilhamento infinito de seus dados pessoais com o controlador.

Ao controlador resta a posição de ter a consciência de seu papel social ao coletar dados, devendo este utilizar-se dos princípios de Privacy by Design ao desenhar a experiência do cliente com seus produtos. Ademais, ele deve oferecer ao titular políticas de privacidade que possuam uma linguagem adequada para todas as realidades. Por fim, o controlador deve se atentar que precisam partir dele as primeiras iniciativas de assegurar os direitos do titular, tendo em vista que nessa relação jurídica ele irá possuir grande poder, e a outra parte estará sempre em posição de vulnerabilidade.

Dessa forma, será possível caminhar em direção a efetividade do instituto do consentimento, possibilitando que este seja de fato livre, inequívoco e informado.

## REFERÊNCIAS

ACQUISTI, Alessandro; ADJERID, Idris; BALEBAKO, Rebecca; BRANDIMARTE, Laura; CRANOR, Lorrie Faith; KOMANDURI, Saranga; LEON, Pedro Giovanni; SADEH, Norman; SCHAUB, Florian; SLEEPER, Manya; WANG, Yang; WILSON, Shomir. **Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online**. Computing Surveys , v. 50, n. 3, 1 maio 2018. Acesso em 30 mar 2022

ALBUQUERQUE, Priscila. **O QUE É UX DESIGN? TUDO QUE VOCÊ PRECISA SABER SOBRE EXPERIÊNCIA DO USUÁRIO**. 22 abr. 2020. Disponível em: <https://catarinasdesign.com.br/ux-design/>. Acesso em: 10 mar. 2022.

ARTICLE 29 DATA PROTECTION WORKING PARTY, **Opinion 03/2013 on purpose limitation**, 00569/13/EN WP 203, Europa, Abril de 2013. Acesso em 10 abril 2022. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf)

BARREDA, Alejandra R. **Você deve aceitar o uso de cookies na Internet? É melhor pensar duas vezes**. CNN, 27 maio 2021. Disponível em <https://www.cnnbrasil.com.br/tecnologia/voce-deve-aceitar-o-uso-de-cookies-na-internet-e-melhor-voce-pensar-duas-vezes/> Acesso 22 maio 2022

BESSA, Leonardo Roscoe. **A Lei Geral de Proteção de Dados e o direito à autodeterminação informativa**. Conjur. 26 out. 2020. Disponível em: Por Leonardo Roscoe Bessa. Acesso em: 22 set. 2021.

BESSA, Leonardo, R. **LGPD: direito ou dever de privacidade?**. Conjur, 8 fev. 2021. Disponível em: <https://www.conjur.com.br/2021-fev-08/leonardo-bessa-lgpd-direito-ou-dever-privacidade>. Acesso em: 22 maio 2022.

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

BOFF, Salete Oro; FORTES, Vinícius Borges. **A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil**. Sequência (Florianópolis), p. 109-127, 2014.

BORGESIU, F. Z. **CONSENTIMENTO INFORMADO. PODEMOS FAZER MELHOR EM DEFESA DA PRIVACIDADE**. Logeion: Filosofia da Informação, v. 2, n. 2, p. 80–90, 2016. DOI: 10.21728/logeion.2016v2n2.p80-90. Disponível em: <http://revista.ibict.br/fiinf/article/view/1768>. Acesso em: 19 nov. 2021.

BORTOLOZO, Luciana. Política de privacidade - **O que é e como criar esse documento**. 12 agos. 2021. Disponível em: <https://www.migalhas.com.br/depeso/350020/politica-de-privacidade--o-que-e-e-como-criar-esse-documento>. Acesso em: 17 maio 2022.

BORTOZOLO, Luciana F. **Política de privacidade - O que é e como criar esse documento** 12 ago. 2021. Disponível em: <https://www.migalhas.com.br/depeso/350020/politica-de-privacidade--o-que-e-e-como-criar-esse-documento>. Acesso em: 17 maio 2022.

BÖSCH, Christoph; ERB, Benjamin; KARGL, Frank; KOPP, Henning; PFATTHEICHER, Stefan . **Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark patterns**. Proc. Priv. Enhancing Technol., v. 2016, n. 4, p. 237-254, 2016.

BOWLES, Cennydd. **If you think all design is manipulation, please stop designing.** 31 jan. 2022. Disponível em: <https://cennydd.com/writing/if-you-think-all-design-is-manipulation-please-stop-designing>. Acesso em: 22 maio 2022.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, [2016]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/Constituicao/Constituicao.htm](http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm). Acesso em: 19 set. 2021.

BRASIL. Constituição (1988). **Emenda constitucional nº 15**, de 10 de fevereiro de 2022, Brasília. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/Emendas/Emc/emc115.htm](http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm)

BRASIL. **Lei Geral de Proteção de Dados**. Lei Nº 13.709, de 14 de agosto de 2018. Brasília, DF: Presidência da República, 2018. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm) Acesso em 19/09/2021

BRASIL. **Marco Civil da Internet**. Lei 12.964/14. Disponível em: < [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm) >. Acesso em 07 abril 2022

BRIGNULL, Harry. **DARK PATTERNS INSIDE THE INTERFACES DESIGNED TO TRICK YOU.** Disponível em: <https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you> Acesso em 20 de nov de 2021

BROWNLEE, John. **Why Dark patterns won't go away.** 22 ago. 2016. Disponível em: <https://www.fastcompany.com/3060553/why-dark-patterns-wont-go-away>. Acesso em: 22 maio 2022.

CALIFÓRNIA. **THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020**. Estado da Califórnia, Estados Unidos da América, [2020]. Disponível em: [https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29\\_1.pdf](https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf) Acesso em: 19 set. 2021

CARVALHO, Antonio Ramalho DE Souza. Cadernos Adenauer XX (2019), nº3 **Proteção de dados pessoais: privacidade versus avanço tecnológico**. Rio de Janeiro: Fundação Konrad Adenauer, outubro 2019. isbn 978-85-7504-230-4.

CAVOUKIAN, Ann. **Privacy by design: The 7 Foundational Principles**. Ontário, Canadá, 20 ago. 2011. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>. Acesso em: 19 maio 2022.

COLORADO. **PROTECT PERSONAL DATA PRIVACY** Estado do Colorado, Estados Unidos da América, [2021]. Disponível em: <https://leg.colorado.gov/bills/sb21-190> Acesso em 18 set 2021

Comission Nationale, Informatique e Liberté (CNIL), **CONNECTED VEHICLES AND PERSONAL DATA**, edição de outubro de 2017. França.

Commission Nationale de l'Informatique et des Libertés (CNIL). **Cookies: the CNIL fines GOOGLE a total of 150 million euros and FACEBOOK 60 million euros for non-compliance with French legislation**. França. Disponível em: <https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance>. Acesso 22 mai 2022

Commission Nationale de l'Informatique et des Libertés (CNIL). **Cookies and other tracking devices: the CNIL publishes new guidelines**. França. Disponível em:



<https://www.cnil.fr/en/cookies-and-other-tracking-devices-cnil-publishes-new-guidelines>. Acesso em 22 mai 2022

CONJUR. **Proteção de Dados Pessoais passa a ser direito constitucional**, 10 fev. 2022. Disponível em <https://www.conjur.com.br/2022-fev-10/protecao-dados-pessoais-passa-direito-constitucional> Acesso 22 mai 2022

COROVIC, Tiana; AHMAD, Imran. **Privacy in a Parallel Digital Universe: The Metaverse**. 25 jan. 2022. Disponível em: <https://www.dataprotectionreport.com/2022/01/privacy-in-a-parallel-digital-universe-the-metaverse/>. Acesso em: 17 fev. 2022.

COSTA, Ramon silva; OLIVEIRA, Samuel Rodrigues de. **OS DIREITOS DA PERSONALIDADE FRENTE À SOCIEDADE DE VIGILÂNCIA: PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E CONSENTIMENTO NAS REDES SOCIAIS**. Revista Brasileira de Direito Civil em Perspectiva, ed. e-ISSN: 2526-0243, 4 dez. 2019

COUTO, ANA. **Dark patterns em UX: uma interface entre o design e a proteção de dados**. 13 maio 2021. Disponível em: <https://www.semprocesso.com.br/post/dark-patterns-ux-design-e-protecao-de-dados>. Acesso em: 18 nov. 2021

CRIDDLE, Cristina. **Facebook sued over Cambridge Analytica data scandal**, 28 out. 2020. Disponível em: <https://www.bbc.com/news/technology-54722362>. Acesso em: 19 set. 2021.

CUNHA, Juliana. **O Direito à Privacidade e a Proteção de Dados, Princípios Norteadores e Compliance à Luz da Lei Geral de Proteção de Dados**. 2020. Disponível em: <https://julianajcunha.jusbrasil.com.br/artigos/863995334/o-direito-a->

privacidade-e-a-protecao-de-dados-principios-norteadores-e-compliance-a-luz-da-lei-geral-de-protecao-de-dados. Acesso em: 22 maio 2022.

CUSTERS. Barty **Click here to consent forever: Expiry dates for informed consent**. Big Data & Society. Junho 2016. doi:10.1177/2053951715624935

D'URSO , Luiz Augusto; D'URSO , Flávio Filizzola. **O absurdo poder das redes sociais em razão da coleta de dados**. 15 fev. 2021. Disponível em: <https://www.conjur.com.br/2021-fev-15/durso-durso-poder-redes-sociais-coleta-dados>. Acesso em: 19 set. 2021.

Dijck, J. van. (2017). **Confiamos nos dados? As implicações da datificação para o monitoramento social**. MATRIZES, Revista USP, 11(1), 39-59. 2017. Disponível em: <https://doi.org/10.11606/issn.1982-8160.v11i1p39-59>

DONEDA, Danilo. **DA PRIVACIDADE A PROTEÇÃO DE DADOS PESSOAIS**. [S. l.: s. n.], 2020. ISBN 978-65-5065-030-8.

ESTADOS UNIDOS DA AMÉRICA, **Detour Act Final**. 2019. Disponível em: <https://pt.scribd.com/document/405606873/Detour-Act-Final> Acesso 22 mai 2022

EUROPEAN DATA PROTECTION BOARD, **Guideline 03/2022 on *Dark patterns* in social media platform interfaces: How to recognise and avoid them**. Versão 1.0. Adotado em março de 2022. Disponível em: [https://edpb.europa.eu/system/files/2022-03/edpb\\_03-2022\\_guidelines\\_on\\_dark\\_patterns\\_in\\_social\\_media\\_platform\\_interfaces\\_en.pdf](https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf) Acesso em 01 abril 2022

EUROPEAN DATA PROTECTION BOARD. **Guideline 05/2020 on consent under Regulation 2016/679**. Versão 1.1. Adotada em maio de 2020. Disponível em:

[https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf) Acesso em 15 maio 2022

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Direito civil: teoria geral**. 6ª ed. Rio de Janeiro: Editora Lúmen Júris, 2007.

FEDERAL TRADE COMMISSION. **FTC to Ramp up Enforcement against Illegal *Dark patterns* that Trick or Trap Consumers into Subscriptions**. Estados Unidos da América. Disponível em: <https://www.ftc.gov/news-events/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap>. Acesso em 21/12/2021

FILHO, Eduardo Tomasevicius. **O princípio da boa-fé na Lei Geral de Proteção de Dados**. [S. l.], 9 mar. 2020. Disponível em: <https://www.conjur.com.br/2020-mar-09/direito-civil-atual-principio-boa-fe-lgpd>. Acesso em: 13 nov. 2021

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. **Privacidade e lei geral de proteção de dados pessoais**. Revista de Direito Brasileira, v. 23, n. 9, p. 284-301, 2020.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. **PRIVACIDADE e LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS**. Revista de Direito Brasileira, v. 23, n. 9, p. 284-301, fev. 2020. ISSN 2358-1352. Disponível em: <<https://www.indexlaw.org/index.php/rdb/article/view/5343>>. Acesso em: 26 maio 2022. doi:<http://dx.doi.org/10.26668/IndexLawJournals/2358-1352/2019.v23i9.5343>.

FLÔRES, mariana rocha de ; SILVA, Rosane Leal Da. **Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da administração pública: entre o dever público de informar e o direito do cidadão de ser tutelado** |. 14 fev. 2020. Disponível em: [periodicos.ufv.br](http://periodicos.ufv.br). Acesso em: 11 nov. 2021.

FORBRUKERRADET, Norwegian Consumer. Council. **Deceived by design.** Noruega, 2018. Disponível em: <https://www.consumersinternational.org/news-resources/news/releases/new-research-suggests-leading-tech-companies-are-making-it-difficult-for-users-to-opt-of-out-sharing-personal-data/> Acesso em: 15 set. 2021

FORBRUKERRADET, Norwegian Consumer. Council. **You Can Log Out, But You Can Never Leave.** Noruega, 14 jan 2021. Disponível em: <https://fil.forbrukerradet.no/wp-content/uploads/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf> Acesso em 20 maio 2022

FRAZÃO , Ana. **Big data e impactos sobre a análise concorrencial.** 28 nov. 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/columnas/constituicao-empresa-e-mercado/big-data-e-impactos-sobre-a-analise-concorrencial-28112017>. Acesso em: 13 maio 2022.

FRAZÃO, A. N. A.; OLIVA, Milena Donato; TEPEDINO, Gustavo. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** Thomson Reuters Brasil, 2019.

FRAZÃO, Ana; ABILIO, Vivianne; OLIVEIRA, Juliana. **Compliance e políticas de proteção de dado.** Brasil, 2021. 1264 p. ISBN 9786559915408.

FUNG, Bryan . **Lawmakers want to ban ‘Dark patterns,’ the Web designs tech companies use to manipulate you.** The Washington Post, 9 abril 2019. Disponível em: <https://www.washingtonpost.com/technology/2019/04/09/policymakers-are-sounding-alarm-dark-patterns-manipulative-web-design-trick-youve-never-heard/> Acesso em: 22 maio 2022.

GOMES, Helton Simões. **'Cadê o botão de fechar?': como apps e sites usam o design para tapear você...** - 22 abr. 2019. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2019/04/22/cade-o-botao-de-fechar-como-apps-e-sites-usam-o-design-para-tapear-voce.htm>. Acesso em: 15 set. 2021.

GRAY, Colin M.; KOU, Yubo; Hoggatt, Joseph; TOOMBS, Austin L. **The dark (patterns) side of UX design**. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Canada. 2018. p. 1-14.

HILL, Kashmir. **How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did**. [S. l.], 16 fev. 2012. Disponível em: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>. Acesso em: 15 maio 2022.

HOEPMAN, Jaap-Henk. **Privacy Design Strategies**. 29th IFIP International Information Security Conference (SEC), Junho 2014, Marrakech, Morocco. pp.446-459, ff10.1007/978-3-642-55415-5\_38ff. fahal01370395f Acesso em 20 maio 2022.

ISO 9241-210:2019. **Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems**. Geneva, Switzerland: International Organization for Standardization, 2019.

JAISWAL, Arushi. **Dark patterns in UX: how designers should be responsible for their actions**. [S. l.], 15 abr. 2018. Disponível em: <https://uxdesign.cc/dark-patterns-in-ux-design-7009a83b233c>. Acesso em: 19 set. 2021.

JAROVSKY, Luiza, **Dark patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness** 1 Março 2022. Disponível em: SSRN: <https://ssrn.com/abstract=4048582> or <http://dx.doi.org/10.2139/ssrn.4048582> Acesso em: 17 maio 2022

KHOURI, Paulo R Roque. **O problema do consentimento informado na Lei Geral de Proteção de Dados Pessoais**. 31 maio de 2021. Disponível em: <https://www.conjur.com.br/2021-mar-31/garantias-consumo-problema-consentimento-informado-lgpd>. Acesso em: 12 nov. 2021

LEAL, Martha. **Dark patterns e leis de proteção de dados**. [S. l.], 16 nov. 2021. Disponível em: [https://www.conjur.com.br/2021-nov-16/leal-dark-patterns-leis-protecao-dados#\\_ftnref1](https://www.conjur.com.br/2021-nov-16/leal-dark-patterns-leis-protecao-dados#_ftnref1). Acesso em: 21 nov. 2021.

LEAL, Martha. **O protagonismo da transparência na LGPD**. 23 jun. 2021. Disponível em: <https://www.conjur.com.br/2021-jun-23/martha-leal-protagonismo-transparencia-lgpd>. Acesso em: 21 maio 2022.

LEETARU, Kalev. **What Does It Mean For Social Media Platforms To "Sell" Our Data?**. [S. l.], 15 dez. 2018. Disponível em: <https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=3cbab6d92d6c>. Acesso em: 16 set. 2021.

LEQUES, Rossana B. **LGPD prevê consentimento específico para uso de dados, e não autorizações genéricas**. 20 jun 2019. Disponível em: <https://www.conjur.com.br/2019-jul-20/rossana-leques-lgpd-preve-permissao-especifica-uso-dados> Acesso 10 mar 2022

LOMAS, Natasha. **UK now expects compliance with children's privacy design code**. 1 set. 2021. Disponível em: <https://techcrunch.com/2021/09/01/uk-now-expects-compliance-with-its-child-privacy-design-code/>. Acesso em: 19 set. 2021

LUGATI, L. N.; ALMEIDA, J. E. de. **Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa**. Revista de Direito, [S. l.], v. 12, n.

02, p. 01-33, 2020. DOI: 10.32361/2020120210597. Disponível em:  
<https://periodicos.ufv.br/revistadir/article/view/10597>. Acesso em: 19 set. 2021.

MARTINEZ, Maricarmem; DELSOL, Gabriel. **Banning *Dark patterns* – Far From a Light Task. Center for European Policy Analysis**, 5 abr. 2022. Disponível em:  
<https://cepa.org/banning-dark-patterns-far-from-a-light-task/>. Acesso em: 22 maio 2022.

MATTOS , Anderson. **O que é Nudge?**. [S. l.], 20 ago. 2018. Disponível em:  
<https://geekonomics.com.br/2018/08/nudge-siginificado-definicao/>. Acesso em: 18 maio 2022.

MENA, ISABELA. **Verbetes Draft: o que é Capitalismo de Vigilância**. 27 março 2019. Disponível em <https://www.projetodraft.com/verbete-draft-o-que-e-capitalismo-de-vigilancia/> Acesso: 29 maio 2022

MENDONÇA , Suzana. **A autodeterminação informativa no contexto de proteção de dados pessoais**. 20 out. 2019. Disponível em: <https://www.conjur.com.br/2019-out-20/suzana-mendonca-autodeterminacao-informativa-protecao-dados>. Acesso em: 8 mar. 2022.

MOLICONE, Bianca. **Consulta sobre LGPD e Direitos Trabalhistas**. 19 out 2020. Acesso em 20 mai 2022

MORAIS, PAULINE. **O consentimento previsto na LGPD**. 25 out 2020. Disponível em: <<https://www.conjur.com.br/2020-out-25/pauline-moraes-consentimento-previsto-lgpd>>. Acesso em: 22 out. 2021.

NAKASHIMA, Ryan. **AP Exclusive: Google tracks your movements, like it or not**. 13 ago. 2018. Disponível em: <https://apnews.com/article/north-america-science->

technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb. Acesso em: 25 maio 2022.

NÓBREGA, Guilherme. **O mito do consentimento e o paradoxo da privacidade.** , 8 abr. 2020. Disponível em: <https://www.linkedin.com/pulse/o-mito-do-consentimento-e-paradoxo-da-privacidade-guilherme/?originalSubdomain=pt>. Acesso em: 17 maio 2022.

NOUWENS, Midas; LICCARDI, Ilaria; VEALE, Michael; KARGER, David; KAGAL, Lalana. **Dark patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence.** Reino Unido, 2020.

ÓPICE BLUM, Renato et al. **Gestão dos programas de privacidade e proteção de dados.** 13 ago. 2021. Disponível em: <https://opiceblum.com.br/wp-content/uploads/2019/07/EBOOK-DPO-ENCARREGADO-3.pdf>. Acesso em: 25 maio 2022

PATTERNAL, Sanjay. **“Dark patterns” and data protection compliance.** Disponível em: <https://www.trilateralresearch.com/dark-patterns-and-data-protection-compliance/> Acesso em 15 set. 2021

PESTANA, MÁRCIO. **Os princípios no tratamento de dados na LGPD.** 2020. Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em 18/092021

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais : comentários à Lei n. 13.709/2018 (LGPD).** São Paulo : Saraiva Educação, 2018.

PRASS, Ronaldo. **Manipulação do comportamento do usuário pelo controle de dados na internet; entenda como funciona o tema proposto na redação do**



**ENEM.** [S. l.], 4 nov. 2018. Disponível em:

<https://g1.globo.com/economia/tecnologia/blog/ronaldo-prass/post/2018/11/04/manipulacao-do-comportamento-do-usuario-pelo-controle-de-dados-na-internet-entenda-como-funciona-o-tema-proposto-na-redacao-do-enem.ghtml>. Acesso em: 19 set. 2021.

Quintiliano, Leonardo. **Contexto histórico e finalidade da Lei Geral de Proteção de Dados (LGPD).** [S. l.], 17 mar. 2021. Disponível em: <https://iapd.org.br/contexto-historico-e-finalidade-da-lei-geral-de-protecao-de-dados-lgpd/>. Acesso em: 17 nov. 2021.

RODRIGUES, Thoran. **Uma nova etapa na Lei Geral de Proteção de Dados Pessoais.** 20 ago. 2021. Disponível em: <https://www.conjur.com.br/2021-ago-20/thoran-rodriques-etapa-lgpd>. Acesso em: 11 nov. 2021.

ROMAN, Juliana. **A proteção de dados pessoais na Lei nº 13.709/2018: uma análise sobre consentimento e direito à autodeterminação informativa na Lei Geral de Proteção de Dados.** Anais dos Congressos Estaduais de Magistrados-RS, v. 1, n. 1, 2020.

SANTIAGO, Isabel Teixeira; SOUZA, Luana Oliveira Sutério de. **Estudos universitários de direitos fundamentais.** Brasil. Editora Direito Levado a Sério, 2021. v. 1. ISBN 978-65-87020-19-8.

SANTOS, LUIZA MENDONÇA DA SILVA BELO. **O direito da concorrência na economia movida a dados: uma análise dos impactos do big data no controle de estruturas do setor digital.** Brasília: [s. N.], 2019.

SANTOS, Lucas. **O que é Amazon Prime? Veja 5 perguntas e respostas sobre o serviço.** 18 dez. 2017. Disponível em: <https://www.techtudo.com.br/listas/2021/12/o->

que-e-amazon-prime-veja-5-perguntas-e-respostas-sobre-o-servico.ghtml. Acesso em: 25 maio 2022.

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**. 22 de março de 2014. Ethics and Information Technology, The Crisis of Consent: How Stronger Legal Protection may lead to Weaker Consent in Data Protection, DOI: 10.1007/s10676--014--9343--8, Forthcoming, Available at SSRN: Disponível em: <https://ssrn.com/abstract=2412418>. Acesso em 17 maio 2022.

Sebastião, M. P. D. A. . (2020). **Proteção aos dados do usuário de serviços digitais pela LGPD e as cláusulas abusivas na política de privacidade**. Cadernos Jurídicos Da Faculdade De Direito De Sorocaba, 3(1), 107–120. Acesso em: <https://www.fadi.br/revista/index.php/cadernosjuridicos/article/view/92>

SILVA, Rosane Leal. **AS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO E A PROTEÇÃO DE DADOS PESSOAIS**. 2010  
Disponível em:  
<http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/fortaleza/3254.pdf>

Sirotheau, Debora; FERRAZ, Paula. **A importância da conscientização sobre a proteção dos dados pessoais**. [S. l.], 2 out. 2021. Disponível em:  
<https://www.conjur.com.br/2021-out-02/opinioao-conscientizacao-protacao-dados-pessoais>. Acesso em: 11 nov. 2021.

Staben, J. (2012). **Consent under pressure and the Right to Informational Self-Determination**. Internet Policy Review, 1(4). <https://doi.org/10.14763/2012.4.265>

STF. Medida Provisória nº 954, de 17/4/2020. Votos da Ministra Rosa Weber.

Disponível em

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

Acesso em: 14 nov. 2021

SUNDFELD, PHILIPPE; FERNANDES, Maria Luiza. **LGPD e UX: um equilíbrio para o consentimento**. 16 jul. 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-ux-um-equilibrio-para-o-consentimento-16072021>. Acesso em: 21 nov. 2021.

TANAKA, ANDRÉ FELIPE. **Design do consentimento: o papel do design da experiência do usuário na proteção da privacidade na era digital**. (Monografia para MBA em Tecnologias Digitais e Inovação Sustentável) – Escola Politécnica da Universidade de São Paulo, 2019. Orientador: Prof. Persival Ballesté

TECHOPEDIA. What Does Google Mean?. 13 maio 2020. Disponível em: <https://www.techopedia.com/definition/5359/google>. Acesso em: 25 maio 2022.

THE ECONOMIST. **The worlds most valuable resource is no longer oil but data**. [S. l.], 6 maio 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 8 nov. 2021.

**TRATADO DE PROTEÇÃO DE DADOS PESSOAIS** . [S. l.: s. n.], 2020-

Vasconcelos, Fellipe Paraguassú de Almeida Torres de. **Lei geral de proteção de dados pessoais: requisitos para o consentimento válido e interesse legítimo. 2020. Monografia (Bacharelado em Direito)** - Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2020.

VIOLA, MÁRIO; TEFFÉ, Chiara. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. 2020. Disponível em:

<https://civilistica.emnuvens.com.br/redc/article/view/510/384>

WALDMAN, Ari E., **Cognitive Biases, Dark patterns, and the 'Privacy Paradox'** 18 de setembro de 2019. 31 Current Issues in Psychology 2020, Disponível em: SSRN:

<https://ssrn.com/abstract=3456155>

Acesso 18 maio 2022

WOLFGANG, Ingo S. **Proteção de dados pessoais: para além da privacidade e autodeterminação informacional.** 16 jul. 2021. Disponível em:

[https://www.conjur.com.br/2021-jul-16/direitos-fundamentais-protECAo-dados-alem-privacidade-autodeterminacao-informacional#\\_ftn2](https://www.conjur.com.br/2021-jul-16/direitos-fundamentais-protECAo-dados-alem-privacidade-autodeterminacao-informacional#_ftn2). Acesso em: 16 nov. 2021.

YOON, Young-Ho; YOON, Hyun Shik. **A Case Study for Improvement of Users' Right to Informational self-determination: Focusing on the GDPR of EU and the CCPA of California, USA.** The Journal of Information Systems, 2019, 28.4: 65-103.

ZAKRZEWSKI, Cat. **Google deceived consumers about how it profits from their location data, attorneys general allege in lawsuits.** The Washington Post, 24 jan. 2022. Disponível em:

<https://www.washingtonpost.com/technology/2022/01/24/google-location-data-ags-lawsuit/>. Acesso em: 22 maio 2022.