INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA – IDP
ESCOLA DE DIREITO DO BRASIL – EDIRB
MESTRADO PROFISSIONAL INTERDISCIPLINAR EM DIREITO, JUSTIÇA E DESENVOLVIMENTO

JOSÉ GUSTAVO QUADRO

ANÁLISE DOS EFEITOS DA VIGÊNCIA DA LGPD NO BRASIL QUANTO AO PRINCÍPIO DA TRANSPARÊNCIA

ENTRE *WEBSITES* BRASILEIROS, AVISOS DE *COOKIES* E *DARK PATTERNS*

SÃO PAULO
2023

JOSÉ GUSTAVO QUADRO

ANÁLISE DOS EFEITOS DA VIGÊNCIA DA LGPD NO BRASIL QUANTO AO PRINCÍPIO DA TRANSPARÊNCIA

ENTRE *WEBSITES* BRASILEIROS, AVISOS DE *COOKIES* E *DARK PATTERNS*

Dissertação de Mestrado desenvolvida sob a orientação do Professor Doutor Danilo César Maganhoto Doneda (*in memoriam*) e coorientação da Professora Doutora Tainá Aguiar Junquilho, apresentado para obtenção do Título de Mestre em Direito, Justiça e Desenvolvimento.

SÃO PAULO

2023

JOSÉ GUSTAVO QUADRO

ANÁLISE DOS EFEITOS DA VIGÊNCIA DA LGPD NO BRASIL QUANTO AO PRINCÍPIO DA TRANSPARÊNCIA

ENTRE *WEBSITES* BRASILEIROS, AVISOS DE *COOKIES* E *DARK PATTERNS*

Dissertação de Mestrado apresentada ao Programa de Mestrado Interdisciplinar Profissional em Direito, Justiça e Desenvolvimento do IDP, como requisito para obtenção do título de Mestre em Direito, Justiça e Desenvolvimento.

Data da defesa: 31/05/2023

BANCA EXAMINADORA

Profa. Dra. Tainá Aguiar Junquilho
IDP-SP

Prof. Dr. João Paulo Lordelo Guimarães Tavares
IDP-SP

Profa. Dra. Yara Alves Gomes
Uninove

J83aa Quadro, José Gustavo

ANÁLISE DOS EFEITOS DA VIGÊNCIA DA LGPD NO BRASIL QUANTO AO PRINCÍPIO DA TRANSPARÊNCIA / José Gustavo Quadro.— São Paulo: Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, 2023.

188f.

Dissertação (Mestrado Profissional Interdisciplinar em Direito, Justiça e Desenvolvimento) — Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa: São Paulo, 2023.

Orientador(a): Dr. Danilo César Maganhoto Doneda
Coorientador(a): Dra. Tainá Aguiar Junquilho

1. LGPD. 2. Avisos de Cookies. 3. Dark Patterns. 4. Websites brasileiros. 5. Transparência. 6. Robô de software. 7. Pesquisa empírica. I. Título.

E conhecereis a verdade, e a verdade vos libertará.

João, 8:32

AGRADECIMENTOS

Somos a nossa história, o acúmulo das experiências. Somos hoje o que não fomos ontem e o que não seremos amanhã: a mudança, o constante movimento, o fluxo contínuo de energia interpessoal que corre por entre as n dimensões do cosmo. Somos parte dos outros, e os outros são partes de nós. E este trabalho é de muitas pessoas, não é só meu.

A minha família foi muito importante desde quando resolvi ingressar no curso de Mestrado no IDP. A lembrança daquela fina lâmina de água sobre os olhos dos meus queridos pais está gravada pra sempre na minha memória, e portanto o primeiro agradecimento é para a minha família, e também para os demais membros que sempre me apoiaram em tudo.

Também agradeço ao Dr. Flávio Vicente pelos aconselhamentos, e em especial à Dra. Ana Maria Maykot Prates Michels pelas inúmeras conversas que tivemos: você também foi minha orientadora informal – sem você, este trabalho não teria sido concluído.

Agradeço à orientadora Professora Dra. Tainá Aguiar Junquilho pela orientação na reta final e pelo fundamental apoio. Aos membros da banca de qualificação, Professor Dr. Thomas Victor Conti e Professor Dr. Bruno Ricardo Bioni, e da banca de defesa, Profa. Dra. Yara Alves Gomes e ao Prof. Dr. João Paulo Lordelo Guimarães Tavares também sou grato pelo compartilhamento de visões que enriqueceram este trabalho.

Agradeço ao Professor Dr. Fábio Lopes Toledo, certamente uma das pessoas mais competentes e responsáveis que já conheci: este trabalho também é seu.

Agradeço aos seguintes colegas do mestrado, em ordem alfabética: Ana Luiza Araújo, Marcella Leonel Viotti e Rodrigo Toler, pelo apoio mútuo durante todo o tempo. Agradeço pelo apoio dos amigos nos momentos difíceis.

Por fim, preciso agradecer ao Professor Dr. Danilo Cesar Maganhoto Doneda (*in memoriam*) de forma muito especial. Professor Danilo, esta certamente não é a mensagem que eu gostaria de escrever nesse momento. O Sr. foi a minha inspiração, e certamente a de muitos outros colegas, para ingressar no curso de Mestrado e pesquisar sobre Direito da Proteção de Dados. O Sr. foi o pioneiro nesta área no Brasil. A sua humildade sempre foi tão grande! E a sua contribuição como orientador desta pesquisa foi fundamental: não haveria esta linha de trabalho sobre a qual discutimos, e o resultado teria sido diferente. Muito se fala sobre o direito ao esquecimento, mas sempre nos lembraremos daqueles que construíram obras importantes durante o tempo em que viveram. E esta pesquisa também é seu legado, também é fruto do seu trabalho. Muito obrigado, Professor Danilo!

SUMÁRIO

RESUMO

O objetivo desta pesquisa foi analisar os efeitos da vigência da Lei Geral de Proteção de Dados quanto aos avisos de *cookies* nos *websites* brasileiros em relação ao princípio da transparência. Durante a pesquisa, foi construído um robô de software – *crawler bot* – para obter capturas de tela, captura dos *cookies* que são instalados nos dispositivos dos usuários quanto estes acessam os endereços eletrônicos, assim como as políticas de privacidade e os termos de uso. A análise foi automatizada e manual. Os resultados da pesquisa empírica feita sobre 1.282 *websites* com TLD ".br" durante os anos de 2020 e 2022, antes e depois da vigência da LGPD, permitiram a coleta de dados de 1.188 e 1.160 *websites* que estavam acessíveis naqueles anos respectivamente. Com a vigência da LGPD, o percentual de avisos de *cookies* subiu de 6,90% para 55,17% nos anos observados. A pesquisa identificou que o perfil predominante de avisos de rastreamento apresenta elementos afirmativos e informativos para obtenção de consentimento – 63,4% em 2020 e 58,12% em 2022 – e que elementos para negar ou customizar o tratamento de dados são pouco empregados. Quanto ao emprego de *dark patterns* nos avisos de rastreamento, a Ilusão de Controle, a Manipulação Estética e a Falsa Hierarquia são alguns dos padrões mais recorrentes. A presunção de consentimento tácito diminuiu, porém continua alta: de 59,76% para 46,25% nos dois anos observados. O destaque para o elemento afirmativo caiu de 93,90% para 86,25% Identificou-se que apenas 8 *sites* (0,69% do total de 1.160 endereços acessíveis em 2022) atendiam a critérios definidos como ideais para os *banners*, e que destes somente 4 *websites* (0,35% do total de 1.160 endereços acessíveis em 2022) atendiam a critérios adicionais sobre consentimento tácito, destaque para elemento afirmativo, uso de *cookie wall* e de língua estrangeira.

Palavras-chave: LGPD; Avisos de Cookies; Dark Patterns; Websites brasileiros.

ABSTRACT

The objective of this research was to analyze the effects of the validity of the General Data Protection Law regarding cookie notices on Brazilian websites in relation to the principle of transparency. During the research, a software robot – crawler bot – was built to obtain screen captures, capture of the cookies that are installed on the users' devices when they access the electronic addresses, as well as the privacy policies and terms of use. The analysis was both automated and manual. The results of the empirical research carried out on 1,282 websites with the ".br" TLD during the years 2020 and 2022, before and after the LGPD came into force, allowed the collection of data from 1,188 and 1,160 websites that were accessible in those years respectively. With the validity of the LGPD, the percentage of cookie warnings rose from 6.90% to 55.17% in the observed years. The research identified that the predominant profile of tracking notices has affirmative and informative elements to obtain consent – 63.4% in 2020 and 58.12% in 2022 – and that elements to deny or customize data processing are little used. As for the use of dark patterns in tracking warnings, the Illusion of Control, Aesthetic Manipulation and False Hierarchy are some of the most recurrent patterns. The presumption of tacit consent decreased, but remains high: from 59.76% to 46.25% in the two years observed. The emphasis on the affirmative element dropped from 93.90% to 86.25% It was identified that only 8 sites (0.69% of the total of 1,160 addresses accessible in 2022) met criteria defined as ideal for banners, and that of these, only 4 websites (0.35% of the total of 1,160 addresses accessible in 2022) met additional criteria on tacit consent, emphasis on affirmative element, use of cookie wall and foreign language.

Keywords: *LGPD; Cookie Notices; Dark Patterns; Brazilian websites.*

LISTA DE ABREVIATURAS E SIGLAS

5W2H – *Who? What? Where? When? Why? How? How Much?*

AED – Análise Econômica do Direito

ANPD – Autoridade Nacional de Proteção de Dados

API – *Application Programming Interface*

ASP – *Active Server Pages*

CCPA – *California Consumer Privacy Act*

CD/ANPD – Conselho Diretor da ANPD

CDC – Código de Defesa do Consumidor

CEO – *Chief Executive Officer*

CGF/ANPD – Coordenação-Geral de Fiscalização da ANPD

CGI – *Common Gateway Interface*

CGI.BR – Comitê Gestor da *Internet* no Brasil

CGTP/ANPD – Coordenação-Geral de Tecnologia e Pesquisa da ANPD

CIA – *Central Intelligence Agency*

CPF – Cadastro de Pessoa Física

CMP – *Consent Management Platform*

CSV – *Comma-Separated Values*

EC – *European Council*

EDPB – *European Data Protection Board*

EDVAC – *Electronic Discrete Variable Automatic Computer*

ENEM – Exame Nacional do Ensino Médio

ENIAC – *Electronic Numerical Integrator and Computer*

FIPPs – *Fair Information Privacy Principles*

FOIA - *Freedom of Information Act*

GB – Gigabyte

GDPR – *General Data Protection Regulation*

HTTP – *Hypertext Transfer Protocol*

HTTPS – *Hypertext Transfer Protocol Secure*

IAB Europe – *Interactive Advertising Bureau Europe*

ICC UK – *United Kingdom International Chamber of Commerce*

IETF – *Internet Engineering Task Force*

INEP – Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira

IoT – *Internet of Things* (*Internet* das Coisas)

IP - *Internet Protocol*

JSP – *Java Server Pages*

LAI – Lei de Acesso à Informação

LGPD – Lei Geral de Proteção de Dados

LIA – *Legitimate Interests Assessment*

Mbps – Megabits por segundo

MCI – Marco Civil da *Internet*

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

ONGs – Organizações Não-Governamentais

PDF – *Portable Document File*

PETs – *Privacy Enhancing Technologies*

PHP – *PHP: Hypertext Processor*

RAM – *Random Access Memory*

RFC – *Request for Comments*

RTB – *Real-Time Bidding*

SaaS – *Software as a Service*

SEI – Sistema Eletrônico de Informações

STF – Supremo Tribunal Federal

TB – Terabyte

TCF – *Transparency and Consent Framework*

TC String – *Transparency and Consent String*

TJUE – Tribunal de Justiça da União Europeia

TLD – *Top-Level Domain*

URL – *Uniform Resource Locator*

UX – *User Experience*

WP29 – *Working Party* 29

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

Após fazer pesquisas sobre imóveis e investimentos financeiros em um *website* com o seu computador, o usuário de *Internet* entra no *Youtube*, assiste a um vídeo qualquer, e depois assiste a uma aula *online* em alguma plataforma de educação à distância. No dia seguinte, essa mesma pessoa usa novamente o computador para acessar o *Facebook* e ver as postagens dos seus amigos na rede social, e então lê os *emails* do GMail e responde a alguns deles, deixando pra trás aquele *email* com publicidade do mais novo lançamento imobiliário da sua cidade. Já no próximo dia, a pessoa depara-se com um anúncio publicitário de um novo curso sobre investimentos financeiros que promete deixá-la milionária. Esta descrição é fiel à experiência que as pessoas têm ao utilizar os serviços de *Internet* atualmente, e desde muitos anos. A situação descrita pode ter várias denominações, mas pode-se também chamá-la de publicidade comportamental *online*.

Esta prática tira proveito de tecnologias subjacentes aos navegadores de internet. Uma dessas tecnologias é o *cookie*, que é definido na RFC 6265 da Internet Engineering Task Force, que define o padrão HTTP. O padrão HTTP originalmente não possuía controle de estado, sendo chamado de *stateless*. Isto significa que, entre uma mensagem e outra, o padrão HTTP básico não possui a capacidade de controlar os estados entre as requisições. Não tendo controle de estado, não é possível identificar quem é quem no emaranhado de conexões da Internet. Por exemplo, se dois usuários enviassem requisições para um mesmo aplicativo de *Internet Banking*, este aplicativo não teria condições de identificar qual requisição deve receber qual resposta de saldo em conta corrente, ou seja, os saldos poderiam ser enviados para as pessoas erradas. Este é um funcionamento de um protocolo de comunicação *stateless*. Para que cada usuário seja informado acerca do saldo da sua conta bancária corretamente, é preciso que, junto com a requisição de saldo, o usuário informe o nome e o valor do seu cookie de identificação. Este nome e valor foi, obviamente, fornecido anteriormente pela própria aplicação de *Internet Banking* quando a pessoa acessou o sistema. Para contornar o problema de não conseguir identificar a quem pertence qual requisição, foi criada a tecnologia de *cookies*.

Tecnologicamente, os cookies são criados conforme descrito a seguir. Uma mensagem HTTP é enviada do servidor para o navegador do usuário, ordenando a criação de um *cookie*. A criação do *cookie* é feita pelo cabeçalho “Set-Cookie”, seguido pelo nome e valor respectivo. Por exemplo, “Set-Cookie nomeDoMeuPrimeiroCookie=valorDoMeuPrimeiroCookie”. O navegador recebe a

mensagem HTTP, interpreta e cria em sua memória um registro com o nome e o valor do *cookie*. Nas interações seguintes com o primeiro *website* ou outros, os *cookies* são enviados conforme as respectivas configurações. Assim, o usuário do navegador pode transitar entre páginas do mesmo *website* e manter um carrinho de compras, ou navegar entre distintos *sites* e informar os mesmos *cookies*, o que permite que seja feito o rastreamento das pessoas entre *sites* distintos.

Este trabalho se justifica por seu caráter multidisciplinar: trata sobre o tema de Proteção de Dados Pessoais, e assim transita entre o Direito e a Tecnologia da Informação, abordando assuntos de Direito ligados a Proteção de Dados Pessoais e tópicos mais específicos de Tecnologia da Informação, como será visto adiante, além da economia comportamental, sobretudo por conta do emprego de *dark patterns* neste campo de pesquisa.

Pretende-se, nesse sentido, responder à seguinte pergunta: sob a ótica do princípio da transparência, qual foi o impacto da vigência da Lei Geral de Proteção de Dados nos *websites* brasileiros quanto à apresentação dos avisos de *cookies*?

Com o objetivo de responder à pergunta de pesquisa, serão analisados os avisos de *cookies* capturados antes e depois da vigência da LGPD para identificar quais características destes avisos foram alteradas após o vigor da lei. Os avisos de *cookies* serão avaliados sob a ótica do princípio da transparência, para caracterizar a anatomia, os leiautes e os conteúdos dos respectivos avisos, investigando assim o emprego de padrões em conformidade legal, *dark patterns* e *nudges*.

O escopo desta pesquisa abrange a captura e coleta de dados e documentos provenientes de *websites* brasileiros. Apenas *websites* com terminação ".BR" foram considerados. A captura e coleta de dados e documentos dos *websites* brasileiros foi realizada em dois momentos: antes e depois da vigência da LGPD, em junho de 2020 e em agosto de 2022. Após a captura e coleta, os dados e documentos foram analisados individualmente, com resultados apresentados em separado para cada momento de coleta. Em seguida, as análises individuais de cada momento de coleta foram comparadas entre si, para identificar o impacto da vigência da LGPD sobre os *websites* brasileiros no recorte de pesquisa relacionado aos *cookies* e respectivos avisos de *cookies*, que são o objeto deste estudo.

O escopo da pesquisa não abrange a análise dos *websites* brasileiros sobre a prática de captura de geolocalização, a adoção da técnica de *fingerprinting*, nem o emprego de

outros elementos de rastreamento como *pixels*, *web beacons* ou *web bugs*. Esta pesquisa também não aborda a análise de rastreamento por ultrassom, o monitoramento por *watermarking* e outras tecnologias. A pesquisa também não aborda outros tipos de dispositivos tecnológicos de *hardware*, tais como *smartphones*, ou dispositivos de *Internet* das Coisas (IoT). Ainda, a pesquisa não analisa aplicativos de *smartphones*, nem aplicativos que tenham *websites* embutidos neles. Apesar disto, as discussões sobre avisos de *cookies* são igualmente válidas para outras tecnologias de rastreamento, que têm ganhado cada vez mais espaço no mundo *online*.

Esta pesquisa é relevante porque não foi encontrada, na revisão de literatura de Direito, de Ciência da Computação ou de outras áreas correlatas, pesquisa científica que investigue diretamente como a implementação de *websites* no Brasil foi influenciada pela vigência da Lei Geral de Proteção de Dados. Este estudo também é importante porque não foi identificado outro estudo que efetue a análise, em maior escala, dos *cookies* e avisos de *cookies* provenientes de *websites* brasileiros com a vigência da LGPD.

Após esta introdução, o segundo capítulo discute conceitos sobre o relacionamento entre a economia comportamental, o direito e a tecnologia. O capítulo apresenta também *dark patterns* e indica como eles podem ser encontrados nos resultados da pesquisa empírica. Este capítulo apresenta ainda conceitos relacionados a tecnologia da informação e que são usados no desenvolvimento do texto que segue, explicando sobe alguns mecanismos tecnológicos de apoio ao rastreamento *online*.

O terceiro capítulo consolida conceitos de privacidade, proteção de dados pessoais, o princípio da transparência e outros princípios que aqui importam, e ainda legislações sobre o tema tratado no estudo, servindo de referencial teórico para a pesquisa, cujo substrato jurídico-dogmático também se aperfeiçoa com a visão da ótica do direito privado, notadamente a legislação e a doutrina consumerista. Este capítulo também traz decisões jurisprudenciais e soluções orientadoras, provenientes de órgãos reguladores, sobre o emprego de *cookies* e respectivos avisos de *cookies*.

O quarto capítulo detalha os aspectos de metodologia científica da pesquisa utilizados durante o trabalho. O capítulo detalha o procedimento utilizado para a eleição dos *websites* analisados, descreve como ocorreu o desenvolvimento da ferramenta de captura e coleta de dados e documentos, e ao fim apresenta como foi realizada a consolidação e a análise dos dados e dos documentos coletados.

O quinto capítulo apresenta os resultados das análises realizadas após a captura e a coleta dos dados e dos documentos dos *websites* brasileiros, conforme a metodologia exposta no terceiro capítulo. Esta parte também apresenta respostas às perguntas de pesquisa por meio da análise dos resultados, à luz do referencial teórico, empregando os conceitos e comparando com os trabalhos relacionados. O capítulo contém análises de estatística descritiva, com análises quantitativas e qualitativas, tabelas e gráficos com os resultados encontrados durante as capturas e coletas realizadas antes e também depois da vigência da LGPD. É apresentada também uma comparação entre as análises de antes da LGPD e as análises dos dados capturados depois da LGPD. Por fim, o capítulo também responde às perguntas de pesquisa, identificando o impacto que a vigência da LGPD sobre a implementação dos *websites* brasileiros em relação aos *cookies* e aos *banners* de *cookies*.

Por fim, as considerações finais retomam a pergunta de pesquisa, resumem o processo de captura e coleta de dados e documentos, revisita o levantamento de trabalhos relacionados, consolida as respostas à pergunta de pesquisa pelas análises dos dados e documentos capturados, apresenta demais considerações e indica os caminhos futuros de pesquisa nesta área.

2 DIREITO, TECNOLOGIA, ECONOMIA E COMPORTAMENTO HUMANO: TÃO DISTANTES E TÃO PRÓXIMOS

A crescente e cada vez mais profunda dependência das tecnologias faz com que a interação das pessoas com o ambiente *online* aumente. Este constante reforço da relação entre as pessoas e o mundo tecnológico é percebido cotidianamente na vida de grande parte da humanidade. Todas as ciências, de alguma forma, se beneficiam dos avanços tecnológicos, assim entendidos como os avanços da tecnologia digital implementada em computadores, dispositivos móveis, eletrodomésticos, aparelhos de telefone, relógios e toda a sorte de dispositivos que se possa imaginar.

Algumas destas ciências que se beneficiam das vantagens que a tecnologia digital proporciona também estudam os avanços desta mesma tecnologia, assim como investigam as transformações que a tecnologia causa na própria sociedade, seja no âmbito internacional, seja nas relações governamentais, ou ainda nas corporações privada, no seio das famílias e nas mutações comportamentais dos próprios indivíduos. Dentre essas ciências que estudam tais fenômenos propiciados pelo crescente avanço e dependência tecnológica, pode-se elencar o Direito, a Antropologia, a Sociologia, a Economia, a Psicologia, a Ciência Política, a Ciência da Informação e tantas outras.

A Ciência do Direito também estuda esses acontecimentos. Há diversas áreas do Direito que se debruçam sobre a tecnologia, como a Análise Econômica do Direito, o Direito Civil, o Direito Constitucional, o Direito Processual Civil, culminando com o despontar de um novo ramo do Direito que é chamado de Direito Digital. O Direito Digital, por sua vez, abarca uma série de temas distintos e inter-relacionados, tais como Direito e Inovação, Direito e Startups, Inteligência Artificial, *Blockchain*, *Open Banking*, e Direito da Proteção de Dados Pessoais. O Direito da Proteção dos Dados Pessoais, por sua vez, tem seus próprios fundamentos, mas também precisa recorrer a conceitos clássicos do Direito, tanto de Direito Civil, quanto de Direito Constitucional, de Direito do Consumidor e outras disciplinas.

A relação entre as pessoas e os ambientes tecnológicos, fomentado em sua grande maioria de vezes pelo emprego de dispositivos eletrônicos com capacidade computacional e também pela *Internet*, pode ocorrer no meio *online* ou *offline*. A interação *online* ocorre, via de regra, quando há emprego de alguma forma de interconexão entre um dispositivo acessado por uma pessoa e outro computador, com troca de dados entre eles, e interação – ou não, por monitoramento – entre a pessoa e o

dispositivo. No meio *offline*, a interação acontece quando a pessoa acessa um dispositivo que não tem conexão com o mundo exterior, isto é, não acessa outros recursos computacionais extrínsecos. Quando esses dispositivos que estão *offline* são quaisquer outros que não os computadores tradicionais ou *smartphones*, é comum classificá-los como sendo dispositivos da *Internet* das Coisas.

Independentemente de haver ou não conexão com outra rede, com a *Internet* ou qualquer outra espécie de conectividade, existe uma relação entre a pessoa e o dispositivo. O Direito da Proteção dos Dados Pessoais, ou simplesmente Direito de Proteção de Dados, oferece ferramentas para o estudo da relação entre as pessoas e a tecnologia com foco em resguardar os direitos individuais das pessoas. Para cumprir sua função, esta área do Direito precisa estudar tanto os aspectos relacionados à própria pessoa natural quanto os aspectos relacionados à tecnologia e os relacionados aos fornecedores de tecnologia e agentes de tratamento.

Sobre a pessoa natural, o Direito da Proteção de Dados estuda elementos como os direitos da personalidade, os direitos fundamentais, o próprio direito à proteção de dados, a privacidade, a autodeterminação informativa, as mudanças culturais e comportamentais do próprio indivíduo consigo mesmo e com outras pessoas e a sociedade. Sobre a tecnologia, o Direito da Proteção de Dados estuda os procedimentos de implementação de governança de dados, a conformidade com leis e regulamentos, e assuntos congêneres. Quanto aos fornecedores de tecnologias e agentes de tratamento, são estudados diversos assuntos como os fatores de equiparação entre fornecedores e outros agentes de tratamento, a responsabilidade civil, e a relação com o direito do consumidor.

Há ainda outro ponto de interesse do Direito da Proteção de Dados que reside na relação entre as pessoas naturais e os agentes de tratamento de dados, ou ainda entre as pessoas naturais e as outras pessoas, naturais ou jurídicas, que interagem entre si, fornecendo tecnologia própria ou utilizando tecnologia de terceiros.

Para o estudo realizado nesta pesquisa, alguns fundamentos são úteis para a discussão dos resultados. Como este trabalho aborda a transparência, os *websites*, os *cookies*, os avisos de *cookies*, o consentimento, o legítimo interesse, as políticas de privacidade e tantos outros pontos correlacionados, é interessante tratar sobre alguns elementos como privacidade, proteção de dados pessoais, princípio da transparência, bases legais de tratamento de dados, e a legislação brasileira e internacional que tem influência na utilização de *cookies* e avisos de *cookies*.

2.1 Economia Comportamental

Os debates sobre economia comportamental iniciaram no século XX com Herbert Simon e outros, desenvolvendo-se de forma mais ampla e profunda com acadêmicos como Richard Thaler, Amos Tversky, Daniel Kahneman e outros (THALER, 2016, p. 2). A economia neoclássica enxerga os sujeitos como agentes que têm bem definidas as suas preferências e são despidos de vieses ou preconceitos, que tomam decisões ótimas com base nas preferências, e que agem de acordo com seus próprios interesses (THALER, 2016, p. 3): esta é a definição de *homo economicus* (*econs*, para Thaler) dada pela ciência econômica tradicional, enquanto a economia comportamental acrescenta o aspecto do comportamento humano às decisões, cujos representantes seriam os *homo sapiens*, ou *humans*, que nada mais são do que os seres humanos reais (THALER, 2016, p. 3). O *homo economicus* é visto, assim, como um sujeito imparcial e sem sentimentos, enquanto o ser humano real é visto tal como é, com todas as suas imperfeições.

A economia comportamental une as ciências econômicas e da psicologia para estudar os fenômenos da economia (SAMSON, 2015, p. 27), e é vista como uma nova área de estudo das ciências econômicas. Para explicar a importância do assunto, Thaler faz uma analogia: estudar física considerando as condições ideais no vácuo é diferente de realizar o mesmo estudo com a presença do ar atmosférico, cuja existência é reconhecida pelos físicos; o estudo clássico da economia, no entanto, prescindiu do elemento comportamental, cuja existência foi anulada, mas que influencia nos resultados das decisões econômicas realizadas pelos agentes (THALER, 2016, p. 4).

Assim, o *homo economicus* é o agente que toma decisões racionais com vistas a maximizar os resultados, sem outras influências, enquanto as decisões do *homo sapiens* são afetadas por diversos fatores que repercutem na racionalidade. Samson explica que tais fatores originam-se de vieses e heurísticas, assim como de racionalidade limitada, e ainda de fatores sociais. As heurísticas são as tomadas de decisão automáticas, intuitivas e inconscientes realizadas pelos agentes econômicos; os vieses são as tendências, os vícios, as inclinações desses mesmos agentes. A racionalidade limitada reconhece que o *homo sapiens* tem limitações, sejam elas de conhecimento ou de capacidade efetiva de raciocínio; os fatores sociais estão ligados a confiança e desonestidade, assim como a justiça e reciprocidade, e outros (SAMSON, 2015, pp. 29-35). Thaler (2016, p. 5) afirma que uma das hipóteses da pesquisa de Kahneman e Tversky era de que as pessoas fazem escolhas com base em heurísticas.

Para Samson (2015, pp. 29-35), a economia comportamental reconhece, por exemplo, que os seres humanos: têm um viés temporal otimista e por isso subestimam fatores de tempo e custo nos planejamentos; têm um viés temporal de preferir recompensas mais imediatas, e por isso têm mais dificuldade em poupar para o futuro; têm tendência a retribuir gestos de outras pessoas; têm a tendência a cumprir normas sociais, como os costumes; têm aversão a mudança, tendendo a manter a inércia, isto é, o mesmo comportamento. Da mesma forma que os vieses, as heurísticas têm um papel importante: por exemplo, a heurística da disponibilidade é usada pelos seres humanos para calcular a probabilidade de ocorrência de um evento com base na quantidade de vezes que a pessoa se lembra de tal evento ter ocorrido, o que pode induzir o agente a erro, pois de fato a probabilidade de ocorrência de um evento independe de quantas vezes ela se lembra de tal evento ter acontecido (JOLLS; SUSTEIN; THALER, 1998, p. 1477).

Sustein e Thaler (2008) reconhecem um viés importante para esta pesquisa, que é o viés do status quo ou viés da inércia, ou ainda a heurística de "tanto faz": ainda que não seja realmente bom para eles, os agentes econômicos tendem a escolher o caminho de menor esforço, e é por este motivo que as pessoas tendem a manter as opções-padrão dentre demais possibilidades de escolha.

2.2 Economia Comportamental e Análise Econômica do Direito

Para este estudo, é relevante contextualizar em relação ao campo do conhecimento denominado *Law and Economics*, ou Análise Econômica do Direito (AED), e enfatizar que a AED pode ser influenciada pela economia comportamental, como será visto adiante. A análise econômica do direito estuda a ciência do direito com as lentes da ciência econômica, pressupondo que os agentes interagem com o direito conforme a definição econômica clássica: atuam com vistas à maximização da utilidade; têm suas preferências bem definidas, sem vieses ou preconceitos; e decidem conforme seus próprios interesses (JOLLS; SUSTEIN; THALER, 1998, p. 1476). Ou seja, a análise econômica do direito convencional enxerga o sujeito de direitos como sendo um *homo economicus*.

A análise econômica comportamental do direito, por sua vez, adiciona o elemento humano, o elemento real no estudo do direito do ponto de vista econômico, deslocando o espectro de visão de como enxerga o sujeito, ajustando o foco do *homo economicus* para o ser humano real (JOLLS; SUSTEIN; THALER, 1998, p. 1476). Assim como existe a

relação entre o mundo do direito e o mundo dos fatos, há relação entre a economia racional, neoclássica, e a economia comportamental.

2.3 *Homo Economicus* e o ser humano real – *Homo Sapiens*

Como já afirmado anteriormente, o comportamento humano real é influenciado pela imperfeição do ser humano, Jolls, Sustein e Thaler (1998, p. 1476) apresentam, de forma não exaustiva, três fatores que podem limitar o ser humano e assim diferenciá-lo do *homo economicus*: a racionalidade limitada, a força de vontade limitada e os interesses próprios limitados.

Jolls, Sustein e Thaler (1998, p. 1477) atribuem a criação do termo racionalidade limitada ao economista Herbert Simon, para quem a racionalidade do homem é falha, tanto na capacidade de processamento do pensamento quanto na habilidade de gestão da memória, e assim o ser humano real apresenta limitações de ordem. Ou seja, o ser humano real não é capaz de tomar as melhores decisões de forma ótima, nem maximizando os resultados, muito menos todas as vezes, tal como o *homo economicus* supostamente o faz.

Os mesmos autores afirmam que a força de vontade limitada, tida como elemento restritivo da atuação do agente econômico - ou sujeito de direitos - consiste no fato de que as pessoas tomam decisões contrárias aos seus interesses de longo prazo, e isso acontece porque elas preferem obter recompensas instantâneas ao invés de pensar nos benefícios futuros: fumantes prefeririam não fumar, mas fumam; não poupadores prefeririam poupar, mas não poupam; então, elas tentam diminuir os efeitos contratando um plano para parar de fumar, ou preferem que seja instituído um plano compulsório de previdência (JOLLS; SUSTEIN; THALER, 1998, p. 1479). Assim, a força de vontade limitada que caracteriza os seres humanos reais, que "dizem uma coisa e fazem outra", contrasta com a característica do *homo economicus* que "sabe o que quer".

O fator derradeiro que diferencia os *Econs* e *homo sapiens*, ainda segundo Jolls, Sustein e Thaler (1998, p. 1479), é o interesse próprio limitado, que leva as pessoas a se comportarem de forma mais generosa ou maldosa de acordo com a forma como são tratadas por outras pessoas, ou de acordo com o comportamento aceitável ou reprovável exercido por terceiros. A limitação nos interesses próprios é a característica segundo a qual nem sempre as tomadas de decisão dos seres humanos atenderão aos próprios interesses objetivos: por envolver elementos subjetivos que influenciam o comportamento, as pessoas podem tomar atitudes que, do ponto de vista do *homo*

economicus, não a favorecem. Para ficar claro, um exemplo desta característica acontece quando uma pessoa retribui a gentileza de outrem entregando um presente de valor relativamente significativo, apesar de aquela estar passando por um processo de readequação de seus gastos pessoais.

É possível entender, deste modo, que as características do ser humano real indicadas até aqui não se contrapõem às características do *homo economicus*, mas limitam-nas, e assim para a economia comportamental - e portanto para a análise econômica comportamental do direito - os seres humanos reais são instâncias defeituosas e carregadas de vieses, heurísticas, defeitos e imperfeições e que, como manifestação da realidade concreta, contrastam com a abstração do ser humano hipotético denominado *homo economicus* trazido pela economia neoclássica. Todavia, apesar de tais caracteres serem amplamente difundidos, a caracterização do comportamento humano não pode ser reduzida apenas a eles, pois o ser humano comporta-se de maneira muito mais complexa.

2.4 A influência da economia comportamental na análise econômica do direito: desdobramentos para a autodeterminação informativa e a liberdade de escolha

Para Jolls, Sustein e Thaler (1998, pp. 1533-1534), a economia tradicional sugere que a carência de informações sobre determinado assunto pode ser suprida simplesmente pelo aumento do volume de informações disponibilizadas ao público alvo, isto é, a economia comportamental entende que o aumento do volume de informações fornecidas pode não ser suficiente, pois a forma de entrega das informações também importa: ao tratar sobre a forma de apresentação das informações, é comum deparar-se com a impossibilidade de manter a neutralidade na comunicação.

A maneira como as informações são concebidas e apresentadas influencia na forma como a mensagem é recebida pela pessoa. Assim, se as informações da mensagem forem um conjunto de alternativas apresentadas para realizar uma escolha, então tanto a configuração deste conjunto de opções quanto a forma de exposição dessas alternativas influenciam sobremaneira a tomada de decisão a ser feita.

Os mesmos autores trazem um exemplo de apresentação de informações sobre tomada de decisão na contratação de plano de aposentadoria, com duas opções de escolha: um fundo de títulos públicos, aplicação mais conservadora, e outro fundo de ações, aplicação mais arrojada, mas que tem potencial maior de valorização no longo prazo. Para um grupo de pessoas, foram apresentadas as informações sobre valorização no prazo de

30 anos. Para outro grupo, foram apresentadas as mesmas informações de valorização do fundo de aposentadoria, só que no prazo de 1 ano. O grupo que recebeu as informações sobre potencial de retorno em 30 anos escolheu aplicar no fundo baseado em ações; e o grupo que recebeu informações limitadas a 1 ano optou pelo fundo previdenciário lastreado em títulos públicos. Deste exemplo, concluiu-se que quem elabora as alternativas de escolha e determina a forma de apresentação destas alternativas acaba por influenciar a tomada de decisão, sendo irrelevante para tal raciocínio se uma alternativa ou outra é a melhor (JOLLS; SUSTEIN; THALER, 1998, pp. 1534-1535).

Assim, aquele que exige ou que orienta sobre o fornecimento de informações não deve se ater apenas a indicar sobre o dever de informar: deve também orientar sobre a forma como a informação deve ser entregue; Jolls, Sustein e Thaler (1998, p. 1535) trazem então o exemplo de um aviso obrigatório aos funcionários de uma empresa sobre o emprego de substâncias perigosas no trabalho: enquanto a empresa pode preferir um aviso mais tênue, mais brando, o órgão regulador pode indicar que o teor da mensagem deva ser impactante. Outro exemplo de forma de apresentação de mensagem com maior nível de impacto, no Brasil, é a exibição de fotografias de pessoas fumantes, nas caixas de cigarro, mostrando as consequências negativas de seus vícios.

Jolls, Sustein e Thaler (1998, pp. 1535-1536) questionam sobre o que significa "tomada de decisão informada", e confrontam seu significado com a teoria dos prospectos. A chamada teoria dos prospectos, ou teoria da perspectiva, desenvolvida por Kahneman e Tversky, expõe que os seres humanos têm aversão a perda, e que a semântica das palavras empregadas nas alternativas afeta o resultado do processo decisório, quando as opções de escolha são apresentadas – *framed* – como ganhos ou como perdas para o indivíduo, e o resultado é devido ao *framing effect* (THALER, 2016, p. 6).

Pesquisa sobre a teoria dos prospectos também confirmou que a forma como é apresentada a mensagem influencia no resultado do processo decisório; estes autores realizaram pesquisa empírica com 200 pessoas, criando dois processos de tomada de decisão: o primeiro com mensagem positiva, e outro que tinha mensagem com teor negativo, e constataram ao final da pesquisa que o grupo de pessoas que recebeu a mensagem positiva teve maior propensão a aceitar o que foi proposto no processo decisório, enquanto que o grupo que teve que decidir com base em uma mensagem negativa escolheu não aceitar a proposta que lhes havia sido feita (BUDA; ZHANG, 2000). Este resultado aconteceu porque o ser humano tem normalmente aversão ao risco. Assim, o que realmente se pode entender por "tomada de decisão informada"? A depender

de como as alternativas de escolha apresentam teor positivo, teor negativo ou outro, é possível influenciar para um lado ou para o outro os resultados das escolhas dos indivíduos; ou seja, qualquer que seja o formato apresentado nas alternativas, os resultados decisórios serão potencialmente diferentes.

Colocando em prática a análise econômica comportamental do direito, os autores sugerem que o governo tire proveito das características humanas na elaboração de políticas públicas: explorar a aversão a perdas, explorar a saliência e não ser tão otimista.

Outra forma de explorar as características comportamentais humanas na tomada de decisão é tornar as informações mais salientes (JOLLS; SUSTEIN; THALER, 1998, p. 1537). O ser humano tem capacidade limitada de atenção, e quando certas coisas não estão destacadas, passam despercebidas. Sustein afirma que os mágicos e os vendedores de automóveis usados são mestres em evitar as saliências, assim como certos serviços que as pessoas contratam e em cujos termos não se repara (SUSTEIN, 2014, p. 40).

Como já explicado, os seres humanos reais possuem, vieses, heurísticas e crenças. As crenças são informações que habitam o pensamento das pessoas antes mesmo de elas receberem novas informações para outra tomada de decisão. Uma das crenças comuns às pessoas é o excesso de otimismo.

O excesso de otimismo faz com que as pessoas subestimem a probabilidade, e julguem que a escolha que fizeram terá resultados positivos, mesmo que a estatística mostre que não é bem assim. A autoconfiança faz com que as pessoas pensem que seu desempenho está acima da média.

Para Jolls, Sustein e Thaler (1998), uma forma de tirar vantagem do otimismo das pessoas é enfatizar o quão boas, excelentes ou superiores elas são em determinado aspecto, para incentivá-las a agir de acordo com o que se espera em relação àquele aspecto. Os autores exemplificam que uma campanha de trânsito seguro poderia enfatizar que os motoristas que leem a mensagem são realmente bons, e que o problema está nas outras pessoas: "[d]irija defensivamente: cuidado com o outro cara" (JOLLS; SUSTEIN; THALER, 1998, p. 1537); este tipo de informação comunicada usa a característica comportamental do excesso de otimismo para incentivar que os motoristas decidam dirigir com mais segurança.

A forma de apresentação das informações, o *framing effect*, a exploração de saliências, a aversão a perdas e a questão do otimismo, como elementos de economia comportamental, afetam diretamente a liberdade de escolha do indivíduo e, portanto, a autodeterminação informativa quando a decisão envolver seus dados.

2.5 Economia comportamental, arquitetura de escolhas e *nudges*

Como visto até este ponto, a economia comportamental estuda - dentre outros aspectos - os fatores que influenciam a tomada de decisão pelo ser humano, tais como vieses, crenças, preconceitos e heurísticas. Também já foi exposto que a apresentação do conjunto de escolhas possíveis é um fator que também influencia a decisão. Assim, à configuração da estrutura das opções de escolhas dá-se o nome de arquitetura de escolhas. Assim, a arquitetura de escolhas abrange a forma de apresentação das opções, a disponibilidade das opções, e ainda o relacionamento entre as opções. Para Sustein e Thaler (2008, p. 125), aqueles que influenciam as tomadas de decisão são considerados arquitetos de escolhas; além disso, é importante que a arquitetura das escolhas leve em consideração o comportamento humano. O arquiteto de escolhas é responsável por "organizar o contexto no qual as pessoas tomam decisões" (SUSTEIN; THALER, 2008, p. 8).

A arquitetura de escolhas existe sempre que houver algum ponto de decisão. A decisão pode ser tomada apenas de modo racional, pode ser influenciada por aspectos presentes na elaboração das opções, ou ainda por fatores externos às próprias opções, mas que também exercem influência. Elementos que interferem nas decisões podem ser as habilidades cognitivas, o conhecimento, as crenças, o contexto, as circunstâncias, as motivações, as emoções e as percepções. Por exemplo: não perceber um determinado risco que existe; a emoção presente na aversão a perdas; a motivação presente - ou ausente - na perseguição de metas de longo prazo; as circunstâncias da realidade pessoal do indivíduo decisor; o contexto, que pode ser social, econômico ou de outra ordem e que afeta a decisão; a habilidade cognitiva, que favorece ou não o processamento de informações e o uso da memória; e as crenças, que são conclusões pré-formadas sobre algo, permeadas de elementos objetivos e subjetivos. Sustein e Thaler (2008, pp. 9-10) afirmam que meros detalhes presentes na arquitetura de escolhas podem impactar significativamente os resultados, e assim é preciso considerar que todos os aspectos relacionados à decisão interessam no projeto dos sistemas de decisão.

O arquiteto de escolhas, portanto, precisa realizar decisões de projeto, precisa definir a arquitetura das escolhas. A definição das particularidades das escolhas é realizada pelo arquiteto de escolhas, que pode então favorecer um ou outro tipo de opção. O nível de intensidade da influência exercida pelo arquiteto de escolhas vai desde o

(utópico?) nível neutro ou quase neutro, passando pela sutileza, e indo até o extremo da força, esta última representada por alguma escolha única obrigatória, ou ainda pela ausência de qualquer opção, que também tem o mesmo resultado de ignorar a vontade do indivíduo que possuiria, em tese, o poder de decisão.

Sustein e Thaler (2008, p. 10) apresentam o movimento do paternalismo libertário, segundo o qual: "as pessoas devem ter liberdade de fazer o que quiserem, inclusive recusar acordos desvantajosos"; e "os arquitetos de escolha têm toda a legitimidade para tentar influenciar o comportamento das pessoas, desde que seja para tornar a vida delas mais longa, mais saudável e melhor".

Os mesmos autores, ainda, conceituam *nudge* da seguinte maneira:

> [e]sse *nudge*, na nossa concepção, é um estímulo, um empurrãozinho, um cutucão; é qualquer aspecto da arquitetura de escolhas capaz de mudar o comportamento das pessoas de forma previsível sem vetar qualquer opção e sem nenhuma mudança significativa em seus incentivos econômicos. Para ser considerada um *nudge*, a intervenção deve ser barata e fácil de evitar. Um *nudge* não é uma ordem. Colocar as frutas em posição bem visível é um exemplo de *nudge*. Simplesmente proibir a *junk food*, não (SUSTEIN; THALER, 2008, p. 12).

Hansen, revisitando a definição de *nudge* cunhada por Sustein e Thaler, e usando definições de outros autores, compilou a seguinte definição de *nudge*:

> Um *nudge* é uma função de (I) qualquer tentativa de influenciar o julgamento, escolha ou comportamento das pessoas de uma forma previsível, que é (1) possível devido a limites cognitivos, vieses, rotinas e hábitos nas decisões individuais e sociais. criando barreiras para que as pessoas atuem racionalmente em seus próprios interesses autodeclarados, e que (2) funciona fazendo uso desses limites, preconceitos, rotinas e hábitos como partes integrantes de tais tentativas.
> Assim, um *nudge*, entre outras coisas, funciona independentemente de:
> (i) proibir ou adicionar quaisquer opções de escolha racionalmente relevantes,
> (ii) mudança de incentivos, sejam considerados em termos de tempo, problemas, sanções sociais, econômicas e assim por diante, ou
> (iii) o fornecimento de informações factuais e argumentação racional (HANSEN, 2016, tradução nossa).

2.6 Aplicando *nudges*

Os exemplos trazidos por Sustein e Thaler, como o emprego de adesivo com a imagem de uma mosca grudado nos urinóis do aeroporto de Amsterdã para incentivar as pessoas a fazerem xixi no lugar certo, e o caso da organização das prateleiras do supermercado para favorecer o consumo de produtos saudáveis, identificam claramente a aplicação do conceito de *nudge*. O conceito de *nudge* para tais autores, que são alguns dos pioneiros no estudo da economia comportamental, considera que algo só é *nudge* se a influência - exercida pelas definições que são feitas na concepção da arquitetura de

escolha - for cumulativamente: sutil, fácil de ser desconsiderada e ainda beneficiar o indivíduo; então, conforme esta ideia, se alguma prática não tiver tais caracteres, não poderia ser considerada *nudge*. Quando uma prática que influencia a decisão não puder ser enquadrada como *nudge*, Thaler a denomina de *sludge* (THALER, 2018, p. 3). Há autores, como Graßl e outros, que classificam como *nudges* todas as práticas que exercem influência, sejam elas benéficas ou não: nesta classificação, estão incluídos os *nudges* sutis, os que atuam no interesse do indivíduo, os *nudges* mandatórios, assim como os que interessam apenas ao arquiteto de escolhas e não à pessoa que escolhe, estes últimos classificados como *dark patterns* (GRAßL *et. al.,* 2021, pp. 1-3). Para este trabalho, *nudges* são entendidos como as práticas que sutilmente influenciam as pessoas em favor de seus interesses, em linha com o conceito de Sustein e Thaler.

Até este ponto, foi discutido sobre como a economia comportamental se debruça sobre as tomadas de decisão, sua interface com a análise econômica do direito, os fatores que interferem nas decisões. Também foi apresentada a arquitetura de escolha e os *nudges*. O entendimento doutrinário é de que toda formulação de escolha tem uma arquitetura, a arquitetura de escolhas; de que a concepção de toda arquitetura de escolhas, feita pelo arquiteto de escolhas, precisa de decisões de projeto; de que as decisões de projetos feitas pelos arquitetos de escolhas sempre influenciam os resultados das escolhas feitas; de que é necessário ao arquiteto de escolhas entender sobre o funcionamento do comportamento humano para criar arquiteturas de escolhas que considerem tal aspecto comportamental; de que as influências feitas pelos arquitetos de escolhas podem ser chamadas de *nudges*. É necessário, ainda, visitar mais amplamente o panorama dos *nudges*, ou dessas práticas que influenciam as escolhas. E por fim, é preciso fazer considerações sobre boas práticas na criação das arquiteturas de escolhas.

2.7 *Dark patterns* e possível aplicação em *websites* e *apps*

Conforme Gray *et. al.* (2018, p. 1)*,* os *dark patterns* são usados para atender aos interesses de terceiros, e não aos interesses do próprio usuário; sequestram os interesses humanos em favor de objetivos maliciosos; na área de estudo de Interação Humano-Computador e *User Experience* (UX), os designers de interação aplicam tais padrões obscuros conjugando o conhecimento de comportamento humano com os interesses das pessoas, criando funcionalidades que enganam os usuários e não atendem aos interesses destes.

O conceito de *dark patterns* foi introduzido na década passada por Harry Brignull, na discussão sobre o design de interfaces de usuário em *websites* e aplicativos:

> Padrões de design enganosos (também conhecidos como *dark patterns*) são truques usados em *sites* e aplicativos que levam você a fazer coisas que não pretendia, como comprar ou se inscrever em algo. (BRIGNULL *et. al.*, 2023, tradução nossa).

Em 2010, Brignull catalogou uma série de *dark patterns*, criou um *website* e publicou o resultado do seu trabalho. Originalmente, o nome de domínio do *website* era ***darkpatterns.org***, porém posteriormente foi alterado para ***deceptive.design***, para indicar que são padrões enganosos. Brignull também criou uma escala em que as interfaces de usuários podem ser classificadas por nível de honestidade: de um lado, as interfaces honestas que respeitam os direitos das pessoas, passando pelas práticas intermediárias para aumentar as taxas de conversão de usuários em clientes, e chegando até os *dark patterns* que enganam os indivíduos em detrimento dos interesses de quem controla cria, controla e fornece a interface (BRIGNULL, 2011). Brignull criou uma lista com 12 categorias de *dark patterns* (BRIGNULL, 2023). Algumas das categorias que têm relação com esta pesquisa serão apresentadas como segue.

Trick Questions, ou Perguntas Capciosas: ocorre quando o indivíduo é induzido a dar uma resposta que não queria: "a pergunta parece pedir uma coisa, mas quando lida com cuidado, ela pede outra coisa completamente diferente" (BRIGNULL, 2023, tradução nossa). Este *dark pattern* pode ser usado numa frase com dupla negação sobre aceitar o uso de *cookies*, por exemplo: "não aceito que os *cookies* sejam desativados". Neste caso, o "não aceito" e o "desativados" usados em conjunto significam que o titular de dados aceita, sim.

Roach Motel, ou Motel Barato: "Você entra em uma situação com muita facilidade, mas depois descobre que é difícil sair dela", como no caso de alguma assinatura de serviço *online* (BRIGNULL, 2023, tradução nossa). A dificuldade de o titular dos dados retirar o consentimento por meio dos avisos de *cookies* é uma forma de aplicação deste *dark pattern*. A LGPD estabelece que o consentimento pode ser retirado da mesma forma que foi fornecido.

Privacy Zuckering: Segundo Brignull (2023, tradução nossa), "[v]ocê é levado a compartilhar publicamente mais informações sobre si mesmo do que realmente pretendia". Conforme o mesmo autor, o nome deste padrão foi cunhado em referência a Mark Zuckerberg, CEO da *big tech* Meta. Conforme Bösch *et. al.* (2016), este *dark pattern* foi apresentado por Jones (2010). A falta de informações claras e completas sobre

quais dados pessoais serão tratados engana o titular. Talvez seja o *dark pattern* mais popular, pois prescinde de interação com o usuário, uma vez que os *websites* em geral são programados para capturar os dados pessoais dos titulares independentemente de autorização ou consentimento.

Misdirection, ou Desorientação: "O *design* propositalmente concentra sua atenção em uma coisa para distrair sua atenção de outra" (BRIGNULL, 2023, tradução nossa). Salientar os botões de aceitação de *cookies* desfoca a atenção dos titulares de dados sobre a possibilidade de não fornecer o consentimento. Este é outro *dark pattern* muito utilizado, e pode ser empregado para legitimar a captura de dados pessoais por meio de *cookies* que já ocorreu mesmo antes do fornecimento do consentimento.

Bait and switch, ou "Isca e Troca": "Você se propõe a fazer uma coisa, mas uma coisa diferente e indesejável acontece em seu lugar" (BRIGNULL, 2023, tradução nossa). Se o usuário não aceitar os *cookies* e continuar navegando, mesmo assim os dados pessoais são capturados pelo *website*. Neste caso, a falta de fornecimento do consentimento funciona como se fosse a efetiva obtenção do consentimento. É comum, neste caso, que os *websites* apresentem uma mensagem do tipo "ao continuar navegando neste *site*, você aceita o uso de *cookies*" juntamente com um botão "Ok", ou ainda "este *website* usa *cookies*" e um botão "Ok". Neste caso, o usuário pode usar a heurística para simplesmente remover o aviso de *cookies* da sua tela, com a intenção de apenas ter mais espaço para interagir com o *website*, mas acaba aceitando o uso de *cookies* e fornecendo o consentimento. Trata-se da prática de consentimento tácito.

Confirmshaming: "O ato de culpar o usuário a optar por algo. A opção de recusar é redigida de forma a envergonhar o usuário a ponto de ele fazer o que se quer" (BRIGNULL, 2023, tradução nossa). Um exemplo de aplicação deste *dark pattern* é redigir uma mensagem dos avisos de *cookies* com algo assim: "Eu não aceito o uso de *cookies*, e estou ciente de que não poderei aproveitar as ofertas personalizadas deste *website*".

A Figura 1 apresenta os *dark patterns* identificados por Gray *et. al.* (2018) e suas relações com alguns dos padrões catalogados por Brignull *et. al.* (2023), assim como os outros padrões relacionados na figura anterior, todos derivados do trabalho *The Dark (Patterns) Side of UX Design* (GRAY et. al., 2018). Há diversas classificações de *dark patterns*, porém essa de autoria de Gray *et. al.* (2018) foi eleita para uso na presente pesquisa. Os próximos parágrafos descrevem e exemplificam tais padrões no contexto de avisos de *cookies*.

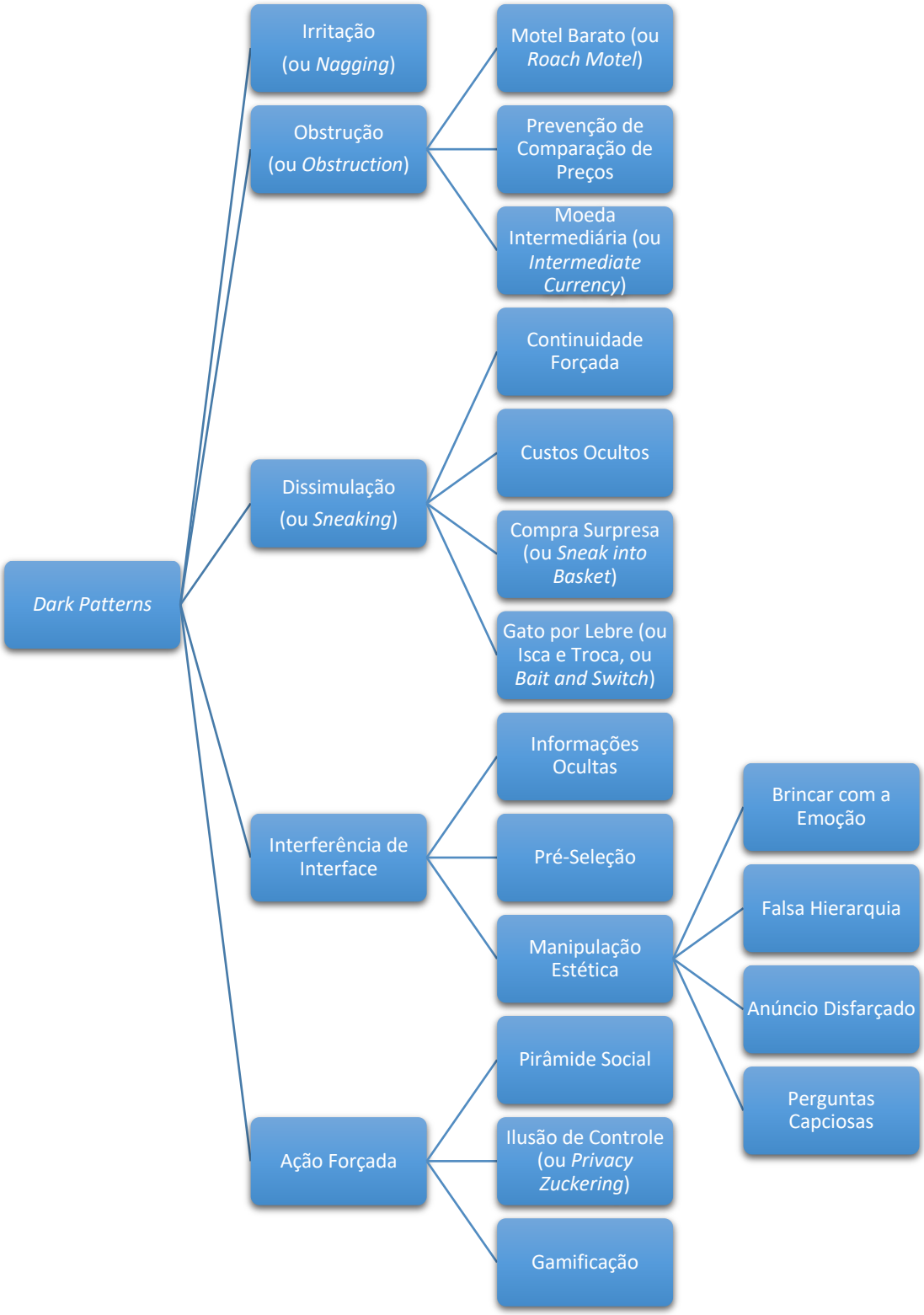


Figura 1: *Dark patterns* e relações com outros padrões de acordo com Gray *et. al.* (2018)
Fonte: elaborado pelo autor.

O objetivo do *dark pattern Nagging*, ou Irritação, de Gray *et. al.* (2018), é desfocar a ação do usuário da ação principal, causando fricção. Este padrão pode ocorrer quando anúncios de publicidade ficam sobrepostos ao conteúdo principal do *site*, bem como sobre os avisos de *cookies*. O exagero de anúncios é algo irritante e que tira a atenção do usuário, que pode deixar de interagir com o referido aviso.

O padrão Obstrução, de Gray *et. al.* (2018), transforma uma ação do usuário em algo mais difícil do que realmente deveria ser, criando dificuldades para certas situações. Este padrão se relaciona com o *dark pattern Roach Motel* – ou Motel Barato em português – e é um termo cunhado por Brignull *et. al.* (2023). No contexto desta pesquisa, este padrão pode acontecer se o usuário autorizar o uso dos *cookies*, e não conseguir posteriormente retirar o seu consentimento com a mesma facilidade de antes quando havia dado o aceite.

Dissimulação ou *Sneaking*, padrão também identificado por Gray *et. al.* (2018, tradução nossa), é outro tipo de *dark pattern*, e consiste na "tentativa de ocultar, disfarçar ou retardar a divulgação de informações que tenham relevância para o usuário". Este padrão se relaciona com outros conforme segue.

O *pattern* Continuidade Forçada (Brignull *et. al.*, 2023) é um tipo de Dissimulação (Gray *et. al.*, 2018). Nesta pesquisa, esse padrão ocorre quando os *cookies* de sessão são restaurados por meio da funcionalidade *session restore*, mantendo-se indefinidamente no navegador quando o usuário recupera a sessão anterior.

Propaganda Enganosa, ou "Isca e Troca" (*Bait and Switch*), que pode também ser associado à expressão "Gato por Lebre", é um padrão identificado por Brignull *et. al.* (2023), e é um tipo de padrão de Dissimulação (Gray *et. al.*, 2018). Na pesquisa, o padrão Gato por Lebre acontece quando o botão "Aceitar Todos os *Cookies*" é posicionado em um local normalmente usado para finalizar as ações, como por exemplo na parte inferior direita dos *banners* de segundo nível, enquanto o elemento que permite rejeitar todos os rastreadores não necessários não existe ou está posicionado na parte superior, ou ainda apenas no segundo nível do aviso de *cookies*.

O padrão de Dissimulação também pode ocorrer quando mensagens de cunho "positivo" são usadas nos avisos de *cookies*, ao invés de linguagem neutra, dissuadindo o usuário a realizar algo que não faria se tivesse acesso a mais informações de forma facilitada. Os resultados de pesquisas, como o desenvolvido por Kulyk *et. al.* (2018), sobre comportamento dos usuários, mostram que estes preferem não concordar em

compartilhar seus dados se souberem que o fornecedor do serviço do *website* se beneficiará com isso.

O *dark pattern* Interferência de Interface manipula a interface apresentada ao usuário de forma a influenciar o indivíduo a se comportar de determinada forma (Gray *et. al.*, 2018), e se relaciona com outros três padrões: Informações Ocultas, Pré-Seleção e Manipulação Estética.

Informações Ocultas é um tipo de Interferência de Interface (Gray *et. al*., 2018). Na pesquisa, este padrão acontece quando o acesso aos elementos gerenciais ou informativos que compõem certos *banners* é quase imperceptível, com letras bem menores do que os demais elementos, ou em posições desfavoráveis na interface. Também acontece quando o aviso de *cookies* como um todo não tem relevância alguma e é quase invisível ao usuário por conta dos demais componentes do *site*.

Pré-seleção é um tipo de Interferência de Interface (Gray *et. al.*, 2018). Neste trabalho, ele acontece quando os *cookies* não necessários estão pré-selecionados no *banner* de segundo nível.

Manipulação Estética é um tipo de Interferência de Interface (Gray *et. al.*, 2018), que se relaciona com os padrões: Brincar com a Emoção, Falsa Hierarquia e Perguntas Capciosas, conforme segue.

Brincar com a Emoção: é um tipo de Manipulação Estética, que por sua vez é um tipo de Interferência de Interface. Nesta pesquisa, ele pode ser identificado em algumas situações:

a. Quando é usado um botão verde para o elemento afirmativo de aceitação de rastreadores e um botão vermelho para a rejeição. As cores verde e vermelho têm um significado de “siga” e “pare”, e isso influencia a escolha.
b. Nos casos que os elementos afirmativos ficam com mais destaque e maiores, e os demais elementos permanecem sem destaque.
c. No emprego de mensagens com cunho negativo, segundo as quais o usuário poderá ser prejudicado na sua navegação caso não aceite as condições impostas no *banner*.

Falsa Hierarquia é um tipo de Manipulação Estética, que por sua vez é um tipo de Interferência de Interface assim como o padrão anterior. Na pesquisa, a falsa hierarquia se dá quando o botão com ação afirmativa fica destacado em relação aos demais elementos negativos, informativos e gerenciais.

Perguntas Capciosas é um tipo de Manipulação Estética, que por sua vez também é um tipo de Interferência de Interface. Na presente pesquisa, um exemplo é ter que ativar um elemento de seleção para desativar o uso de *cookies*, ou então uma mensagem com dupla negação, por exemplo "não aceito rejeitar os *cookies*".

Por fim, o padrão Ação Forçada é "qualquer situação em que os usuários são obrigados a realizar uma ação específica para acessar (ou continuar a acessar) uma funcionalidade específica" (Gray *et. al.*, 2018, tradução nossa). Ilusão de Controle, ou *Privacy Zuckering*: é um tipo de Ação Forçada, quando o usuário é obrigado a executar uma ação que fará com que compartilhe mais dados ou quando tem a falsa ideia de controle e que também o faz compartilhar mais dados.

A Ilusão de Controle ocorre quando, ao se deparar com *cookie walls*, o usuário é obrigado a aceitar os rastreadores pois não há opção para rejeitar. Também acontece quando o aviso de *cookies* mostra apenas a opção de aceitar o rastreamento.

Também ocorre a Ilusão de Controle ou *Privacy Zuckering* quando um *website* compartilha todos os *cookies* possíveis com terceiros, por meio da sincronização de *cookies*, ou *cookie syncing*, que são usados, dentre outras finalidades, também no escopo de *real-time bidding* (RTB). Ao acessar o *site*, os rastreadores são instalados no navegador do usuário inclusive antes de o aviso de *cookies* ser exibido. Mesmo tendo lido as informações do aviso de *cookies* ou não, quando o usuário clica no botão Aceitar, no botão Rejeitar, ou quando altera as preferências de rastreadores, os dados contidos nos identificadores de *cookies* já foram transmitidos a múltiplos domínios de terceiros "há muito tempo", durante o carregamento do *site*. O padrão ilude o indivíduo, pois a interação com o *banner* é apenas um "teatro", e relaciona-se com o paradoxo da privacidade, pois quanto mais o usuário do serviço *online* se sente no controle, mais ele tende a permitir o compartilhamento de seus dados (FORBRUKERRÅDET, 2018).

2.8 Elementos tecnológicos de apoio ao rastreamento *online*

Este capítulo apresenta ainda a especificação utilizadas pela indústria de tecnologia da informação para implementar sistemas no âmbito da *Internet*, o protocolo HTTP (*Hypertext Transfer Protocol*), contemplando uma visão geral da arquitetura organizacional e tecnológica que dá suporte aos *cookies* tais como tratados na presente pesquisa, trazendo aporte de conhecimento sobre o referido protocolo HTTP, a sua especificação técnica, explicando sobre o funcionamento do mecanismo de

gerenciamento do protocolo HTTP, razão pela qual os *cookies* foram criados, e também identificando propriedades e atributos destes componentes.

Esta seção traz subsídios sobre o funcionamento dos *cookies* segundo o protocolo HTTP, assim como apresenta classificações de *cookies* que são utilizadas na pesquisa empírica, e discorre sobre sistemas de gestão de consentimento – *consent management platforms*, ou CMPs.

2.8.1 Protocolo HTTP

O documento IETF[1] RFC[2] 2616 (FIELDING, 1999) especifica o protocolo HTTP versão 1.1, juntamente com RFCs mais recentes que o atualizaram. O HTTP é um protocolo, isto é, uma linguagem utilizada para comunicação entre programas de computador. O HTTP é um protocolo *stateless* (FIELDING, 1999, p. 1), isto é, não mantém o estado entre diferentes requisições e respostas trocadas entre os programas de computador que se comunicam. A falta de manutenção de estado entre diferentes requisições e respostas, na prática, impossibilita que um mesmo servidor possa diferenciar as requisições feitas por agentes distintos. Isto significa que, quando um *website* recebe solicitações de diferentes usuários A e B, o protocolo HTTP não é capaz de diferenciar quais solicitações vieram do usuário A e quais vieram do usuário B. No exemplo da Figura 2, o *website* de comércio eletrônico não consegue diferenciar se o comando para pagar o produto X é proveniente do navegador A ou do navegador B.

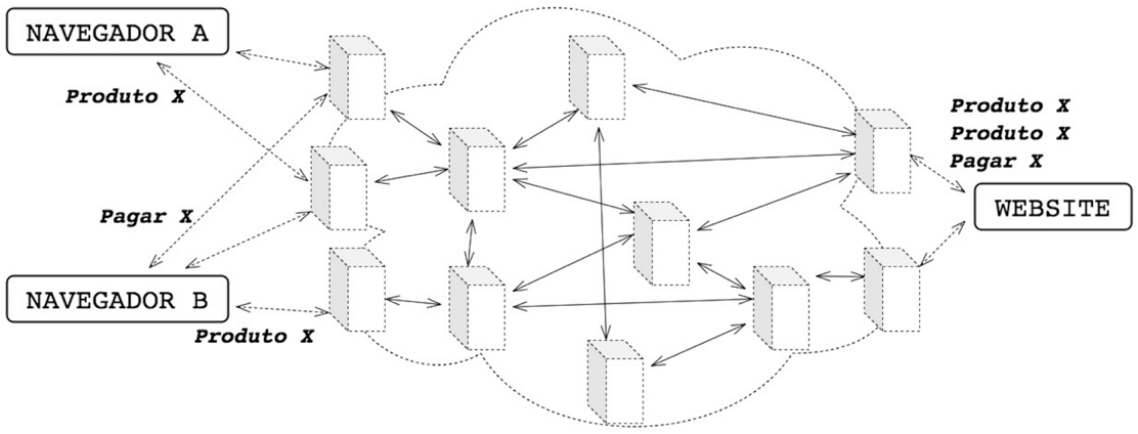


Figura 2: Funcionamento de protocolo HTTP *stateless*
Fonte: Elaborado pelo autor.

[1] *Internet Engineering Task Force.*
[2] *Request for Comments*.

2.8.2 Mecanismo de gerenciamento de estado HTTP

Como explicado anteriormente, o protocolo HTTP não mantém controle de estado. Para superar esta limitação, foi criado o mecanismo de gerenciamento de estado, que está documentado na RFC 6265. Este mecanismo de permite que aos servidores "manter uma sessão *stateful* sobre o protocolo *stateless* HTTP" (BARTH, 2011, p. 1, tradução livre). Esta solução permitiu a continuidade da adoção da tecnologia de comunicação e solucionar o problema encontrado de gerenciamento de sessão:

> Como o protocolo HTTP não mantém o estado entre duas requisições diferentes feitas pelo mesmo cliente ao mesmo servidor, então esta foi a solução inicialmente adotada para manter o estado conversacional entre dois programas de computador que entendem o protocolo HTTP. A RFC 6265 define dois campos de cabeçalho que devem ser usados pelo servidor e pelo cliente, respectivamente: Set-*Cookie* e *Cookie*. (BARTH, 2011, p. 3, tradução livre).

A RFC 6265 (BARTH, 2011) define o conceito de *cookie*. *Cookies* são representações dos estados de agentes de usuários – navegadores –, isto é, aglutinam o contexto de uma conversação complexa entre o navegador e o servidor. Os conteúdos dos estados desses agentes trafegam na rede por meio de campos de cabeçalho. O sistema de controle de sessão proposto pela RFC 6265 permite que o *website* identifique a origem da requisição que recebe, que é algo impossível sem tal mecanismo. Após receber a requisição do navegador, o *website* responde informando um identificador, que será o código que identificará unicamente aquele navegador, assim o *website* consegue saber de onde partiu a mensagem, e controlar uma transação, ou uma sessão com diversas requisições intermediárias, do início ao fim.

Na Figura 3, o *website* de comércio eletrônico recebe uma requisição do navegador A – controlado pelo usuário A – e devolve uma resposta com um identificador único “ID A”. Este “ID A” é o *cookie*, que tem nome “ID” e tem valor “A”. O navegador A envia o *cookie* “ID A” juntamente com o comando para o *website* colocar o produto X no carrinho de compras. O *website* recebe requisição similar do navegador B – controlado pelo usuário B – e devolve uma resposta com um identificador único, no caso “ID B”. Este “ID B” também é um *cookie*, que tem nome “ID” e tem valor “B”. O navegador B envia o *cookie* “ID B” juntamente com o comando para o *website* colocar o mesmo tipo de produto X no carrinho de compras. Neste momento, o *website* consegue controlar o estado de duas sessões distintas, dos usuários A e B, pois sabe que existe um

carrinho de compras com o produto X pertencente ao ID A, e que há outro carrinho de compras com outro produto X, só que pertencente ao ID B. Esta capacidade é viabilizada pelo *cookie* de nome ID, que tem valores A e B que identificam os respectivos usuários. Então, o usuário B emite um comando para pagar a compra do produto X, enviando o *cookie* "ID B" junto com o pedido. Então, o *website* identifica que o comando de finalização da compra partiu do usuário B, encontra o pedido correspondente a ele e finaliza a compra. Note-se que este controle da sessão de compra no exemplo do *website* de comércio eletrônico não seria possível no caso apresentado pela figura que ilustra o protocolo *stateless*, pois o controle do estado da sessão é viabilizado, aqui, pela comunicação dos *cookies* entre os navegadores e o *website*.

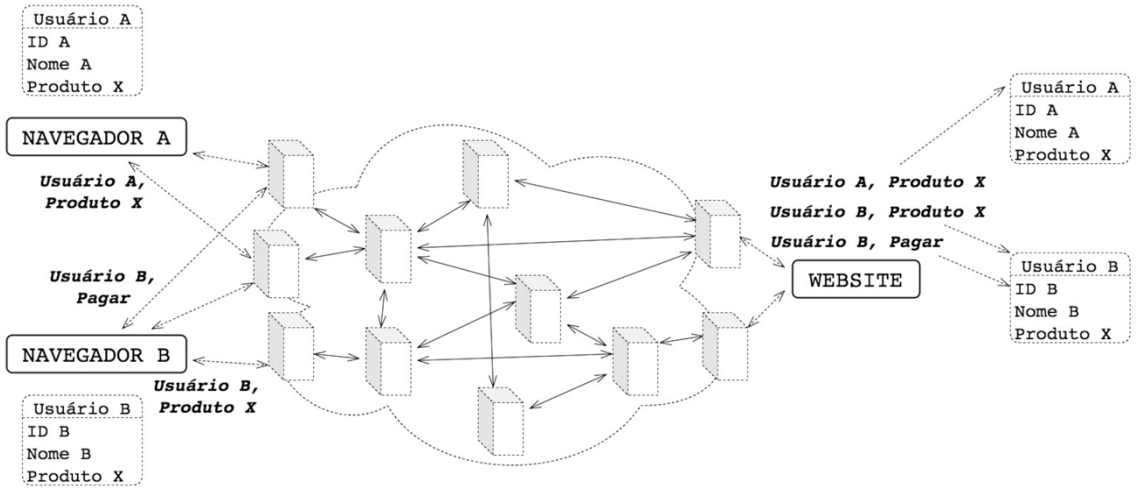


Figura 3: Funcionamento de protocolo HTTP *stateful*
Fonte: Elaborado pelo autor

2.8.3 Classificação dos *cookies*

Dentre diversos critérios, os *cookies* ou rastreadores podem ser classificados quanto à origem[3] – primários ou de terceiros –, quanto à sessão[4] –de sessão ou persistentes

[3] É possível identificar os *cookies* como primários ou de terceiros por causa do nome do domínio ao qual pertencem. Os *cookies* primários são aqueles que têm o mesmo nome de domínio do *website* que está sendo visitado pelo usuário. Os *cookies* de terceiros, por sua vez, têm nome de domínio de outro *website*. Os *cookies* que controlam as sessões dos usuários são, por excelência, exemplos de *cookies* primários. Os *cookies* de terceiros têm origem naqueles *website*s que incluem componentes vindos de outros *sites*. O exemplo típico de *cookie* de terceiro é aquele que é instalado no computador do usuário por um banner de publicidade.

[4] Os *cookies* têm diversos atributos, e um deles indica se o *cookie* é de sessão ou não. Por padrão, os *cookies* de sessão são eliminados quando o navegador é fechado, isto é, eles são programados para durarem apenas durante aquela sessão de uso do navegador. Nos *cookies* persistentes, por sua vez, o atributo que indica se é *cookie* de sessão vem com valor "falso", indicando que não é de sessão. Ora, se não é de sessão, é

–, quanto à lei – estritamente necessários e não necessários –, quanto à categoria – estritamente necessários, de desempenho ou analíticos, funcionais e de publicidade. Não há uma padronização ampla sobre isto, apesar de ser possível inferir algumas categorias, conforme demonstrado a seguir.

2.8.3.1 Classificação quanto à lei: estritamente necessários e não necessários (ou opcionais)

A GDPR define que os *cookies* estritamente necessários ao funcionamento adequado dos *websites* podem ser utilizados com base no legítimo interesse do fornecedor do *website*, e que os demais *cookies* devem ser empregados se e somente se houver autorização prévia dos usuários mediante o fornecimento de consentimento ativo. A LGPD não faz referência direta aos *cookies*, porém é possível interpretar que os *websites* que dependem de *cookies* para exercer suas funções de forma legítima, correta e adequada podem usá-los com base no legítimo interesse, da mesma forma que a GDPR. Todavia, é de se lembrar que a Lei Geral de Proteção de Dados prevê diversas outras hipóteses que autorizam o tratamento de dados pessoais. Apesar disto, o raciocínio binário entre consentimento e legítimo interesse pode ser aplicado para os demais *cookies*, todos opcionais, ou não necessários: se não tiverem o propósito de contribuir para o bom funcionamento do *website*, se tiverem propósito diverso daquele para o qual o *website* deve ser utilizado de forma precípua, o *website* deve primeiro obter o consentimento do usuário, por meio de *opt-in*, para que então possa armazenar e acessar tais *cookies* no dispositivo respectivo.

Tanto no caso dos *cookies* estritamente necessários quanto no caso dos *cookies* opcionais, contudo, o *website* tem o dever de informação, de prestar serviço com transparência aos seus usuários, informando ao titular de dados de forma ativa, clara, ostensiva e adequada sobre os detalhes do tratamento de dados realizado.

Recentemente, em 2022, a ANPD publicou o Guia orientativo sobre *cookies* e proteção de dados pessoais. Este guia traz divide os *cookies* em duas naturezas conforme a base legal: necessários e não necessários. O emprego dos necessários pode se basear no legítimo interesse, tal como o raciocínio elaborado supra, e os não necessários podem ser usados com a autorização por meio do consentimento do titular de dados. O guia

---

persistente. Os *cookies* persistentes só são removidos pelo navegador quando expirar a data de validade indicada neles.

classifica, ainda, em quatro tipos quanto à finalidade específica de cada um: necessários, funcionais, analíticos e de publicidade. Os necessários são aqueles indispensáveis ao funcionamento apropriado do *site*, tais como os *cookies* de sessão. Os funcionais são aqueles cuja existência pode ser essencial ou não ao funcionamento do serviço. Os analíticos são utilizados para medir o desempenho do *website* e formar estatísticas sobre o perfil dos visitantes. E os de publicidade são aqueles cujo objetivo é participar do sistema de marketing digital. Note-se que, conforme o referido guia, os *cookies* funcionais podem ser baseados tanto no legítimo interesse quanto no consentimento, à medida que sua razão de existir seja essencial ou não ao serviço (BRASIL, 2022d, p. 10)

2.8.3.2 Classificação quanto à categoria: estritamente necessários, de desempenho ou analíticos, funcionais e de publicidade

A Câmara Internacional de Comércio do Reino Unido (ICC UK, ou *International Chamber of Commerce*) criou, há vários anos, uma classificação de *cookies* muito utilizada pelo mercado de tecnologia, que por sua vez fornece componentes de *software* para gestão do consentimento. Esta classificação é compatível com a classificação dos *cookies* quanto à lei, e tem quatro categorias: *cookies* estritamente necessários, *cookies* de desempenho, *cookies* funcionais e *cookies* de publicidade. Esta é a classificação também adotada no Guia orientativo sobre *cookies* e proteção de dados pessoais publicado pela ANPD, como já apresentado.

Os *cookies* estritamente necessários são aqueles cujo armazenamento e leitura são obrigatórios, isto é, sem o seu emprego pelos *websites* nos dispositivos dos usuários é impossível fornecer o serviço de maneira adequada. Estes *cookies* estritamente necessários são aplicados pelos *websites* nos equipamentos dos usuários de forma automática, e não dependem de autorização prévia do titular dos dados para o seu uso.

Os *cookies* de desempenho ou analíticos são utilizados pelos *websites* para analisar quais páginas os usuários utilizam e eventuais erros que podem ocorrer nessas páginas. Estes *cookies* não identificam os usuários, podem ser anonimizados e são utilizados com propósitos de melhoria do *website*. Também são conhecidos como *cookies* de análise, ou ainda *web analytics*, e também podem ser usados para controlar a interação dos usuários com quaisquer componentes do *website* (ICC, 2012, p. 8).

Os *cookies* funcionais têm o propósito de melhorar a experiência do usuário no *website*. Eles podem armazenar valores que o próprio usuário define, para customizar o

ambiente *online*. Por exemplo, os *cookies* funcionais podem armazenar o nome do usuário, as suas preferências de configurações personalizadas para o *website*, e outros valores com o mesmo fim. Os *cookies* funcionais, como o próprio nome diz, exercem uma funcionalidade no *website*, que é relacionada com a própria atividade do *website*, mas que não necessariamente precise ser executada para que o *website* funcione corretamente. Estes *cookies* também podem ser anonimizados, não identificam os usuários e não podem rastrear as atividades dos visitantes. Tais *cookies* podem ser utilizados para guardar as preferências pessoais dos usuários, como o a cidade, o tamanho do texto, o nome de usuário, as cores e outros atributos, conforme o *website*. Neste exemplo, os dados de localização e o nome do usuário não podem ser usados para fins publicitários (ICC, 2012, p. 9). Se assim, forem, então o *cookie* deveria pertencer às duas categorias concomitantemente, ou seja, seria um *cookie* funcional e de publicidade.

Por fim, a última categoria é a dos *cookies* de publicidade. Estes *cookies* são usados para exibir anúncios publicitários, e servem também para controlar o número de "impressões" de cada anúncio, pois a indústria do marketing digital vende os espaços publicitários controlando a quantidade de vezes que um anúncio é exibido no *website* (ICC, 2012, p. 9). Os *websites* disponibilizam espaços de anúncios publicitários, e terceiros "compram" esses espaços por meio de leilões em tempo real – *real time bidding*. Os terceiros, por sua vez, remuneram os *websites* de acordo com métricas pré-definidas: se o usuário apenas visualizou o anúncio, se visualizou e clicou no anúncio, ou ainda se visualizou, clicou e adquiriu algo relacionado ao anúncio. Os *cookies* de publicidade são, em sua maioria, *cookies* de terceiros, pelos motivos aqui apresentados, e isto será demonstrado nos resultados da pesquisa empírica.

2.8.4 *Consent Management Platforms* (CMPs)

CMPs são sistemas de gestão de consentimento, que permitem que o controlador de dados gerencie os registros de consentimento dos indivíduos de forma organizada. Os CMPs surgiram no contexto da União Europeia, com base na iniciativa de autorregulação promovida pela IAB Europe (*Interactive Advertising Bureau Europe*), denominada TCF (*Transparency and Consent Framework*). O IAB Europe é uma organização privada organizada pelos participantes da indústria de *marketing*. O TCF, por seu turno, é composto por diversas especificações técnicas com o objetivo de padronizar as práticas de transparência e gestão do consentimento. Com o advento da GDPR (Regulamento

Europeu de Proteção de Dados), diversos produtos de *software* de gestão de consentimento começaram a ser produzidos com base nas especificações técnicas publicadas pela IAB, e a comercialização desses produtos ganhou escala mundial, atingindo também o Brasil, muito devido à introdução do normativo legal de proteção de dados brasileiro.

Em decisão de fevereiro de 2022, a autoridade de proteção de dados da Bélgica decidiu que o IAB Europe deveria ser considerado como controlador de dados, em conjunto (co-controlador) com os demais participantes do sistema de gestão de consentimento com finalidade de *marketing* digital. Os demais *joint controllers* que participam da operação do TCF são os anunciantes interessados em veicular publicidade e as *adtechs*, empresas que organizam quais anúncios devem ser vinculados para quais indivíduos, por meio de RTB (*Real Time Bidding*) que são leilões em tempo real para determinar os anúncios vencedores da disputa e que serão exibidos para certo usuário que usa um *website* ou outro tipo de recurso, como aplicativo de *smartphone*. Como o TCF é composto de uma *string*, chamada de *TC String* (*Transparency and Consent String*), que nada mais é do que um identificador único, a autoridade de proteção de dados belga entendeu que a *TC String* deveria ser considerada como dado pessoal, pois teria o potencial de identificar unicamente o usuário na *Internet*. Dentre outros motivos como falta de transparência, e também por entender que não há base legal adequada para emprego da *TC String*, a autoridade belga aplicou multa de 250 mil euros na IAB Europe. Sem decisão transitada em julgado, atualmente este caso está em sede de apelação na segunda instância belga, porém o processo foi suspenso no aguardo de decisão do Tribunal de Justiça da União Europeia (TJUE) sobre o caso (IAPP, 2022).

3 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Uma das primeiras menções feitas ao direito à privacidade surgiu no artigo científico muito conhecido de autoria de Samuel D. Warren e Louis D. Brandeis em 1890. Para tais autores, o direito à privacidade foi concebido com base em um "direito a ser deixado só", ou *right to be let alone*, muito relacionado ao incômodo sentido pelas pessoas devido à divulgação de fotografias pessoais e reprodução de imagens e sons, acelerado pelo crescente uso de máquinas de fotografia e aumento da atividade da imprensa (DONEDA, 2019, p. 30).

A partir da década de 1960, diversos fatores contribuíram para o fortalecimento da relação entre os dados pessoais e o direito à privacidade, dentre eles a atuação do Estado, o reconhecimento de direitos trabalhistas e o aumento do fluxo de informações (DONEDA, 2019, p. 33).

A proteção dos dados pessoais pode ser utilizada como um meio para garantir a privacidade (DONEDA, 2019, p. 173). Assim, a evolução histórica do conceito de privacidade proporcionou a emergência do direito à proteção dos dados pessoais.

As primeiras leis sobre proteção de dados pessoais surgiram na Alemanha, e foi lá também que, nos primeiros anos da década de 1980, o tratamento de dados pessoais pelo Estado foi questionado judicialmente: a organização do censo alemão previa a aplicação de perguntas aos cidadãos germânicos e o posterior processamento de dados por meio de computador (DONEDA, 2019, p. 165), suscitando dúvidas na sociedade sobre possibilidade de criação de riscos à proteção dos dados pessoais.

Há uma categorização de gerações de leis sobre proteção de dados, sendo a primeira geração marcada pelo controle dos bancos de dados por meio de autorização do Estado; com a popularização dos computadores, a segunda geração transferiu a responsabilidade desse controle para o próprio cidadão, por meio do consentimento; a terceira geração de leis deu ao titular o controle amplo sobre o tratamento de dados pessoais, introduzindo o conceito de autodeterminação informativa como será visto adiante; e a quarta geração de leis incluiu autoridades independentes de proteção de dados e outras ideias, de forma a diminuir a dependência do consentimento, que marcou fortemente a geração anterior (BIONI, 2019, pp. 114-117).

Quanto à lei do censo alemão, que a doutrina identifica como sendo um marco da terceira geração de leis (BIONI, 2019, p. 116), além de declarar a inconstitucionalidade de alguns dispositivos lei, a Corte Constitucional alemã reconheceu a importância de

todos os tipos de dados pessoais, tomados individualmente ou de forma conjunta, e reconheceu o direito à autodeterminação informativa (DONEDA, 2019, pp. 166-168).

O reconhecimento constitucional deste direito, que aconteceu pela primeira vez com o Tribunal Constitucional Alemão em 1983 (MENDES, 2020, p. 2), se deu frente à falta de transparência do tratamento de dados pessoais e ao princípio da dignidade da pessoa humana (MENDES, 2020, p. 10), sendo que tal sentença decidiu que o titular de dados pessoais teria o direito a decidir sobre os aspectos de tratamento de dados realizado por terceiros – o Governo alemão, no caso. Assim, a Corte alemã entendeu que, se o dado é pessoal, ele demanda proteção, independentemente de ser da esfera privada ou íntima da pessoa (MENDES, 2020, p. 12). É possível afirmar, então, que o reconhecimento do direito à autodeterminação informativa veio a fortalecer o direito à proteção dos dados pessoais.

A Constituição Federal de 1988 dispõe, no artigo 5º, que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988). A Carta Constitucional, ao se referir à inviolabilidade da intimidade e da vida privada, consagrou a proteção constitucional do direito à privacidade (DONEDA, 2019, p. 261).

No Brasil, em 2022, a Emenda Constitucional 115 incluiu no rol de direitos fundamentais "a proteção dos dados pessoais, inclusive nos meios digitais" (BRASIL, 1988). Tal reconhecimento como direito fundamental no inciso LXXIX do artigo *5º* da Carta Magna demonstra a direção que o legislador constitucional quis indicar em busca da promoção da privacidade que é, por fim, assegurado por meio da proteção de dados pessoais.

A Lei Geral de Proteção de Dados (LGPD), Lei Federal 13.709, foi publicada em 2018, mas entrou em vigor no Brasil em 2020 "com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018).

A autodeterminação informativa é um dos fundamentos desta lei, conforme o artigo *2º*, inciso II, e assim é de se notar que o legislador brasileiro adotou aquele mesmo direito que havia sido reconhecido na Alemanha na década de 1980. A Lei Geral de Proteção de Dados brasileira, aliás, segue em grande parte o direito positivado no Regulamento Geral de Proteção de Dados europeu. No artigo *7º*, a LGPD assegura ao titular de dados pessoais que ele "tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e

ostensiva" (BRASIL, 2018). Este é um dos exemplos de aplicação da autodeterminação informativa, além do direito ao consentimento do artigo *7º*, inciso I.

O Marco Civil da *Internet* (MCI), Lei Federal 12.965/2014, estabeleceu "princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil" (BRASIL, 2014), definindo, dentre outros, os princípios da proteção da privacidade e da proteção dos dados pessoais no seu artigo 3º (DONEDA *et. al.,* 2021). A autodeterminação informativa foi uma das diretrizes que também orientou esta lei (BIONI, 2019, p. 132) no seu artigo *7º*, pois dentre os seus incisos o cidadão possui os direitos de "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de *Internet*, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei", "informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais", assim como de "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais", e ainda de "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de *Internet*, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros" (BRASIL, 2014).

Uma das características da Lei Geral de Proteção de Dados é a de ser uma lei principiológica. Ela traz consigo princípios que devem ser observados do tratamento de dados. Estes princípios derivam em parte do rol de princípios divulgado em 1973 pelo Departamento de Saúde dos Estados Unidos (DONEDA, 2019, p. 180). Durante os anos de 1980, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) publicou diretrizes sobre proteção de dados a serem seguidas pelos países-membros que também elencavam princípios, conhecidos também como *Fair Information Privacy Principles*, ou simplesmente FIPPs (BIONI, 2019, pp. 119-120).

Além da boa-fé, a LGPD elencou os princípios acima mencionados e outros, formando no total um rol de dez princípios que devem ser atendidos pelos agentes de tratamento de dados: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, e responsabilização e prestação de contas.

O princípio da boa fé informa o dever de agir com honestidade e respeito aos valores éticos e morais da sociedade, e é o princípio que transita entre todos os demais aqui descritos. A aplicação do princípio da boa fé atrai o princípio da confiança (MORAIS, 2021, Cap. 6), que é fundamental para as relações jurídicas entre as partes. A

boa fé é um conceito jurídico indeterminado, que deve ser aplicada em todas as relações – porquanto é um dever geral de conduta – e avaliada casuisticamente, e da qual originam-se deveres derivados tais como os elencados por Caio Mário da Silva Pereira: “dever de correção, de cuidado e segurança, de informação, de cooperação, de sigilo, de prestar contas” (PEREIRA, 2022), na busca da satisfação dos interesses das partes.

Tal lei definiu o princípio da finalidade como a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (BRASIL, 2018). Os dados pessoais devem ser tratados unicamente para atingir os fins que foram predeterminados. O agente de tratamento de dados pessoais somente é autorizado a realizar o tratamento para atingir os resultados esperados pela finalidade informada. Há que se ter respeito pela correlação entre a finalidade, que é informada ao titular de dados pessoais, e o tratamento que se pretende realizar (TEPEDINO *et. al.,* 2019, p. 73). Este princípio pode ser utilizado como ferramenta argumentativa para que o titular de dados se oponha a determinado tipo de tratamento, como por exemplo certa transferência de dados ou ainda armazenamento de dados por um longo período, permitindo também a concepção de critérios para identificar se determinado tratamento de dados é abusivo ou não (DONEDA, 2019, p. 182). Há que se frisar que os propósitos da finalidade devem atender aos requisitos da lei: legítimos, específicos, explícitos e informados ao titular (BRASIL, 2018), ou seja, a finalidade deve ser legal, deve estar bem definida, deve estar clara e deve ser informada ao titular.

A LGPD também definiu o princípio da adequação como a "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" (BRASIL, 2018). Os tipos de tratamento devem guardar coerência com as finalidades que se pretende atingir, para que não ocorra desvio de finalidade. O princípio da adequação orienta que as formas de tratamento a serem realizadas nos dados pessoais sejam necessárias e suficientes para o alcance da finalidade informada.

O princípio da necessidade foi tratado na LGPD como a "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" (BRASIL, 2018). Somente aqueles dados estritamente necessários devem ser tratados, reduzindo assim eventuais riscos. Além da restrição de dados para tratamento com vistas a atingir determinada finalidade, o princípio da necessidade também orienta que os dados sejam eliminados ao fim do tratamento ou a pedido do titular (TEPEDINO

et. al., 2019, p. 75). O princípio da necessidade também pode ser entendido como princípio da proporcionalidade, sendo que fundamenta o conceito de minimização de dados (BIONI, 2019, p. 123).

Já o princípio do livre acesso para a mesma lei é a "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" (BRASIL, 2018). Os titulares de dados pessoais têm o direito de saber quais são os dados que estão sendo tratados, a forma de tratamento e por quanto tempo serão tratados. Este princípio indica prerrogativas dos titulares sobre requisições que pode m ser feitas aos agentes de tratamento (TEPEDINO *et. al.,* 2019, pp. 75-76). O princípio do livre acesso permite que o titular acesse bancos de dados com seus dados pessoais, obtenha cópias dos seus dados, efetivamente controle seus dados, possa corrigi-los e também eliminá-los se for o caso (DONEDA, 2019, p. 182).

A qualidade dos dados, como princípio da Lei Geral de Proteção de Dados, é a "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" (BRASIL, 2018). Para que a almejada finalidade seja atingida, os titulares de dados pessoais têm o direito de assegurar que os seus dados estão corretos, estão atualizados e íntegros. O resultado assertivo obtido pelo tratamento dos dados pessoais atenderá à finalidade se os dados apresentarem boa qualidade. O princípio da qualidade dos dados tem relação com o princípio do livre acesso e com o princípio da transparência, pois estes informam sobre o tratamento e permitem a retificação de dados para garantir a qualidade (TEPEDINO *et. al.,* 2019, p. 76). O princípio da exatidão é outro nome dado ao princípio da qualidade, segundo o qual os dados pessoais tratados devem refletir a realidade (DONEDA, 2019, p. 182).

O princípio da transparência na LGPD é a "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" (BRASIL, 2018). Os titulares de dados pessoais têm o direito de serem informados sobre as possibilidades de tratamento de seus dados pessoais, e também sobre quais são os agentes de tratamento, sejam controladores, co-controladores ou operadores de dados pessoais. O princípio da transparência aplica-se ao longo de toda a cadeia de tratamento, desde a coleta ou obtenção, até a eliminação dos dados pessoais (TEPEDINO *et. al.,* 2019, p. 76). Este princípio também é conhecido como princípio da publicidade, sobre a divulgação pública da existência de bancos de dados pessoais (DONEDA, 2019, p. 181).

A Lei de Acesso à Informação, Lei Federal 12527/2011, define normas especializadas para a divulgação de informações pelo Poder Público, também para o atendimento do princípio da transparência com reconhecimento da necessidade de proteção de dados pessoais (DONEDA *et. al.,* 2021). É importante notar que a acepção do princípio da transparência, para esta lei, é no sentido de viabilizar o controle social das contas públicas, enquanto que o princípio da transparência presente na LGPD tem a finalidade de informar o titular sobre o tratamento dispensado a seus dados. O Supremo Tribunal Federal atuou no julgamento de um processo que discutia qual seria a prevalência entre o direito do cidadão sobre dados geridos pelo poder público e o direito à privacidade dos servidores públicos sobre suas informações de remuneração. A disputa confrontou o direito à privacidade e a Lei de Acesso à Informação, e ao final a decisão entendeu pela legitimidade da divulgação dos dados remuneratórios dos servidores públicos, com nome e número do cadastro de pessoa física (CPF) parcialmente mascarado (DONEDA *et. al.* 2021). Tal caso contrasta com a recente decisão administrativa exarada por meio da Nota Técnica no. 46/2022/CGF/ANPD, da Autoridade Nacional de Proteção de Dados, que ordenou suspender publicação de dados do censo escolar e do ENEM pelo INEP "e a posterior publicação da Nota de Esclarecimento INEP (SEI n° 3289150) no sítio eletrônico do instituto" (BRASIL, 2022b). Neste caso administrativo, estudo realizado pelo Laboratório Inscrypt do Departamento de Ciência da Computação da Universidade Federal de Minas Gerais identificou que existe "risco potencial de identificação das pessoas a quem os dados estatísticos se referem" (BRASIL, 2022b), pelo cruzamento de microdados publicamente disponibilizados, porquanto a mesma espécie de vulnerabilidade deste caso do INEP existe para o caso supramencionado julgado pelo STF.

A transparência sobre o tratamento das informações dos indivíduos é um meio utilizado para proteger os cidadãos, inclusive por parte de ações estatais que possam ameaçar as liberdades individuais (DONEDA *et. al.,* 2021). As leis sobre proteção de dados privilegiam o princípio da transparência numa lógica de análise de risco e *accountability* com o objetivo de diminuir a probabilidade de impacto sobre os direitos individuais (DONEDA *et. al.,* 2021).

Conforme a LGPD, o princípio da segurança é a "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" (BRASIL, 2018). Este princípio tem o objetivo de garantir a confidencialidade, a

integridade e a disponibilidade dos dados, além da autenticidade nos casos em que for necessária, por meio do emprego de ferramentas, adoção de medidas tecnológicas ou organizacionais. O princípio da segurança também tem o objetivo de evitar a existência de situações ilegais (TEPEDINO *et. al.,* 2019, p. 77). Este princípio também é referido como princípio da segurança física e lógica, e deve ser adotado para evitar ou minimizar os riscos de incidentes que os afetem (DONEDA, 2019, p. 182).

A mesma lei define o princípio da prevenção como a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" (BRASIL, 2018). As medidas técnicas ou administrativas devem ser adotadas para evitar que os incidentes ocorram, de forma proativa, diminuindo a probabilidade e o impacto, e assim mitigando o risco de ocorrência de tais incidentes.

A LGPD traz o princípio da discriminação da seguinte forma: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos (BRASIL, 2018). A lei veda que os dados pessoais sejam tratados de forma diferente sem respeitar a isonomia e a equidade. O tratamento de dados, principalmente dos dados sensíveis, não deve ser usado para diferenciar ilegalmente pessoas por raça, cor, religião ou qualquer outro atributo (TEPEDINO *et. al.,* 2019, p. 79).

Por fim, o princípio da responsabilização e prestação de contas na LGPD é a "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). As sucessivas gerações de leis de proteção de dados trouxeram novos componentes de prestação de contas, ou *accountability*, para demonstrar a observância das normas legais. O princípio da responsabilização e prestação de contas, relacionado ao termo *accountability*, serve para garantir que o agente de tratamento de dados pessoais demonstre que efetivamente adota práticas que protegem os dados pessoais. Tal princípio também informa que as medidas adotadas pelos agentes de tratamento de dados pessoais devem estar adequadas às necessidades de proteção respectivas, de modo a garantir a sua eficácia.

A Lei Geral de Proteção de Dados define as hipóteses de tratamento de dados pessoais no artigo *7º* e no artigo 11 para dados pessoais sensíveis. Ou seja, a lei autoriza o tratamento de dados pessoais por parte dos agentes de tratamento nos casos previstos em lei. São dez as situações que permitem o tratamento de dados: consentimento do titular, para atender a lei ou regulamento, na execução de políticas públicas pela administração pública, nas investigações científicas por órgão de pesquisa, para executar

contratos ou seus atos preparatórios, no exercício regular de direitos em processos judiciais ou extrajudiciais, para proteger o bem da vida ou a integridade física, para garantir a saúde em procedimentos relacionados, no legítimo interesse do controlador ou de terceiro, e na proteção do crédito (BRASIL, 2018). Para este estudo, as hipóteses de tratamento de dados pessoais mais relevantes são o consentimento do titular e o legítimo interesse do controlador ou terceiro.

O consentimento, como hipótese de tratamento de dados pessoais, foi inicialmente caracterizado como livre, informado, inequívoco e específico pela Diretiva Europeia de Proteção de Dados Pessoais 95/46/EC, classificada como sendo da quarta geração de leis, na tentativa de efetivar o controle dos dados pessoais pelo seu titular (BIONI, 2019. pp. 122-124), e que foi posteriormente substituída pela GDPR. Apesar de ter sido considerado como a única hipótese de tratamento de dados durante o período de gestação do anteprojeto da LGPD, ele está posicionado topologicamente no mesmo nível das demais hipóteses (BIONI, 2019, p. 133). Para Bruno Bioni (2019, pp. 134-135), apesar de haver outras bases legais de tratamento de dados pessoais, o consentimento ainda tem o papel de protagonista na lei brasileira por várias razões, dentre elas a centralização dos princípios e o reforço dos mecanismos de controle para o titular de dados, a conhecida adjetivação do consentimento, que o caracteriza conforme já mencionado. Na lei brasileira de proteção de dados, o consentimento deve ser livre, informado e inequívoco, e específico para o tratamento de dados pessoais sensíveis. Deve ser livre porque não compulsório, deve ser apresentado àquele que consente, inequívoco porque deve ser claro e não ambíguo, e específico, nos casos necessários, para que seja destacado de outras cláusulas.

3.1 O princípio da transparência na lei geral de proteção de dados

Este tópico foi desenvolvido com a finalidade de identificar elementos que formam a transparência para a proteção de dados no escopo deste trabalho. Para este mister, a análise dos elementos de transparência foi realizada à luz da doutrina nacional da diretriz sobre transparência criada pelo Grupo de Trabalho do Artigo 29 do Conselho Europeu e da Resolução CD/ANPD no. 2 de 2022.

O Grupo de Trabalho do Artigo 29, também conhecido pela sigla WP29, foi um comitê estabelecido no âmbito da União Europeia que tinha fins consultivos, e que existiu até 25 de maio de 2018, quando iniciou a vigência da GDPR (UNIÃO EUROPEIA, 2022).

Atualmente, o *European Data Protection Board* (EDPB) é o substituto do WP29. Este grupo de trabalho elaborou uma diretriz chamada de *Guidelines on transparency under Regulation 2016/679*, com o objetivo de servir de orientação e de suporte à interpretação sobre o princípio da transparência da GDPR (UNIÃO EUROPEIA, 2017, p. 4).

3.1.1 Elementos gerais de transparência

A Lei Geral de Proteção de Dados faz menção à transparência em 5 pontos do seu texto: artigo *6º*, inciso VI, artigo *9º*, § 1º, artigo 10, § 2º, artigo 40 e artigo 50, § 2º, inciso I, alínea e (BRASIL, 2018).

No artigo *6º*, inciso VI, a lei define transparência como a "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" (BRASIL, 2018). Inicialmente, cumpre destacar que a leitura completa que leva ao princípio da transparência na LGPD deve começar pelo *caput*, que afirma que "[a]s atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios", e então seguir com o princípio da transparência (BRASIL, 2018).

A transparência é uma garantia, como o próprio texto apresenta, de que as informações sejam entregues com clareza, precisão e fácil acessibilidade quanto a quais atividades de tratamento de dados são realizadas e sobre quem as executa (BRASIL, 2018). Esta parte do texto em diante tem o objetivo de localizar na lei quais são os elementos de transparência que servem para o cumprimento do dever de informar o titular sobre o tratamento de dados realizado pelo controlador, com a identificação do elemento legal e então a análise do respectivo item.

3.1.1.1 Clareza

O primeiro elemento de transparência identificado na lei geral de proteção de dados é a característica de **clareza** presente no artigo 6º, inciso VI (BRASIL, 2018). A clareza contribui para a facilidade de interpretação. Para o tratamento de dados ser considerado transparente, a informação apresentada sobre o tratamento deve ser clara, isto é, não deve suscitar dúvidas naquele que a lê, deve evitar obscuridades por usar termos desconhecidos ou pouco conhecidos (UNIÃO EUROPEIA, 2017, p. 7). O requisito da clareza requer que a comunicação seja realizada em linguagem simples, sem

rebuscamentos desnecessários, sem utilizar expressões complexas, nem jargões técnicos demais (UNIÃO EUROPEIA, 2017, p. 8). Em outras palavras, a clareza impõe que o texto seja inteligível pelo homem médio de maneira rápida e simples, e que até aquela pessoa mais simples e desprovida de maior acesso a cultura ou educação formal tenha condições de entender a mensagem que estiver sendo comunicada a ela (UNIÃO EUROPEIA, 2017, p. 7). Ou seja, aquele que formula a mensagem no intuito de atender ao princípio da transparência precisa usar a razoabilidade na sua atividade, com a empatia necessária para entender que os destinatários apresentam diversos perfis, cada um com as suas características específicas de receptores da comunicação, com maior ou menor facilidade de compreensão daquilo que lhes é transmitido.

A clareza também pode compreender o uso de signos, formas, formatos, símbolos, desenhos ou quaisquer outros elementos gráficos, sonoros ou táteis que sejam adequados para que a comunicação aconteça com sucesso. Os componentes gráficos devem empregar ícones e sinais comuns, de fácil compreensão, e que sejam usados comumente, ou padronizados, permitindo o entendimento sem criar dúvidas (UNIÃO EUROPEIA, 2017, p. 25); os ícones devem ser "algo que se parece com aquilo que significa" (GALITZ, 2007, p. 653). Toda comunicação envolve um emissor, um receptor, um canal de transmissão, a linguagem de codificação e os ruídos, conforme o sistema de comunicação de informação proposto por Shannon (CARISSIMI ; GRANVILLE; ROCHOL, 2009, p. 24). Mensagens claras são comunicadas na linguagem compreendida pelo receptor. Sendo assim, a essência da mensagem até pode ter sido elaborada em uma linguagem distinta; contudo, se a mensagem for processada para então ser transmitida no formato que o interlocutor entende, então a mensagem tem clareza. A informação clara também é transparente quando há pouca ou nenhuma interferência no canal de comunicação por meio do qual trafega, de forma que a mensagem seja apresentada com integridade. Assim, a informação clara encurta o caminho do raciocínio, auxiliando o processo interpretativo, tornando-o mais direto. Para quem a recebe, a informação clara diminui a dependência da ciência prévia de múltiplos conceitos relacionados àquela informação, fazendo então com que a curva de conhecimento a ser percorrida para compreender corretamente a informação tenda a ser nula. Também pode-se dizer que, quanto mais clara é a informação, menor é a bagagem intelectual necessária para o seu entendimento correto, evitando assim a fadiga informacional (UNIÃO EUROPEIA, 2017, p. 7).

3.1.1.2 Precisão

O segundo elemento de transparência presente no artigo 6º, inciso VI da LGPD é a **precisão** da informação (BRASIL, 2018). A informação precisa é aquela que não deixa dúvidas quanto a ser isto ou aquilo. Ser preciso na comunicação é ter a habilidade de gerar uma mensagem que não induza ao erro, não pela interpretação equivocada por parte de quem a recebe, mas por não ser objetivo o suficiente nos termos empregados. A precisão da informação pode requerer o emprego de termos ou expressões mais específicas, afastando o uso de elementos genéricos que possam levar a interpretações distintas (UNIÃO EUROPEIA, 2017, p. 8). O requisito de precisão deve impedir que se tome uma espécie por outra dentro do mesmo gênero, e assim é preferível fazer menção ao gênero correto dentro daquela espécie, se tal distinção for importante. A precisão também cumpre a função de diferenciar algo que é daquilo que não é, isto é, a mensagem que é precisa permite excluir possibilidades, dando maior condição para que o seu receptor localize, no campo das ideias, aquilo que pode estar e aquilo que pode não estar incluído no entendimento feito pelo receptor. A comunicação da informação de maneira precisa orienta aquele que a recebe, e o instrumentaliza para que o raciocínio sobre a mensagem seja feito utilizando os fundamentos corretos. A informação dotada de precisão, assim, permite que o entendimento da mensagem seja feito de forma correta, e pode então levar a decisões acertadas. O Grupo de Trabalho do Artigo 29 supramencionado ainda argumenta que a comunicação deve ser eficiente e sucinta, ao comentar sobre o termo **conciso** da GDPR, que tem certa proximidade com o elemento de precisão da LGPD (UNIÃO EUROPEIA, 2009, p. 7).

Ressalte-se que a falta de precisão da mensagem pode suscitar indagações por quem a lê, e assim pode conferir também falta de clareza. As informações imprecisas podem criar uma espécie de miopia por quem as acessa, e assim pode ser a causa de decisões erradas por parte daqueles que as usam.

3.1.1.3 Fácil acessibilidade

A **fácil acessibilidade** é o terceiro elemento de transparência trazido pelo artigo 6º, inciso VI da lei geral de proteção de dados (BRASIL, 2018). O ordenamento jurídico brasileiro tem a lei 10.098 de 2000, que estabelece normas e critérios sobre acessibilidade, e que define o que é acessibilidade nos seguintes termos:

> possibilidade e condição de alcance para utilização, com segurança e autonomia, de espaços, mobiliários, equipamentos urbanos, edificações, transportes, informação e comunicação, inclusive seus sistemas e tecnologias, bem como de outros serviços e instalações abertos ao público, de uso público ou privados de uso coletivo, tanto na zona urbana como na rural, por pessoa com deficiência ou com mobilidade reduzida (BRASIL, 2000).

Para além da expressão "facilmente acessíveis", deve-se consignar que o termo "acessível", refere-se a algo ou alguém a quem se pode ter acesso. Então, a acessibilidade determina em que medida se pode ter acesso a algo ou alguém. Assim, fácil acessibilidade remete à facilidade de acesso a algo ou alguém. O verbo "acessar", a seu turno, tem vários significados. Sem a pretensão de esgotar o rol de sinônimos, o verbo acessar pode significar: ler, ver, obter, possuir, adquirir, comprar, usar, manipular, interagir com, atingir, alcançar, tocar, pegar, mexer, avaliar, abrir, apreciar, dentre outros. Sendo assim, para dizer que algo ou alguém é acessível ou não é necessário identificar a espécie de acesso. Para este estudo, fácil acessibilidade é característica de informação, e assim a fácil acessibilidade da informação é elemento fundamental para o alcance da transparência sobre quais são as atividades de tratamento de dados realizadas, e ainda sobre quem as realiza. Ainda que se tenha delimitado que o que deve ser facilmente acessível é a informação acerca das operações de tratamento e de quem as faz, mesmo assim diversas espécies de significados podem se aglutinar no gênero "acesso". A acessibilidade e a compreensibilidade são tão importantes quanto o próprio conteúdo divulgado na informação sobre transparência (UNIÃO EUROPEIA, 2017, p. 5). Por exclusão, como os elementos de clareza e precisão se prestam à interpretação das informações, num espectro mais lógico, então é possível interpretar que o "acesso" tem um caráter mais físico do que lógico. Se for neste sentido, então o termo acesso pode ter acepções de ler, visualizar, ouvir, mexer, usar, manipular, interagir com, abrir e outros. Tem-se, assim, a facilidade de leitura, a facilidade de visualização, a facilidade de audição e a facilidade de interação como possíveis subelementos de transparência do elemento facilidade de acesso.

Tomando facilidade de leitura como sendo um tipo de facilidade de acesso, portanto um subelemento formador da transparência, então é possível analisar de que forma a facilidade de leitura contribui para a transparência. Deixando de lado os aspectos de interpretação que são facilitados pela clareza e pela precisão da informação, há outras características que facilitam a leitura. Dentre elas, podem ser destacadas a tipografia, o tamanho, e a cor da fonte utilizada no texto. O texto que tem letras apropriadas, de tipografia simples sem aspecto cursivo, contribui também para a facilidade de leitura,

assim como o texto que tem fontes de tamanho apropriado para a leitura, inclusive das pessoas que têm dificuldade de visão por distância. Outro aspecto é a cor do texto, que deve contrastar com o seu fundo, podendo ser lida inclusive por pessoas portadoras de daltonismo. Dado o grande volume de informações disponibilizado à pessoa, o *Working Party 29* sugere que os avisos de privacidade sejam elaborados usando a *layered approach*, ou abordagem em camadas, segundo a qual as informações de transparência são agrupadas em categorias, para que o titular possa interagir com o documento evitando a fadiga informacional de longos documentos; o WP29 recomenda, ainda, que na primeira camada da solução adotada pelo controlador sejam exibidas informações que, em especial, poderiam causar surpresa aos titulares (UNIÃO EUROPEIA, 2017, p. 19).

Outro facilitador de acesso à informação é a facilidade de visualização. Neste caso, não se considera o texto em si, pois já foi tratado no ponto anterior, mas sim os elementos gráficos nos quais os textos e outros símbolos, signos ou figuras estão contidos. A informação é facilmente acessível se for apresentada em componentes destacados de outros elementos visuais, contrastando com os demais, e se a eles estiver sobreposta. As diretrizes sobre transparência do Grupo de Trabalho do Artigo 29 classifica como facilmente acessíveis aquelas informações aparentes de forma imediata, com sinalizações, com *pop-ups* contextuais, ou interfaces de *chatbot* (UNIÃO EUROPEIA, 2017, p. 8). Há casos em que as informações sobre transparência são exibidas obrigatoriamente e somente permitem qualquer outra ação se o indivíduo com elas interagir. Este é um tipo de comportamento que torna a visualização obrigatória, contribuindo para a transparência se for aplicado da maneira correta. Outro aspecto que facilita a visualização é o tamanho total do contêiner de informação de transparência, que deve ser proporcionalmente significativo em relação ao todo, ao campo de visão daquele que lê. Por fim, também o posicionamento da informação na janela de visualização é relevante, pois em certos casos pode não cumprir com o seu papel de comunicar, isto é, pode ter baixa efetividade. É possível, ainda, o uso de *dashboards* de privacidade, típicos centros de controle que organizam as informações sobre privacidade do usuário (UNIÃO EUROPEIA, 2017, p. 20).

Em seguida, a facilidade de acesso pode ser obtida por promoção da comunicação por meios sonoros, para aqueles impossibilitados da leitura visual, como a facilidade de audição. Os métodos audiovisuais podem ser utilizados para comunicar com linguagem clara e simples (UNIÃO EUROPEIA, 2017, p. 8). O fornecimento de informações sonoras, de forma oral automatizada no caso dos meios eletrônicos, é uma medida

possível para situações deste tipo (UNIÃO EUROPEIA, 2017, p. 13). Nos sistemas computacionais modernos, tanto nos navegadores quanto nos sistemas operacionais, há ferramentas disponíveis que cumprem esta função, desonerando a carga deste tipo de adaptação aos agentes de tratamento em geral, porquanto há suporte do sistema operativo que apoia a interação com a pessoa. É importante ressaltar que no Brasil existe o Estatuto da Pessoa com Deficiência, ou Lei Brasileira e Inclusão da Pessoa com Deficiência, "destinada a assegurar e a promover, em condições de igualdade, o exercício dos direitos e das liberdades fundamentais por pessoa com deficiência, visando à sua inclusão social e cidadania" (BRASIL, 2015) e que tutela, dentre outros, o direito das pessoas que têm necessidades especiais para acesso à informação e às tecnologias. É possível notar, ao menos nos *websites* do Governo Federal brasileiro, a presença de elementos de acessibilidade, como a tradução em libras com o emprego de um assistente virtual e uma seção dedicada sobre acessibilidade.

Por fim, há a facilidade de interação, que também contribui para facilitar o acesso à informação para a transparência. Este requisito consiste na capacidade que tem o conjunto de elementos que apresentam a informação para permitir a boa usabilidade. Em sistemas eletrônicos, como em *websites*, os componentes que dão suporte às informações de transparência devem permitir fácil uso, devem se comportar conforme o esperado, e devem ter robustez e resiliência durante o seu uso. A abordagem em camadas, anteriormente explicada, também contribui para facilitar a interação com o usuário titular de dados. No caso do direito comunitário europeu, as diretrizes sobre transparência do *Working Party 29* recomendam o uso de avisos de privacidade em camadas para os casos de controladores com presença digital (UNIÃO EUROPEIA, 2017, p. 14), como *websites*, aplicativos e metaversos.

Nesse sentido, a clareza, a precisão e a acessibilidade têm papel relevante no desempenho do processo interpretativo das informações que são comunicadas, pois influenciam a eficiência, a eficácia e a efetividade da comunicação (UNIÃO EUROPEIA, 2017, pp. 7-26). A eficiência, assim entendida como a medida de racionalidade dos recursos, é a medida da obtenção dos melhores resultados com o menor nível de esforço, e é ferramenta de análise objetiva, de racionalização dos insumos com o fito de gerar a maior economicidade, o menor custo, e o mais alto resultado que for possível. Evitar a fadiga da informação (UNIÃO EUROPEIA, 2017, p. 7) é uma das formas de garantir a eficiência. A eficácia, que confere assertividade ao objeto de estudo, é a medida que informa que o alvo foi ou não alcançado, que algo foi atingido ou não, de forma objetiva,

se o resultado foi obtido ou não, sem relativizações sobre economicidade ou nível de esforço empregado, sendo assim também um instrumento objetivo de medição. A adoção de medidas que permitam ao titular o controle de seus dados por meio de recursos visuais (UNIÃO EUROPEIA, 2017, p. 25), com alta granularidade de detalhamento, é medida eficaz se implementada corretamente. A efetividade, por sua vez, é medida de desempenho que avalia se o resultado alcançado atende aos propósitos a que se destina, desta vez com uma análise mais subjetiva que as demais, a eficiência e a eficácia, apesar de ser possível determiná-la a partir de elementos objetivos. A efetividade pode ser medida em uma escala de graus, sendo assim comparar os resultados que sejam mais ou menos efetivos. A medida da efetividade pode ser calculada utilizando fatores exógenos à eficiência e à eficácia, tomando-se outros elementos como seus balizadores, tais como os valores morais, que são de natureza subjetiva. Da mesma forma, a efetividade também pode ser aferida a partir de elementos objetivos, como a tempestividade dos resultados alcançados. Assim, é possível estabelecer índices de transparência com base nos elementos da clareza, precisão e acessibilidade, utilizando medidas calculadas com o uso da eficiência, eficácia e efetividade da informação comunicada.

3.1.2 Elementos de transparência no tratamento de dados pessoais

O princípio da transparência apresenta outro elemento formador, que é o objeto sobre o qual versam as "informações claras, precisas e facilmente acessíveis" (BRASIL, 2018). Este elemento é o assunto de que tratam tais informações: são as **informações sobre o tratamento dos dados pessoais**, e as **informações sobre os agentes de tratamento respectivos**. Dar transparência sobre o tratamento é muito mais do que indicar as possíveis formas de tratamento do artigo *5º*, inciso X da LGPD.

Para organizar todos os aspectos envolvidos no tratamento de dados, pode-se usar a ferramenta 5W2H, que permite analisar sete dimensões do objeto de estudo. Esta ferramenta é muito utilizada em planejamentos administrativos, e também em programas de qualidade. As dimensões do 5W2H auxiliam o entendimento sobre qualquer assunto, inquirindo sobre: o quê, por que, quem, quanto, como, quando e onde (PAIM, 2009, p. 197). Então, aplicando esta ferramenta para investigar quais as características do tratamento de dados devem ser informadas, pode-se afirmar que são as seguintes: a) quais dados pessoais são tratados; b) por que os dados pessoais são tratados; c) quem trata os dados pessoais; d) quanto custa o tratamento dos dados pessoais; e) como os dados

pessoais são tratados; f) quando os dados pessoais são tratados; e g) onde os dados pessoais são tratados. A aplicação da técnica proporcionada por esta ferramenta administrativa favorece a organização das ideias em torno de quais informações de transparência devem ser apresentadas. Cada uma delas tem seu grau de importância, e a relação entre elas está representada na Figura 4.

Figura 4: aplicação da técnica 5W2H para identificar as características do tratamento de dados
Fonte: Elaborado pelo autor.

3.1.2.1 Quais dados pessoais serão tratados

Aplicando a técnica 5W2H para estudar o tratamento de dados, tem-se que inicialmente devem ser apresentadas informações sobre **quais dados pessoais são tratados**. A LGPD conceitua dados pessoais e dados pessoais sensíveis no artigo *5º*, incisos I e II: dado pessoal é a "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018), e dado pessoal sensível tem uma caracterização especial, sendo "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (BRASIL, 2018). Os dados pessoais podem ser, então dos mais variados

tipos, tais como nome, endereço, identificador pessoal, CPF, valores de *cookies*, localização geográfica, fotografia, preferência religiosa ou política, dentre outros. Assim, a informação sobre quais são esses dados deve ser comunicada para atender ao princípio da transparência.

Como é nota característica da tecnologia, a sua constante evolução causa efeitos que modificam continuamente a realidade. Assim, o conceito de dado pessoal se altera à medida que vão surgindo novas formas de tratamento e de reidentificação dos indivíduos (DONEDA *et. al.,* 2021). O volume exponencial, a velocidade crescente e a variedade cada vez maior forma os três Vs, uma forma de explicar o que é big data. *Big data* permite que uma quantidade imensa e cada vez maior de dados, proveniente de novas fontes, seja tratada com o objetivo de resolver problemas que não poderiam ser solucionados sem os três Vs – volume, velocidade e variedade (ORACLE, 2022). A solução de problemas usando *big data* é possível pelo emprego de técnicas computacionais avançadas, tais como aquelas do campo da inteligência artificial (DONEDA *et. al.,* 2021, Cap. 9, item 1). Um dos papeis da proteção de dados pessoais é evitar a ocorrência de discriminações, que podem ocorrer após a formação de perfis correspondentes às pessoas utilizando a inteligência artificial (DONEDA *et. al.,* 2021), pela realização de análises comportamentais, e consequente inferência de atributos pessoais muitas vezes sensíveis.

A classificação dos dados quanto à sensibilidade – dados pessoais e pessoais sensíveis – é complementada pela classificação quanto à identificabilidade do indivíduo – dados desanonimizados, pseudoanonimizados e anonimizados. O espectro da identificabilidade da pessoa a quem pertencem também é informação importante para a finalidade da transparência, pois pode também influenciar e determinar tanto as hipóteses legais quanto as formas de tratamento. A pseudonimização, a exemplo, mascara a identificação da pessoa, sendo possível ao agente reidentificá-la posteriormente por meio de cruzamento com dados adicionais (SOMBRA, 2019, p. 159) ou outras técnicas computacionais. A anonimização, por seu turno, impossibilita estabelecer vínculo de pertinência a um indivíduo específico; dados anonimizados não são objeto de regulação pela lei se não for possível a reidentificação do titular (SOMBRA, 2019, p. 170). Assim, a classificação do tipo de dado pode justificar o uso de uma ou outra base legal de tratamento.

3.1.2.2 Por que os dados pessoais serão tratados

Outro elemento importante de transparência do tratamento é **o porquê, ou motivo, ou razão do tratamento**. A LGPD usa um termo específico: hipótese. Esta lei apresenta dez hipóteses de tratamento de dados pessoais no artigo *7º*, que são, de forma genérica: pelo fornecimento de consentimento, para cumprimento de obrigação legal ou regulatória pelo controlador, para execução de políticas públicas pela administração pública, para realização de pesquisas, para execução de contratos, para exercício regular de direitos, para proteção da vida, para tutela da saúde, para atender o interesse legítimo do controlador, e para proteger o crédito (BRASIL, 2018). Marcacini faz uma classificação binária das hipóteses de tratamento, separando entre aquelas que acontecem por algum tipo de vontade do indivíduo e aquelas que prescindem de autorização (DE LIMA, 2020, p. 143). Para o mesmo autor, há casos em que o consentimento é expresso e outros em que a autorização é tácita (DE LIMA, 2020, pp. 143-148), enquanto que há hipóteses que permitem o tratamento de dados pessoais ainda que sem depender da autorização do titular para tal, e outras que até podem ocorrer mesmo que o titular se oponha ao tratamento de seus dados (DE LIMA, 2020, pp. 143-155).

Para além do rol das hipóteses legais de tratamento de dados, assim como das muitas classificações instrumentais sobre o tratamento de dados e os elementos da transparência, está a importante crítica feita pela doutrina nacional sobre o papel da autodeterminação informativa como elemento central dos sistemas normativos de proteção de dados atuais. Segundo obra de Bruno Bioni, ideias tais como a do princípio da participação individual propalado pelas *guidelines* da OCDE lançaram mais luzes no próprio cidadão, para municiá-lo de poderes com em busca da proteção dos dados da pessoa (BIONI, 2019, pp. 117-121). A quarta geração de leis de proteção de dados pessoais evoluiu em algumas áreas, e manteve o consentimento como elemento central de seus debates, inclusive o qualificando com adjetivos, gerando quase uma simbiose entre consentimento e autodeterminação informativa (BIONI, 2019, p. 117).

O estudo do presente trabalho se concentra na transparência dos *websites*, avisos de *cookies* e políticas de privacidade. Como tal, as hipóteses legais que mais se destacam, ao menos da perspectiva atual, são o consentimento e o legítimo interesse.

Como assinalado anteriormente, o consentimento ocupa um papel importante também na lei de proteção de dados brasileira; exemplo disto é o fato de que ele é mencionado trinta e cinco vezes no seu texto, e é a única hipótese mencionada no artigo 5º do diploma legal, como sendo a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade

determinada" (BRASIL, 2018). Passa-se agora a analisar as características do consentimento conforme a LGPD, presente nos artigos 5º, 8º e 11. O consentimento livre é expressão da autodeterminação do indivíduo no respeito às suas próprias convicções, sem imposições, devendo ser considerado o "poder de barganha" e o grau de assimetria existente na situação (BIONI, 2019, p. 197). O consentimento informado é expressão do dever de informação do controlador e do direito de informação deste titular com o objetivo de reduzir a assimetria informacional (BIONI, 2019, p. 196). O consentimento inequívoco, por sua vez, é aquele sobre o qual se tem certeza da decisão (BIONI, 2019, p. 199), enquanto que o consentimento para finalidades determinadas é aquele que indica de forma específica quais são os respectivos propósitos (BIONI, 2019, p. 198). Também o consentimento é específico quando se refere a algumas hipóteses determinadas, em que haja maior risco, como dados sensíveis, dados de menores, na transferência internacional para países com nível de proteção de dados menor que o do Brasil, e na transferência para terceiros que não mantenham relação direta com o titular (BRASIL, 2018; BIONI, 2019, p. 201). Acerca das finalidades do consentimento, a teoria da privacidade que alude ao consentimento contextual tem o objetivo de flexibilizar os mecanismos de ajuste e de licitude do tratamento de dados, por meio da adequação da dinâmica que envolve o tratamento de dados e os negócios, de um lado, e as legítimas expectativas do titular, de outro, de forma que o consentimento seja continuamente convalidado à medida em que o contexto se altere (BIONI, 2021, item 5.4.1).

O legítimo interesse é a hipótese de tratamento de dados prevista no artigo 7º, inciso IX da LGPD: "quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais" (BRASIL, 2018). A possibilidade de tratamento de dados por legítimo interesse do controlador ou de terceiro, que foi trazida ao Brasil na LGPD por influência da GDPR, precisa atender a parâmetros legais que podem ser avaliados por meio do teste de proporcionalidade, ou *legitimate interests assessment*, ou simplesmente LIA (BIONI, 2021). Este procedimento tem o condão de avaliar o equilíbrio entre os interesses legítimos do controlador, de um lado, e as legítimas expectativas do titular de dados, de outro lado, conforme documentado no artigo 10 da LGPD (BIONI, 2021). Bruno Bioni entende que o teste do legítimo interesse em quatro fases é o que tem maior aderência ao contexto brasileiro, da seguinte forma: a) legitimidade: avaliação, pelo controlador, se a finalidade do tratamento no caso concreto é legítima, se não viola normas legais; b) necessidade: avaliação, pelo controlador, se os

dados tratados são aqueles minimamente necessários à finalidade pretendida, e se não há outra base legal mais apropriada; c) balanceamento: ponderação, à luz do princípio da boa-fé, pelo controlador, indagando se as legítimas expectativas do titular de dados são atendidas mediante o tratamento de dados para a finalidade pretendida, e avaliando o impacto sobre os direitos dos titulares; e d) emprego de medidas que promovam a transparência sobre as atividades de tratamento realizadas e que minimizem os riscos que possam trazer consequências negativas aos titulares (BIONI, 2021).

3.1.2.3 Por quem os dados pessoais serão tratados

O componente seguinte que faz parte do elemento de transparência do tratamento de dados é aquele que informa sobre **quais são os agentes de tratamento**. Os agentes de tratamento são aqueles responsáveis pelo tratamento e também aqueles que efetivamente o exercem, operacionalizando as funções finais. Novamente, o artigo *5º* da LGPD indica que os agentes de tratamento são os controladores e os operadores de dados: controlador é toda "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", e operador é a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador". O termo “responsável”, que constava no anteprojeto da lei, foi substituído por “controlador” (DE LIMA, 2020). Os atributos sobre o agente de tratamento podem ser depreendidos do art. *9º*, incisos III, IV e V: identificação do controlador, informações de contato do controlador e do uso compartilhado de dados pelo controlador (BRASIL, 2018). Por identificação do controlador, há como se entender o nome da pessoa natural, o nome social, o nome empresarial, o nome fantasia, números de identificação como do cadastro de pessoas físicas, do cadastro nacional de pessoas jurídicas, e outros similares. Sobre informações de contato do controlador, podem estar presentes os números de telefone, endereços de correio eletrônico, endereços físicos, identificadores de endereços eletrônicos de contato de redes sociais e outros. Sobre o uso compartilhado de dados, é necessário informar sobre o co-controlador participante do compartilhamento.

O artigo 41 define que o "controlador deverá indicar encarregado pelo tratamento de dados pessoais" (BRASIL, 2018). O § 1º do mesmo artigo da LGPD estabelece que a "identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do

controlador" (BRASIL, 2018). Sendo assim, em se tratando de transparência sobre os agentes de tratamento, os referidos dados sobre o encarregado precisam ser informados também.

O artigo *9º*, inciso VI da LGPD, estabelece que também devem ser informadas as "responsabilidades dos agentes que realizarão o tratamento" (BRASIL, 2018). Nas situações em que houver múltiplos agentes de tratamento, é necessário indicar as responsabilidades respectivas (MALDONADO, 2019, p. 192). Quanto a responsabilidades dos agentes, é possível estabelecer uma fronteira sobre a segregação de funções, com ou sem terceirização de atividades de tratamento, mediante a indicação de quais espécies de tratamento são de responsabilidade direta do controlador e quais são de responsabilidade direta do operador, assim como sobre a duração de tratamento de cada um, e demais condições conforme já apresentado, construindo uma separação de responsabilidades. Assim, todos os atributos que determinam a separação de responsabilidades devem ser informados, isto é, todos os aspectos do tratamento de dados sob responsabilidade do operador devem ser comunicados, inclusive os dados de identificação e de contato do operador, numa interpretação extensiva do artigo *9º*, inciso III e IV que determinam a divulgação destes atributos em relação ao controlador.

3.1.2.4 Quanto custará se os dados pessoais forem tratados

O seguinte ponto do elemento de transparência do tratamento de dados é o que indica o **custo do tratamento**. O tratamento de dados pode ser gratuito ou oneroso. Nos serviços pagos, o tratamento de dados pessoais pode ser realizado de forma distinta daqueles gratuitos, como nos casos em que os dados pessoais podem ser armazenados por um longo tempo ou podem ser tratados apenas como temporários, de acordo com o tipo de serviço contratado. No campo da publicidade comportamental *online*, também conhecida como *online behavioral advertising*, *online profiling*, ou ainda *behavioral targeting*, as organizações obtêm dados pessoais e os repassam para agregadores de dados, ou *data brokers*, implantando componentes de terceiros de publicidade em seus *websites*; estes componentes embutem códigos que são carregados pelo navegador e capturam dados pessoais, com o objetivo de formar perfis das pessoas ou identificá-las; tal prática permite que anunciantes de produtos e serviços tenham maior assertividade em suas campanhas publicitárias, muitas vezes ao custo da privacidade do público alvo (BOERMAN; BORGESIUS; KRUIKEMEIER, 2017, p. 364). Este modelo de negócio

pode ser denominado *zero-price advertisement business model* (BIONI, 2021), e tem como combustível, de um lado, o fornecimento dos dados pessoais pelos titulares a título gratuito, e de outro lado a prestação de serviços também gratuitos e a personalização de anúncios publicitários monetizados. É certo que os indivíduos podem até preferir receber anúncios personalizados, pois têm o direito de decidir o que fazer com os seus dados, com base na autodeterminação informativa, utilizando de forma "gratuita" certos serviços na *Internet*. Porém, o indivíduo não tem controle sobre que tipo de tratamento será realizado com seus dados (BIONI, 2021), sendo necessário dar transparência àquilo que será feito com os dados pois nada é tão gratuito assim, uma vez que a indústria de marketing digital movimenta cifras astronômicas – usando o "novo petróleo" – que são os dados pessoais. Assim, é também elemento de transparência a informação de que o tratamento de dados poderá ser realizado de forma gratuita ou onerosa, a depender da situação, e que, respeitados todos os direitos fundamentais do respectivo titular e com base nas hipóteses legais adequadas, os dados serão tratados de uma ou outra forma, podendo ser comercializados com terceiros com objetivos econômicos.

3.1.2.5 Como os dados pessoais serão tratados

Parte integrante, e talvez a mais importante sobre o tratamento de dados, é a informação sobre a **forma de tratamento realizado**, respondendo à questão sobre **como os dados são tratados**. O artigo *5º*, inciso X da LGPD exemplifica as formas de tratamento. Os dados pessoais têm um "ciclo de vida", que se inicia quando passam a estar no domínio do controlador, e que termina quando deixam de existir na esfera de atuação do controlador. As informações de tratamento de dados precisam indicar quais são as formas de tratamento realizadas, permitindo que o titular decida sobre o tratamento, se aceita ou não a coleta, a transmissão para terceiros, o processamento ou outra forma de tratamento. É usual encontrar avisos sobre tratamento de dados que indicam diversas formas de tratamento, porém que não permitem que o titular escolha quais tipos de tratamento ele permite que sejam realizados, nos casos baseados em consentimento. O ideal é que o controlador forneça meios para que o titular de dados pessoais possa controlar as formas de tratamento disponíveis, com o uso de ferramentas que forneçam maior granularidade em sua composição. O aumento de granularidade das possibilidades de tratamento de dados também é útil ao próprio controlador, pois favorece a utilização de bases legais distintas para formas de tratamento distintas. Sendo assim, certos tipos de

tratamento podem ocorrer à vista do legítimo interesse do controlador ou de terceiro, e outros mediante o consentimento do titular.

3.1.2.6 Por quanto tempo os dados pessoais serão tratados

Avançando nos itens que compõem os elementos de transparência, há também o **aspecto temporal do tratamento de dados**. Este atributo traz a **duração do tratamento**, como também indicado no artigo *9º*, inciso II da LGPD. Esta lei define hipóteses para o início e para o término do tratamento de dados, nos artigos *7º* e 15 respectivamente. No caso da GDPR, a informação sobre a duração do tratamento também é elemento de transparência (DONEDA *et. al.,* 2021), e influencia no ciclo de vida dos dados pessoais em poder dos controladores, pois determina o início e o fim do tratamento. A depender das hipóteses legais informadas, a duração do tratamento pode se estender por muitos anos ou durar poucos instantes. Nos casos em que houver obrigação legal de conservação de dados pessoais por parte do controlador por longos períodos, o ciclo de vida dos dados pode perdurar longamente. Em outros casos como o uso de dados pessoais com base no legítimo interesse, para que um *website* seja montado corretamente de acordo com as características do navegador usado pelo indivíduo, certos dados que possam identificar a pessoa podem ser obtidos instantaneamente e eliminados no minuto seguinte, pois não são mais necessários àquela finalidade. A LGPD define que o ciclo de vida dos dados inicia, se desenvolve e termina (DONEDA, *et. al.,* 2021). O ciclo de vida dos dados pessoais tem início nas formas de tratamento que expõem os dados aos agentes de tratamento, controladores e operadores. A coleta de dados massiva da atualidade é uma das formas de iniciar este ciclo de vida (DONEDA, *et. al.,* 2021). A gênese do ciclo de vida dos dados tem lugar na verificação de uma das dez hipóteses de tratamento indicadas no artigo *7º*. Com a coleta massificada de dados, há um grande risco de iniciar o tratamento sem a devida cautela de cumprimento da lei.

Ainda sobre o critério temporal que deve ser informado ao titular pelos agentes de tratamento respectivos, a Lei Geral de Proteção de Dados dedica os artigos 15 e 16 ao assunto no que diz respeito ao término do tratamento.

O artigo 15 especifica as hipóteses de término do tratamento de dados pessoais, marcando assim o encerramento do ciclo de vida do dado para os agentes de tratamento. A primeira hipótese diz respeito à **finalidade**: o tratamento dos dados deve se encerrar quando a finalidade que deu início ao ciclo de vida for atingida, ou ainda quando não for

possível atingir a finalidade determinada, tanto por falta de necessidade, como por excesso, quanto por falta de pertinência, como a obsolescência (DONEDA, *et. al.,* 2021). Esta hipótese de fim de tratamento envolve alguma forma de avaliação qualitativa mais apurada sobre os dados em poder dos agentes. A segunda hipótese de finalização do tratamento é pelo **decurso do tempo**, isto é, esvaiu-se o lapso temporal durante o qual os dados poderiam ser tratados. Esta hipótese acena com um critério mais objetivo de tratamento, desde que seja mantido controle sobre a data de início do tratamento juntamente com o período máximo permitido, ou ainda se o próprio dado fizer menção a uma data específica. A doutrina apresenta duas possibilidades: tratamento esporádico ou quando se espera que o tratamento dure por um tempo limitado (DONEDA, *et. al.,* 2021). É possível utilizar tabelas de temporalidade para controle do fim do período de tratamento para atender a esta hipótese legal. A terceira via de término do tratamento de dados trazida pelo artigo 15 da LGPD é aquela que privilegia o princípio do livre acesso por parte do titular, no exercício da **autodeterminação informativa**: trata-se da "comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento", e ainda "resguardado o interesse público". É de se dizer que o titular tem o direito de se opor ao tratamento de dados realizado pelo agente. Sendo assim, usando do direito de petição conferido ao titular pelo artigo 18 da presente lei, o indivíduo pode determinar o término do tratamento, tenha ele iniciado de forma lícita ou não, e por qualquer hipótese legal que seja. O mesmo artigo 15, inciso III que cuida da hipótese em tela ressalta o direito de revogação do consentimento outrora fornecido pelo titular. Supõe-se que os controladores se aparelhem para atender às solicitações dos titulares por meio de canais de comunicação ou meios de gestão específicos (DONEDA, *et. al.,* 2021). Por fim, a última hipótese de término de tratamento de dados é admitida pela lei nos casos em que a **Autoridade Nacional de Proteção de Dados assim ordenar**, para os casos de inobservância da lei de proteção de dados.

Também sobre o critério temporal do tratamento de dados, o artigo 16 traz no seu *caput* que "[o]s dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades" (BRASIL, 2018). O comando determina que, em regra geral, a única forma de tratamento possível, após a ocorrência de uma das hipóteses do artigo 15, é a eliminação dos dados. O mesmo dispositivo também esclarece que a eliminação ocorrerá no escopo das atividades desempenhadas pelo agente de tratamento respectivo. Ou seja, este ponto revela a importância de definir, documentar e informar as responsabilidades

de cada agente de tratamento, atendendo ao disposto no artigo *9º*, inciso VI, que informa o direito do titular a ser informado sobre as responsabilidades de cada agente que tratar seus dados pessoais.

O artigo 16 ainda admite que a eliminação de dados ao fim do tratamento pode sofrer restrições de ordem técnica, reconhecendo a chance de ocorrência de situações em que a eliminação dos dados seja impossibilitada por fatores técnicos. Neste ponto, a LGPD admite que a evolução tecnológica pode impactar o tratamento de dados quanto ao seu término (DONEDA, *et. al.,* 2021). Ressalva ao término do tratamento de dados nesta hipótese deve ser feita para os casos deste artigo 16 da LGPD. Estas hipóteses contrabalançam com a possibilidade de término compulsório do tratamento de dados, garantindo direitos ao controlador, para algumas finalidades bem determinadas: para o atendimento da lei pelo controlador; para estudos científicos, com anonimização se possível; para transferir os dados a outro controlador, nos termos legais; e para uso próprio do controlador, também com anonimização, e com proibição de uso por terceiro. Estas exceções à regra de término de tratamento de dados devem ser fruto de ponderação dos interesses dos envolvidos (DONEDA, *et. al.,* 2021).

Tais possibilidades trazidas pelo artigo 16 permitem a extensão do ciclo de vida dos dados pessoais, pois são finalidades que autorizam a sua conservação. Assim, também são hipóteses que garantem direitos aos controladores, desde que observadas as normas legais. Estas possibilidades do artigo 16 são hipóteses legais de tratamento de dados subsidiárias àquelas informadas ao titular no início do tratamento. Vale dizer, em tese o tratamento de dados pode ter se iniciado com base em uma das dez hipóteses do artigo *7º*, porém os dados podem ser conservados com fundamento em uma das quatro hipóteses do artigo 16. Por exemplo, os dados inicialmente obtidos mediante consentimento do titular podem ser conservados para atendimento de obrigação regulatória do controlador; ou os dados obtidos mediante consentimento do titular podem ser compartilhados com órgão de pesquisa, que por sua vez poderá manter tais dados em seu poder, anonimizando se possível. A doutrina exemplifica com os casos dos setores financeiro e de telecomunicações, que têm regras específicas que obrigam os agentes a manterem os dados sob certo período (DONEDA, *et. al.,* 2021).

3.1.2.7 Onde os dados pessoais serão tratados

Mediante o uso da ferramenta 5W2H apresentada anteriormente, a última propriedade do elemento que caracteriza o tratamento de dados é aquela que determina **onde** os dados pessoais são tratados. O local do tratamento não se confunde com o sujeito que realiza tal ofício, apesar de estarem intimamente ligados. Acerca do local do tratamento, é importante tecer comentário sobe a aplicabilidade da lei geral de proteção de dados, que em seu artigo 3º define que ela se aplica "a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados", estabelecendo alguns requisitos para sua incidência. A lei de proteção de dados incide independentemente de qual for o meio de suporte dos dados pessoais. Se a mídia onde os dados estão ou por onde transitarem for física, tais como papel, ou ainda se o meio for digital, então a lei ainda tem aplicabilidade, qualquer que seja o meio usado. A Lei geral de Proteção de dados é mais abrangente que o Marco Civil da *Internet*, pois este se refere somente ao meio *online*, porém não há revogação tácita deste diploma pela LGPD (COTS; OLIVEIRA, 2020, p. 62).

Esta lei pode ser aplicada a qualquer agente de tratamento, seja pessoa natural ou jurídica, de direito público ou privado, não importando qual for país da sede. No caso de aplicação da LGPD a pessoa natural, pode-se entender o termo "sede" como sendo a nacionalidade da pessoa natural. Assim, a lei não faz distinção de nacionalidade de origem do agente de tratamento de dados. O mesmo excerto legal informa que o local onde os dados pessoais estiverem localizados não influencia na aplicabilidade da lei de proteção de dados brasileira. Portanto, a lei geral de proteção de dados pode ser aplicada a todas as pessoas que tratam dados, independente do local da sua sede ou da sua nacionalidade, e tem autorização para incidir nos casos em que os dados estejam em território nacional ou estrangeiro. Desta forma, a LGPD não discrimina o agente de tratamento em função da nacionalidade, e admite a ubiquidade dos dados, que podem ser transferidos, replicados ou espelhados em diversos sítios de nações diferentes, moldando-se à ideia de computação em nuvem, ideia que abstrai a noção de espaço físico com localização determinada e que cria uma espécie de ambiente virtual em que o entendimento do local dos serviços, dados e programas não comporta fronteiras.

Ainda no artigo *3º*, os requisitos que determinam o uso da lei não são cumulativos, assim basta que um deles seja atendido para que o documento legal em estudo possa ser aplicado. A primeira possibilidade de aplicação influenciada pelo atributo de localização acontece desde que "a operação de tratamento seja realizada no território nacional"

(BRASIL, 2018). Deste modo, se os dados estiverem em território estrangeiro, e ainda que a nacionalidade do agente de tratamento de dados seja também alienígena, aplicar-se-á a lei brasileira quando a operação de tratamento de dados ocorrer no Brasil.

A LGPD tem que lidar com a possibilidade de os dados e os programas que os manipulam estarem dispersos em arranjos computacionais distribuídos, evolução da "arquitetura de von Neumann" e seguintes quando os computadores eram monolíticos. A lei brasileira se aplica mesmo quando os elementos que a compõem estão distribuídos geograficamente, desde que a unidade de processamento – que trata os dados pessoais – esteja localizada em território brasileiro. Dermot Turing conta, em seu livro sobre a história da computação, que a concepção da ideia da arquitetura de von Neumann é atribuída a John von Neumann, húngaro que trabalhou com o famoso matemático Alan Turing, e que propôs uma evolução ao computador ENIAC (*Electronic Numerical Integrator and Computer*). Juntamente com outros pesquisadores, escreveu o chamado "Primeiro esboço de relatório sobre o EDVAC" (*Electronic Discrete Variable Automatic Computer*), porém somente o nome de von Neumann constou na capa do relatório, o que causou disputa judicial por causa da patente da invenção anos depois. A inovação da patente era a de que a máquina que fazia os cálculos, as computações – o computador – poderia armazenar também as próprias instruções computacionais. O ENIAC, computador com o qual John von Neumann trabalhava à época, na década de 1940, não possuía capacidade de armazenar as instruções, sendo uma grande máquina de executar rapidamente cálculos complexos; para cálculos que exigissem o uso de resultados intermediários, era necessário a intervenção humana. Assim, von Neumann e seus colegas John Mauchly e Presper Eckert conceberam a ideia inovadora de uma máquina que armazenasse um conjunto de instruções de forma que cálculos feitos um após o outro, em sequência, com ou sem repetição de operações e com ou sem avaliação de condicionantes, pudessem ser executados de forma autônoma. Até então, para operar um computador era necessário a máquina de calcular – que era o próprio computador – e também um operador humano que ordenava as instruções uma a uma. A partir da ideia concebida pelos inventores, os computadores passaram a comportar instruções de cálculo neles mesmos, substituindo a necessidade de intervenção humana a cada nova operação computacional. A ideia central deste invento é conhecida como Arquitetura de von Neumann (TURING, 2019, pp. 96-98).

A ideia básica da arquitetura de von Neumann continua válida até os dias de hoje, tendo sofrido evoluções técnicas como a Arquitetura de Harvard. Na época daquela

invenção, as instruções para efetuar os cálculos – o que se denomina programa de computador – e os próprios dados de entrada e de saída, que são os operandos e os resultados, estavam localizados na mesma instalação física. Com o advento das redes de computadores, ocorreu o espalhamento tanto dos programas de computador comunicantes quanto dos dados a serem computados. Passa-se a tratar de uma arquitetura distribuída: os dados podem estar localizados em um ponto remoto daquele onde são executados os cálculos sobre esses mesmos dados. O que viabiliza essa operação é a rede de interconexão entre os componentes, que une as partes que estão distribuídas em unidades distintas. Esta arquitetura distribuída é a que fundamenta o uso da atual expressão "computação em nuvem".

Assim, se as instruções computacionais que tratam dados pessoais forem executadas em território nacional, então é possível aplicar a lei geral de proteção de dados. Todavia, existe uma exceção à incidência da lei geral de proteção de dados quando os tratamentos de dados pessoais ocorrerem em território nacional. Esta exceção existe por força do § 2º do artigo *3º*: "[e]xcetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do *caput* do art. 4º". De acordo com o artigo *4º*, inciso IV, a LGPD não é aplicável quando os dados pessoais forem "provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei". Este dispositivo permite que se aplique outra legislação de nível compatível com o brasileiro naqueles casos em que os dados, vindos do exterior, são tratados no Brasil e não são compartilhados com agentes de tratamento brasileiros nem com outros países exceto o país de onde os dados vieram, se a lei de proteção de dados do país de origem dos dados for do mesmo nível da legislação pátria (BRASIL, 2018). Neste ponto, quanto ao fluxo transfronteiriço de dados, o Brasil adotou o "modelo geográfico", ao valorizar mais o arcabouço normativo do outro país, em detrimento do "modelo de responsabilidade", que privilegia a *accountability* e a assunção de responsabilidades pelas partes (DONEDA *et. al.,* 2021, Cap. 15, item 2.2).

A segunda possibilidade "geográfica" que permite a aplicação da LGPD é ocorre desde que "a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional" (BRASIL, 2018). Assim, se bens ou serviços forem apenas ofertados, ou ainda

efetivamente prestados ou fornecidos em território nacional, então a LGPD pode ser aplicada. Note-se que a simples oferta de bens ou de serviços – ainda que sem a efetiva prestação destes serviços ou fornecimento de tais bens – implica a incidência da lei de proteção de dados brasileira, desde que a oferta, a prestação ou o fornecimento aconteçam em território nacional. Neste caso, aplica-se a lei mesmo se o agente que quem promove, oferta ou fornece for estrangeiro, e ainda que os dados estejam fora do Brasil, e mesmo que a própria atividade de tratamento de dados pessoais ocorra em outro país. Este caso permite a aplicabilidade da lei mesmo quando o ciclo de vida de tratamento de dados inicia no Brasil e continua ou se encerra em outro país, valendo-se de operações de tratamento que transportam os dados, como a transferência, a distribuição, a transmissão, a comunicação, a difusão e outros. Ainda neste caso, a lei brasileira deve ser observada. Este é um dos argumentos relevantes para que o tratamento de dados pessoais regido pela LGPD se dê no âmbito de relações entre controladores, co-controladores e operadores de dados pessoais que estejam localizados em países "que proporcionem grau de proteção de dados pessoais adequado", nos termos do artigo 33, inciso I da mesma lei (BRASIL, 2018).

Ainda na segunda possibilidade de incidência da lei de proteção de dados em função do aspecto geográfico, está a situação de tratamento de dados das pessoas localizadas em território nacional. Ou seja, basta a pessoa estar geograficamente presente na circunscrição territorial brasileira para que a lei brasileira de proteção de dados seja aplicada quando os dados pessoais desta pessoa forem tratados.

A terceira possibilidade de incidência da LGPD em função do aspecto geográfico existe para os casos em que "os dados pessoais objeto do tratamento tenham sido coletados no território nacional". Nesta situação, a lei usou o termo "coletados" para indicar que há aplicação da norma brasileira quando o ciclo de vida dos dados pessoais simplesmente iniciar no Brasil. Coleta é uma das formas de tratamento indicadas no rol do artigo *5º*, inciso X. Haverá incidência da lei de proteção de dados brasileira quando formas de tratamento originárias, tais como a coleta, a produção, a recepção, o acesso, o recebimento iniciarem no país. Usando interpretação teleológica, o objetivo do disposto neste artigo é o de tutelar todos os casos em que os dados pessoais transitem, em território nacional, da própria pessoa do titular de dados para o controlador, ou ainda quando o agente exercer o controle ou operar tais dados pela primeira vez em território nacional. O § 1º do mesmo artigo *3º* ainda define um critério temporal para identificar a incidência da norma brasileira: o titular dos dados deve estar em território brasileiro no mesmo tempo

em que a coleta ocorrer, isto é, quando iniciar o ciclo de vida de tratamento de dado pessoal (BRASIL, 2018).

A transparência sobre aspectos de localização geográfica no tratamento de dados pessoais deve ocorrer também em função da portabilidade de dados pessoais prevista no artigo 11, § 4º, inciso I da LGPD, pois há modificação do controlador, com possibilidade de alteração da localização de onde os dados pessoais estão ou de onde é realizado o tratamento respectivo (BRASIL, 2018). Sendo assim, o controlador para quem os dados são destinados na operação de portabilidade também deve ser transparente quanto ao tratamento de dados que realizar.

Ainda, deve haver transparência sobre a possibilidade de transferência internacional de dados, tais como os casos descritos no artigo 33 da LGPD. O inciso VIII deste artigo estabelece de forma explícita que o titular deve ser informado previamente, sobre a transferência ou compartilhamento internacional, quando o tratamento de dados ocorrer com base no consentimento: "quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades" (BRASIL, 2018). Este dispositivo ainda exige que a a informação ao titular dê ênfase ao caráter internacional, evidenciando a operação de tratamento que tiver pretensões internacionais (BRASIL, 2018).

A transparência, além disto, tem um elemento de restrição: deve respeitar o segredo comercial e industrial dos negócios, sendo necessário então contrabalançar o sigilo necessário à preservação das informações confidenciais que dão condições aos negócios competirem no mercado, de um lado, e o dever de apresentar as condições de tratamento de dados, de outro lado (BRASIL, 2018). Não se pode, então, de maneira irracional, dar transparência ao tratamento de dados pessoais em detrimento de segredos comerciais e industriais, sem qualquer critério. Tampouco se pode negligenciar o princípio da transparência sobre as formas de tratamento de dados e sobre quem as exerce, com justificativa simplista de proteção de segredo comercial ou industrial. É necessário, então, haver adequação para atender aos interesses que existam no caso concreto. Seria possível, neste caso, aplicar um teste de proporcionalidade, de forma análoga àquele afeito ao tratamento de dados pessoais com fundamento no legítimo interesse.

3.1.3 Elementos complementares de transparência

Após o inciso VI do artigo *6º*, o próximo dispositivo legal que menciona transparência é o artigo *9º*, § 1º. O *caput* deste artigo define que o "titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva", mencionando de forma genérica "outras características previstas em regulamentação para o atendimento do princípio do livre acesso", e então indica os assuntos sobre os quais as informações deverão ser apresentadas: "finalidade específica do tratamento", "forma e duração do tratamento", "identificação do controlador", "informações de contato do controlador", informações sobre o "uso compartilhado de dados pelo controlador", "responsabilidades dos agentes que realizarão o tratamento" e "direitos do titular, com menção explícita aos direitos contidos no art. 18" (BRASIL, 2018) Neste ponto, é de salientar o tratamento diferenciado prestado aos agentes de pequeno porte do Anexo I da Resolução CD/ANPD no. 2 de 2022, que é o Regulamento de aplicação da LGPD aos agentes de tratamento de pequeno porte. Tal diploma estabelece normas infralegais, dentre outras, sobre o *caput* do artigo 9º e o artigo 18, § 5º da LGPD, dispondo no artigo 7º sobre a forma a ser adotada pelos controladores de pequeno porte para "atender às requisições dos titulares em conformidade com o disposto nos arts. 9º e 18 da LGPD, por meio: I – eletrônico; II – impresso; ou III – qualquer outro que assegure os direitos previstos na LGPD e o acesso facilitado às informações pelos titulares" (BRASIL, 2022a). Observe-se que o regulamento flexibiliza o meio utilizado para atender ao princípio do livre acesso, e assim atender também à transparência. É coerente que, mesmo para agentes de pequeno porte, o tratamento de dados pessoais realizado pelos respectivos *websites* seja realizado eletronicamente, utilizando o mesmo meio, porém isto não foi objeto da presente resolução em tela.

O *caput* do artigo 9º refere-se ao acesso facilitado, que já foi analisado anteriormente, e explicita que este é um direito do titular de dados pessoais. O titular de dados pessoais, de acordo com a dogmática da LGPD, é a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (BRASIL, 2018). Não resta dúvida de que o direito de acesso tem base no princípio da transparência. O princípio da transparência serve de fundamento ontológico do direito de acesso (SOMBRA, 2019, p. 174). Assim, é possível afirmar que o direito de acesso se apoia também no princípio da transparência, e que é elemento que contribui na formação da autodeterminação informativa (SOMBRA, 2019, p. 173). O direito de acesso não é exatamente elemento constituinte da transparência, mas também nele fundamenta a sua existência. Na

continuidade, o *caput* caracteriza como "clara, adequada e ostensiva" a forma de apresentação das informações sobre o tratamento. Como o elemento de clareza para a transparência já foi analisado, resta avaliar os elementos "adequada" e "ostensiva".

A forma "adequada" de disponibilização da informação é um tanto subjetiva de ser avaliada, porém é elemento formador da transparência. Este é um critério qualitativo, assim como a clareza e a ostensividade (BIONI, 2019, p. 194). Apesar de o termo "adequada" ser distinto do princípio da adequação, é possível usar alguma analogia. Ser adequado é ser razoável, é ser proporcional, é guardar compatibilidade entre meios e fins. Assim, apresentar informações sobre tratamento de dados usando uma forma adequada é apresentar tais informações usando meios compatíveis com os fins almejados. Como o objetivo de apresentar a informação é levar as informações sobre tratamento de dados ao indivíduo, então fazê-lo de forma adequada é lançar mão de meios que efetivamente entreguem a informação ao titular. Ter forma adequada é se amoldar à situação concreta, atingindo o objetivo de realmente informar, numa sinergia entre todos os demais elementos de transparência contribuindo para que se alcance a concretização desta.

A forma "ostensiva" que deve tomar a apresentação das informações sobre tratamento é um elemento de transparência que abrange tanto componentes visuais quanto componentes comportamentais. A informação ostensiva é expressa, é clara, é fácil de ser identificada, é rapidamente notada. O emprego correto dos elementos visuais, conforme analisados anteriormente, é fundamental para a ostensividade. Assim, os avisos contendo informações sobre tratamento devem ter a capacidade de chamar a atenção da pessoa, devem estar evidenciados com sobreposição a outros de menor relevância, em busca da maior transparência possível. As comunicações ostensivas são extremamente aparentes, são manifestas. Não se trata de aplicar padrões exagerados, mas sim também de usar do elemento de adequação para que a ostensividade presente seja suficiente ao caso. Outro ponto importante da ostensividade é o componente comportamental. Os comunicados que atendem à transparência devem impor caminhos necessários ao indivíduo, exigindo deles certas ações, tornando-se indispensáveis à continuidade da interação que estiver sendo realizada. Os informes devem atuar de forma compulsória, devem ser imprescindíveis para o andamento das tarefas. O comportamento imperioso obtido com a ostensividade revela-se como garantia tanto da pessoa natural quanto do controlador de dados, porquanto permite o registro de entrega da informação em busca da transparência, contribuindo assim com a formação de registros de captura de consentimento e de cumprimento do princípio da transparência.

As "outras características previstas em regulamentação para o atendimento do princípio do livre acesso" (BRASIL, 2018), ainda no *caput* do artigo *9º*, caracterizam uma norma de eficácia limitada, porquanto dependem de regulamentação posterior para ter eficácia plena. Mesmo assim, tais características são elementos que devem ser considerados como parte da transparência.

O seguinte elemento de transparência é a "finalidade específica do tratamento" do artigo *9º*, inciso I (BRASIL, 2018). Este elemento se funda no princípio da finalidade, que é a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (BRASIL, 2018). A menção às possíveis hipóteses legais do artigo *7º* também atende à transparência da finalidade específica. A especificação da finalidade, ademais, deve ser informada de forma a não deixar dúvidas quanto ao tratamento, relacionando-se com os elementos de clareza e precisão da informação. Assim, deve ser informado o fim específico, evitando ater-se apenas a menções como "finalidade de atender ao legítimo interesse do titular", ou "finalidade de melhorar a experiência do usuário". É preciso ser preciso, é preciso explicitar e especificar que o tratamento de dados pessoais pode ser utilizado, por exemplo, para fins de publicidade direcionada, para apresentar opções de produtos que estejam mais de acordo com o perfil da pessoa, ou para exibir corretamente os elementos gráficos de *website*. Conforme o princípio da finalidade, os propósitos do tratamento devem ser "legítimos, específicos, explícitos e informados ao titular". O elemento de finalidade específica do tratamento, portanto, deve ser legítimo, isto é, deve ser ato lícito, e também deve ser explícito por ser claro e expresso.

3.2 Políticas de privacidade na legislação brasileira: LGPD, Marco Civil da *Internet* e o caso do Whatsapp

A LGPD faz referência a boas práticas de governança no artigo 50, sendo possível posicionar a política de privacidade nestas boas práticas. A política de privacidade é um instrumento usado a favor da transparência e que apresenta ao titular de dados pessoais os diversos aspectos do tratamento de dados realizado pelos controladores e respectivos operadores. Na esteira do artigo 50, o § 2º, inciso I, alínea “e” recomenda – aos controladores e operadores – que o programa de governança em privacidade “tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular” (BRASIL, 2018). O

§ 3º do mesmo artigo arremata ao final definindo que "[a]s regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional" (BRASIL, 2018).

Conforme visto acima, a lei sugere que o princípio da transparência seja utilizado para criar uma relação de confiança entre os agentes de tratamento e os titulares, assim como o princípio do livre acesso, que é referido pelo mesmo artigo 50 quanto à disponibilização de formas para que o titular possa exercer seus direitos. Ao final, o dispositivo legal ainda reforça o dever de informação, contido no princípio da transparência, por meio do comando de publicidade e atualização periódica das boas práticas de governança. Neste ponto, entende-se pelos motivos aqui expostos que está incluída a necessidade de publicação e atualização das políticas de privacidade.

O Marco Civil da *Internet* trata sobre transparência no artigo 7º, inciso XI, prescrevendo que a lei assegura o direito à "publicidade e clareza de eventuais políticas de uso dos provedores de conexão à *Internet* e de aplicações de *Internet*" (BRASIL, 2014). No caso, a lei utilizou o termo "políticas de uso" para indicar os termos de uso usualmente apresentados pelos *websites*. Os termos de uso são distintos da política de privacidade, pois aqueles estabelecem condições de prestação do serviço específico do *website* (DE LIMA, 2014, p. 10); as políticas de privacidade, por seu turno, são relacionadas aos aspectos de privacidade e proteção de dados tal como exposto anteriormente.

De acordo com Cíntia Rosa Pereira de Lima, o conjunto destes documentos é denominado *browse-wrap agreements*. A autora afirma que não é possível considerá-los como contratos de adesão, porquanto lhes falta o cumprimento do dever de transparência e de coleta da autorização por parte do usuário (DE LIMA, 2009, p. 628). A mesma autora afirma que, se forem respeitados os elementos contratuais de existência, validade e eficácia mediante o princípio da transparência, esses termos de uso podem ser considerados condições gerais dos contratos, e assim ser incluídos no rol de cláusulas contratuais (DE LIMA, 2014, p. 11). Para Kamantauskas, nas situações corriqueiras de *browse-wrap* não é possível a formação de contratos pois a parte pretensamente contratante não é informada sobre os termos do contrato, porém existe a possibilidade da sua formação se o dever de informação for efetivamente cumprido (KAMANTAUSKAS, 2015, p. 79). Bruno Bioni, por sua vez, não tem opinião formada sobre a classificação de políticas de privacidade como contratos de adesão, e considera que há divergência doutrinária acerca da possibilidade de considerar as políticas de privacidade como sendo

contratos de adesão, citando que Cláudia Lima Marques entende que são contratos de adesão e Orlando Gomes com posição contrária à classificação como contrato de adesão (BIONI, 2019, pp. 170-171). Aquele autor, porém, considera que a tutela da privacidade por meio da invocação das garantias de natureza consumerista deve ser feita apenas subsidiariamente, devendo prevalecer a o exercício da defesa dos direitos do indivíduo por meio da estrutura regulatória de proteção de dados pessoais (BIONI, 2019, pp. 173-174).

Apesar das nuances doutrinárias sobre considerar se as políticas de privacidade são ou não contratos, reafirma-se que tais documentos compõem o programa de governança em privacidade, e assim são documentos fundamentais aos agentes de tratamento de dados para o exercício do dever de informar, e são instrumentos capazes de dar transparência aos titulares de dados pessoais e, em último caso, promover a relação de confiança entre os participantes das relações jurídicas.

No âmbito brasileiro, a ANPD publicou a Nota Técnica no. 49/2022/CGF/ANPD, por meio da qual deu publicidade ao conteúdo do processo administrativo 00261.000012/2021-04, cujo objeto abrangia a adequação das Políticas de Privacidade e dos Termos de Serviço do WhatsApp (BRASIL, 2022c, p. 1). O processo fiscalizatório da ANPD foi motivado pelo fato de o WhatsApp ter alterado os termos de uso da sua plataforma de comunicação, após exigir a partir de janeiro de 2021 que os usuários aceitassem os termos de uso e a política de privacidade de forma integral. No caso apresentado, a Autoridade Nacional de Proteção de Dados fez uma série de recomendações para que o WhatsApp observasse a norma brasileira de proteção de dados, por meio do atendimento das disposições da Nota Técnica 02/2021/CGTP/ANPD.

3.3 O Guia orientativo sobre *cookies* e o Ofício da ANPD ao Governo Federal sobre os avisos de *cookies*

A ANPD fez recomendações ao Governo Federal sobre as medidas a serem adotadas nos *websites* respectivos. Estas recomendações constavam no portal da ANPD, porém não estão mais acessíveis diretamente através do *link* https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-emite-recomendacoes-para-adequacao-da-pratica-de-coleta-de-*cookies*-do-portal-gov.br. Contudo, a pesquisa pelo assunto em outros *websites* revelou que o conteúdo das recomendações da ANPD se aproximava das diretrizes da

União Europeia em relação ao tratamento dos *cookies*, indicando a necessidade de exibir avisos de *cookies* em dois níveis.

A recomendação indica que, no *banner* de primeiro nível, deve haver botão visivelmente adequado para rejeitar *cookies* não necessários e que se aplique o padrão *opt-in*. No segundo nível: devem ser informadas as bases legais conforme a classificação dos *cookies* que também precisa ser feita; deve haver consentimento específico conforme os tipos de *cookies*; deve haver botão para rejeitar todos os *cookies* não necessários.

O padrão adequado para a obtenção do consentimento é o *opt-in*, pois o ordenamento jurídico brasileiro entende que o consentimento do titular não pode ser presumido, pois a manifestação deve ser feita de forma livre, e também porque o consentimento deve ser expresso, e não tácito, isto é, deve haver manifestação ativa por parte do titular. O tratamento de dados com base no legítimo interesse deve ser feito para os casos em que for necessário para atender ao legítimo interesse do controlador ou de terceiro, respeitadas as legítimas expectativas do titular. No caso dos *cookies*, há *cookies* que são necessários para que a funcionalidade dos *websites* seja exercida de forma segura e apropriada, tanto para o controlador ou terceiro, quanto para o titular dos dados. A classificação dos *cookies*, distinguindo entre quais são necessários e quais são facultativos ao bom funcionamento dos *websites*, é fundamental para exercitar a transparência e permitir que o titular exerça sua autonomia.

Como já mencionado, em 2022 a ANPD publicou um guia com orientações sobre o emprego de *cookies* em *website*s e aplicativos, enfocando na estrutura de apresentação dos avisos de *cookies* (BRASIL, 2022d). Tal documento, percebe-se, se assemelha à estrutura dos avisos de *cookies* implementados na União Europeia, todavia é desprovido de força normativa, sendo apenas – como o próprio nome diz – orientativo.

3.4 E-Privacy Directive

A Diretiva 2002/58/CE, também conhecida como *E-Privacy Directive*, ou Lei dos *Cookies*, é a norma jurídica em vigor na União Europeia que trata sobre privacidade e comunicações eletrônicas. A Diretiva 2009/136/CE – produzida sete anos mais tarde – alterou três normas europeias, dentre elas a Diretiva 2002/58/EC, no intuito de reforçar a proteção dos dados pessoais. A primeira redação da Diretiva de 2002 permitia o uso da lógica do *opt-out* (POULLET, 2010, p. 24), segundo a qual o consentimento do usuário poderia ser presumido, ou então indicado por padrão. A redação original também não

deixava claro se os *cookies* poderiam ser considerados dados pessoais (POULLET, 2010, p. 14).

É interessante notar que, na Europa, existe uma diferença entre Diretivas e Regulamentos: enquanto Regulamentos são normas que possuem eficácia plena, as Diretivas são ordens de eficácia limitada porquanto dependem de internalização por parte de cada Estado Membro da União Europeia, ou seja, as Diretivas são normas mais abstratas a partir das quais as legislações internas devem elaborar seus próprios ordenamentos (PALHARES, 2020, Cap. 1, item 4).

Assim, como atualmente a lei dos *cookies* é constituída por uma Diretiva, cada Estado Membro precisa criar sua legislação interna. Com a vigência da referida lei, o emprego de avisos de *cookies* se proliferou pelos *websites* da União, sendo que em muitos casos entendia-se que o consentimento seria válido mesmo que fosse dado de forma implícita, por exemplo se o usuário continuasse a navegar pelo *website* (PALHARES, 2020, Cap. 1, item 4), numa lógica de *opt-out* por padrão.

A redação proposta pela Diretiva de 2009 *supra* alterou o artigo 5º, nº 3 para adotar o padrão *opt-in*, dando a seguinte redação e que ainda vigora:

> Os Estados Membros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos termos da Directiva 95/46/CE, nomeadamente sobre os objectivos do processamento. Tal não impede o armazenamento técnico ou o acesso que tenha como única finalidade efectuar a transmissão de uma comunicação através de uma rede de comunicações electrónicas, ou que seja estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador. (UNIÃO EUROPEIA, 2009).

Na Diretiva de 2009, o Considerando 66 – ou *Recital* 66 – traduz a intenção do legislador em regular mais detalhadamente a operacionalização do artigo 5(3) acima transcrito: ante a possibilidade de que terceiros armazenem ou acessem informações nos terminais de usuários, é necessário que os cidadãos sejam informados de forma efetiva sobre a possibilidade de tais ocorrências, e que a transparência seja implementada de maneira simples e por fim que o consentimento seja obtido de forma adequada (UNIÃO EUROPEIA, 2009). A exceção a esta norma reside nas situações em que tais armazenamentos ou acessos sejam feitos de forma compulsória, com base na estrita necessidade para o funcionamento apropriado dos serviços (UNIÃO EUROPEIA, 2009).

A proposta legislativa 2017/0003, também chamada de *ePrivacy Regulation* (ETTELDORF, 2020, p. 567) está em apreciação pelo Parlamento Europeu desde o ano de 2017, e após a sua vigência ela revogará a Diretiva 2002/58/CE. Pretende-se atualizar

a *E-Privacy Directive* pela introdução da *ePrivacy Regulation* no intuito de adaptar as normas aos contextos atuais. Esta atualização ainda não aconteceu, por divergências entre os legisladores – a Comissão, o Conselho e o Parlamento – quanto às regras sobre o armazenamento de *cookies* nos terminais dos cidadãos, e quanto ao uso dos dados e dos metadados no âmbito deste processamento (ETTELDORF, 2020, p. 567).

O Parlamento Europeu tinha a pretensão de aprovar a nova norma que revisa a Diretiva E-*Privacy* de 2002, porém isto ainda não aconteceu devido a conflitos de opiniões entre a Comissão, o Conselho e o Parlamento europeus. A lide se concentra nos artigos 5º a 10 da nova proposta de Regulamento. Além da atualização do conceito de dados pessoais e metadados, uma das questões em discussão se refere à aplicação do legítimo interesse para atender a questões técnicas de desempenho, manutenção e segurança das comunicações eletrônicas (ETTELDORF, 2020, p. 568). Outro ponto debate o emprego de *cookie walls*, que permitiriam aos *websites* conceder acesso aos seus serviços somente se os usuários aceitassem o uso de certos *cookies* (ETTELDORF, 2020, p. 569). Há discussão também sobre as soluções técnicas possíveis para a concessão e o registro – evidência – do consentimento (ETTELDORF, 2020, p. 569). A última questão importante trata sobre a proposta da Comissão para que o mecanismo de gestão do consentimento seja embutido diretamente nos navegadores de *Internet*, que atuariam como guardiões dos dados dos seus usuários, e ainda para que todo e qualquer sistema de *software* comercializado permitam que os usuários escolham se querem ou não que terceiros armazenem ou acessem dados nos seus equipamentos (ETTELDORF, 2020, p. 569). Este último item afetaria de forma negativa principalmente as plataformas – que trabalham e lucram na economia movida a dados – e os próprios *websites* (ETTELDORF, 2020, p. 569) – cujas receitas são advindas também de anúncios publicitários direcionados, assim como os produtores de *software*s e aplicativos de celular que oferecem seus produtos gratuitamente e também obtêm receitas publicitárias. À parte da discussão sobre efeitos negativos para a ampla indústria que lucra com o comércio de dados pessoais, a possibilidade de atribuir a gestão de consentimento para os navegadores de *Internet* teria o potencial de aumentar a concentração de mercado destes agentes: Google, Apple e Microsoft já têm seus navegadores, e a recente indústria que se formou em torno das soluções de gestão de consentimento também seria prejudicada.

A sentença do Tribunal de Justiça da União Europeia no caso C-673/17 Planet49 pode acelerar a aprovação da *ePrivacy Regulation* (DONEDA, *et. al.,* 2021, Cap. 5, item 1). A Planet49, responsável por serviços de loterias, apresentava um formulário para

preenchimento pelos seus clientes com duas pretensas opções que já vinham pré-marcadas no primeiro nível do formulário: autorizar tratamento de dados para fins de marketing, e autorizar armazenamento e acesso de *cookies* em seus dispositivos. Para apostar nas loterias, os usuários eram obrigados a autorizar o tratamento de seus dados para fins de marketing, mas poderiam participar mesmo se desmarcassem a autorização para uso de *cookies*. Se a opção de autorização fosse mantida pré-marcada, a Planet49 poderia compartilhar os dados dos clientes com até 30 dos 57 patrocinadores e parceiros de negócio, a não ser que o usuário entrasse no segundo nível do formulário e desmarcasse aqueles agentes com quem não gostaria de fazer o compartilhamento (JABLONOWSKA; MICHALOWICZ, 2020, p. 138). A Corte Europeia analisou o caso e decidiu, à luz dos artigos 2(f) e 5(3) da *E-Privacy Directive*, dois pontos relevantes.

O primeiro ponto da decisão comentada revela que o consentimento não é válido quando o usuário precisa desmarcar uma *checkbox* que já vem pré-selecionada. Ou seja, decidiu que o *opt-out* não é válido para o tratamento de dados com base no consentimento, argumentando que, para aquela jurisdição, o consentimento deve ser: livre específico, informado e inequívoco (JABLONOWSKA; MICHALOWICZ, 2020, p. 139). Aquele Tribunal ainda justificou que a legislação europeia requer que o usuário se expresse ativamente para fornecer a autorização – consentimento ativo, e que muito provavelmente o usuário não tomará ciência nem se procurará ler detalhes sobre o tratamento de dados se houver uma caixa de seleção pré-marcada (JABLONOWSKA; MICHALOWICZ, 2020, p. 139).

O segundo ponto importante da decisão sobre o caso da Planet49 refere-se aos tipos de dados que podem ser objeto de tratamento. Para a Corte, o consentimento é inválido se obtido pelo padrão *opt-out*, com autorizações pré-selecionadas, e continua havendo ilicitude mesmo se os dados armazenados ou acessados no dispositivo do usuário não forem dados pessoais (JABLONOWSKA; MICHALOWICZ, 2020, p. 139).

É importante salientar, ainda, que a *E-Privacy Directive* de 2002 apenas faz distinção entre dois tipos de *cookies*: aqueles que são necessários para efetivar a comunicação e o adequado funcionamento dos serviços, e todos os demais *cookies*. A ICC, Câmara Internacional de Comércio do Reino Unido, publicou um guia sobre os *cookies* (BOLLINGER, 2021, p. 14), no qual sugeriu quatro categorias: *cookies* estritamente necessários, *cookies* de desempenho, *cookies* de funcionalidade e *cookies* de publicidade (ICC, 2012). Este é um exemplo de classificação possível para os *cookies*. Para a classificação dos *cookies*, o que é relevante saber é que há no mínimo duas

categorias: os necessários e os facultativos ou opcionais. Os *cookies* necessários são os *cookies* de sessão, que têm a finalidade de manter o estado entre as requisições feitas pelos usuários e as respostas entregues pelo *website*, controlando assim as transações e as janelas de início e fim de atividades em ambientes que precisem de controle interação entre os participantes da sessão de uso. Esses *cookies* necessários, ou estritamente necessários, representam exceção ao consentimento, isto é, a base legal para seu emprego nos *websites* é o legítimo interesse. Os *cookies* facultativos, ou opcionais, não são necessários para o funcionamento adequado dos sistemas, pois têm apenas funcionalidades adicionais, finalidades distintas daquelas básicas do serviço prestado pelo *website*. A classificação da ICC, conforme acima descrita, é utilizada como um padrão de fato pela indústria de tecnologia para agrupar os *cookies* em diferentes finalidades, todas facultativas, exceto a categoria dos *cookies* estritamente necessários. Assim, as categorias de *cookies* de desempenho, de funcionalidade e de publicidade são todas opcionais. Para armazenamento e acesso dos *cookies* categorizados nessas classes opcionais, é exigido o consentimento do titular.

Quanto ao Brasil, inicialmente, cumpre salientar que não há menção direta ao termo *cookie* na lei geral de proteção de dados brasileira, tampouco o Marco Civil da *Internet*, Lei 12.965/2014, menciona *cookie* ou assemelhado. Todavia, o regulamento do Marco Civil da *Internet*, constituído pelo Decreto Federal 8.771/2016, ao firmar o que é dado pessoal para os fins a que se destina tal decreto, define que dado pessoal é o "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa" (BRASIL, 2016). Ora, os *cookies* servem para, entre outras finalidades, identificar as pessoas no ambiente *online*. Assim, pode-se concluir em primeiro lugar que *cookie* é um tipo de identificador eletrônico. Em segundo lugar, também é possível concluir que *cookie* é um dado pessoal, pois carrega em seu conteúdo as informações capazes de identificar um indivíduo na *Internet*, e também porque tais informações sobre a pessoa podem caracterizá-la, sendo possível ainda que os *cookies* portem dados pessoais sensíveis, além de atributos comportamentais que podem ser objeto de análise de preferências pessoais de diversas ordens, por meio da estipulação do perfil socioeconômico da pessoa, ou ainda suas preferências musicais, políticas, religiosas e tantas mais.

O Regulamento Geral de Proteção de Dados Europeu, que foi utilizado como referência para a elaboração da LGPD brasileira, faz referência a *cookies* apenas uma vez em todo o texto legal, no Considerando 30:

> As pessoas singulares podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (*Internet Protocol*) ou testemunhos de conexão (*cookie*) ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares. (UNIÃO EUROPEIA, 2018).

Como existe a possibilidade de armazenarem informações relacionadas a pessoa natural identificada ou identificável, considera-se que os *cookies* são dados pessoais (PALHARES, 2020, Cap. 1, item 3) pois armazenam conteúdo que pode revelar atributos das pessoas que operam os dispositivos que se comunicam utilizando o protocolo HTTP. Ademais, as informações carreadas nos *cookies* podem ser consideradas dados pessoais tanto pelo seu conteúdo, quanto pela sua finalidade e ainda pelas consequências advindas do tratamento sobre elas realizado (POULLET, 2010, p. 14). Os *cookies* podem ser considerados dados pessoais por conta da possibilidade de impactarem as decisões ou os direitos dos indivíduos, mesmo que esses indivíduos nunca possam ser identificados; basta que o tratamento de determinada pessoa seja realizado um pouco diferente das demais, em função de características relacionadas a ela, para que seja possível entender que tais características, embutidas nos *cookies*, são dados pessoais (UNIÃO EUROPEIA, 2007, p. 11)

3.5 A proteção de dados pessoais e o consumidor

Com base na previsão do artigo 5°, inciso XXXII da Constituição Federal de 1988 que afirma que "o Estado promoverá, na forma da lei, a defesa do consumidor" (BRASIL, 1988), a doutrina jurídica entende que o sistema protetivo dos consumidores fundamenta a ideia de que o Código de Defesa do Consumidor (CDC) é norma principiológica, prevalecendo sobre outras normas setoriais (TARTUCE, 2022, p. 8). Assim, e sendo classificada como norma que atinge os direitos de terceira geração, o Código de Defesa do Consumidor é dotado de eficácia supralegal na pirâmide de Hans Kelsen, ocupando posição intermediária entre a Constituição Federal e as leis ordinárias (TARTUCE, 2022, pp. 8-9).

Os direitos relacionados ao mundo digital estão classificados como direitos de 5a geração (TARTUCE, 2022, p. 8), assim o Direito Digital pode ser visto como representante da geração mais nova de direitos; isto tanto é verdade que, apenas recentemente, a Emenda Constitucional 115 de 2022 incorporou à Constituição Federal brasileira o direito fundamental à proteção dos dados pessoais no artigo 5°, inciso LXXIX: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (BRASIL, 1988).

Tanto a defesa do consumidor quanto a proteção dos dados pessoais têm guarida constitucional, é verdade, e ambos são instrumentos de proteção da parte vulnerável, guardando forte correspondência entre seus princípios e abstrações. Uma abstração comum entre os dois diplomas é o objetivo almejado de defesa ou proteção; outra é a noção de vulnerabilidade, dada as diferenças de poder entre as partes nas relações de consumo e nas relações que envolvem tratamento de dados, esta última decorrente da assimetria de informação. Pelo lado dos princípios, há em comum por exemplo a boa fé e a transparência.

O Código de Defesa do Consumidor tem caráter multidisciplinar (GRINOVER *et. al.,* 2019, p. 73), mantendo assim relação com a proteção de dados pessoais dos consumidores. Estes são vistos como a parte mais fraca da relação jurídica de consumo, que se dá pela circulação de produtos e serviços com o uso dos instrumentos do crédito e do marketing (GRINOVER *et. al.,* 2019, p. 63); esta tônica de diferenças de forças também permeia a lei geral de proteção de dados, na medida em que aquele diploma introduz no ordenamento jurídico brasileiro algumas ferramentas, como princípios, direitos e obrigações, para contrabalançar a assimetria de poder existente entre os titulares e os agentes de tratamento de dados pessoais.

A política nacional de relações de consumo trata da harmonia nas relações de consumo, tendo o consumidor como parte vulnerável e assim merecedor de "um tratamento desigual para partes manifestamente desiguais" (GRINOVER *et. al.,* 2019, p. 70). Assim, a vulnerabilidade está para as relações consumeristas no CDC assim como a assimetria de poder e de informação está para as relações entre titulares e agentes de tratamento na LGPD.

O Código de Defesa do Consumidor é mais importante pela sua perspectiva e por suas diretrizes na defesa do consumidor, do que propriamente pelo esgotamento da matéria e previsão de todos os possíveis casos (GRINOVER *et. al.,* 2019, p. 72), assim

como a Lei Geral de Proteção de Dados, que é uma lei de princípios e que indica as linhas gerais sobre o respectivo assunto.

Para o CDC, existe relação de consumo quando há destinação final e quando a vulnerabilidade está presente; os consumidores submetem-se ao poder dos fornecedores em uma relação desigual; o direito do consumidor abrange a pessoa natural e – em alguns casos - a pessoa jurídica no conceito de consumidor (GRINOVER *et. al.,* 2019, pp. 75-105). O CDC também equipara a coletividade de consumidores ao conceito de consumidor, quando não tomados individualmente, mas quando forem em número determinado ou indeterminado, e tiverem participado de relações de consumo; este ponto mira a universalidade dos consumidores, efetivos ou potenciais; nestes casos, dada a natureza indivisível dos interesses, a sua defesa ocorre por meios de tutela coletiva assim como pela atuação no campo dos interesses difusos e a todos aproveita (GRINOVER *et. al.,* 2019, pp. 105-106).

Relacionados ao tema desta pesquisa, colacionamos alguns dos direitos básicos do consumidor previstos no artigo 6º do CDC. O inciso I daquele artigo garante o direito à **proteção da segurança** do consumidor. Os arts. 8º e 9º definem que os fornecedores de serviços *online* que empreguem com componentes potencialmente maliciosos, ou que acarretem risco à segurança dos consumidores, devem "dar as informações necessárias" e informar "de maneira ostensiva e adequada" (BRASIL, 1990). Por exemplo, se no acesso ao *website* forem instalados rastreadores no computador do consumidor, pode ser introduzido risco à segurança por ataques de "roubo de sessão", por exemplo.

Segundo o inciso II do mesmo artigo, a garantia da "**liberdade de escolha e igualdade** nas contratações" também é um direito do consumidor. Este direito tem objetivo de proteger o consumidor por conta de sua vulnerabilidade. É relacionado ao princípio da equivalência negocial, segundo o qual as contratações devem ser realizadas em preconizando a igualdade. Além disso, a boa fé objetiva se aproxima da liberdade de escolha no atendimento ao dever de lealdade entre as partes (TARTUCE, 2022, p. 66). Ademais, o art. 4º, inc. I do Decreto 7.962/2013, que regulamenta o CDC sobre aspectos do comércio eletrônico, impõe que o prestador de serviço deve respeitar a liberdade de escolha do consumidor, antecipando as informações (BRASIL, 2013).

O direito à "**informação adequada e clara**" inclusive sobre os riscos, previsto no inciso III, fundamenta o dever anexo de informar, assim como propicia condições à liberdade de escolha (TARTUCE, 2022, p. 66). O art. 2º, incisos III e IV do Decreto 7.962/2013 também dispõe sobre a clareza das informações quanto ao serviço e respectivo

prestador: no que tangem as **principais características** do serviço, inclusive quanto à **segurança** do consumidor, e sobre **possíveis restrições** do serviço (BRASIL, 2013). Assim, no caso de avisos de *cookies*, é necessário informar o consumidor sobre o emprego de *cookies* **essenciais ou de sessão**, assim como os demais tipos; e também é preciso informar as restrições sobre fornecimento ou não de autorização do respectivo tratamento de dados. Também o Decreto 5,903/2006, que dispõe sobre "o direito básico do consumidor de obter informação adequada e clara sobre produtos e serviços" (BRASIL, 2006), regulamenta a discriminação de preços e estabelece critérios sobre a apresentação de informações aos consumidores, assim como define condutas infracionais a este direito básico do consumidor; dentre as práticas, estão o uso de letras e disposições textuais que dificultem a legibilidade, e a prestação de informações que deixem o indivíduo em dúvida sobre o objeto contratado.

O direito de ser informado também atua no sentido de inibir abusos e enganos promovidos por meio de publicidade, e de coibir "métodos comerciais **coercitivos** ou **desleais**, bem como contra **práticas e cláusulas abusivas ou impostas**" (BRASIL, 1990). O CDC, art. 6º, inc. V, também protege o consumidor quanto às **mudanças posteriores** de cláusulas contratuais – e pré-contratuais – "que estabeleçam prestações desproporcionais ou sua revisão em razão de fatos supervenientes que as tornem excessivamente onerosas" (BRASIL, 1990). É possível sustentar que há proteção contra a alteração das finalidades de uso dos dados pessoais sem comunicado e autorização respectiva, assim como alteração das políticas de privacidade, políticas de *cookies* e termos de uso de forma a aumentar ainda mais a assimetria de poder e informação em relação ao consumidor.

A responsabilidade do fornecedor por defeito nos serviços prestados ou nas respectivas informações é definido no art. 14 do CDC, segundo o qual a **responsabilidade civil** do fornecedor de serviços *online* é **objetiva**. Desta forma, ocorrendo defeito na prestação do serviço por questões de segurança advindos da própria plataforma dos *websites*, salvo as excludentes de culpabilidade, o prestador do serviço responde objetivamente, independentemente de culpa.

Da mesma forma, a responsabilidade prescinde do nexo causal quando houver deficiência no dever de informar, com base no mesmo art. 14, *caput*. Sendo assim, se a informação prestada não for adequada em informar dos riscos à privacidade na autorização de tratamento de dados, ou se não esclarecer sobre os cuidados de segurança

na fruição dos serviços, o fornecedor dos serviços *online* também responde de forma objetiva.

Mesmo que não seja celebrado efetivamente um contrato de serviço eletrônico ou de produto pela *Internet*, e ainda que a relação entre indivíduo e fornecedor fique apenas no nível pré-contratual conforme o CDC, art. 30 conjugado com o art. 48, se ocorrer a hipótese de violação de dados desse sujeito, ou ainda outro tipo de dano por questão de segurança ou falta de atendimento da **legítima expectativa** do indivíduo – conforme o CDC, art. 12, § 1°– ainda assim o responsável pelo serviço *online* responde pelo fato do serviço, pois as informações prestadas no pré-contrato **vinculam** o fornecedor, devido à possibilidade de equiparação do indivíduo a consumidor na relação aqui descrita. Isto se fundamenta também no art. 17: "[p]ara os efeitos desta Seção, equiparam-se aos consumidores todas as vítimas do evento" (BRASIL, 1990).

Para Cláudia Lima Marques, "[a] jurisprudência brasileira valorizou o dever de informar, sua origem na boa-fé e seus efeitos para determinar a prestação esperada" (MARQUES, 2019, p. 874). O dever de informar, como dever instrumental, anexo à prestação principal, é derivado do princípio da transparência e precisa carregar a informação com suas características já apresentadas no subcapítulo sobre este princípio. Na ótica do CDC, este dever se fundamenta principalmente no art. 31, segundo o qual as informações devem ser "corretas, clara, ostensivas e em língua portuguesa", e devem versar sobre os diversos aspectos do serviço (BRASIL, 1990).

A publicidade enganosa ou abusiva também é combatida pelo sistema de proteção do consumidor. O art. 37 do CDC versa sobre isto, e afirma a abusividade de publicidade que explore fraqueza ou induza o comportamento do consumidor de forma negativa (BRASIL, 1990). O artigo 39 do CDC traz ainda lista não exaustiva de práticas abusivas; algumas destas que têm relação com a presente pesquisa são: recusa de atendimento ao consumidor na medida de sua disponibilidade (inc. II), como no caso de emprego de *cookie walls* e avisos de *cookies* bloqueantes; fornecimento de serviço ao consumidor sem solicitação prévia, como no caso de instalação de rastreadores no dispositivo do usuário sem sua autorização (inc. III); abuso da vulnerabilidade do consumidor para "impingir-lhe seus produtos e serviços", como no caso de indução do comportamento do consumidor frente ao consentimento nos *banners* de *cookies* (inc. IV); "exigir do consumidor vantagem manifestamente excessiva" (inc. V), como no caso dos *cookie walls*, ou no emprego de outros *dark patterns* que influenciam as ações do usuário em prol apenas do controlador do *website*; executar serviços sem autorização expressa, como

no caso de práticas que envolvam consentimento tácito para tratamento de dados pessoais (inc. VI); fornecer serviço de *website* em desconformidade com normas legais e técnicas (inc. VIII) (BRASIL, 1990).

Ponto importante da defesa do consumidor quanto aos seus dados é o art. 43, § 2° do CDC, segundo o qual o consumidor deve ser informado sobre a abertura de cadastro com seus dados. Esta abertura de cadastro deve ser informada quando o consumidor não a solicitar, e ele deve ter acesso às respectivas informações, assim como tem o direito de saber das fontes que forneceram tais dados.

O Código de Defesa do Consumidor afirma no artigo 48 que **pré-contratos** e declarações de vontade têm força **vinculante** em relação ao fornecedor (BRASIL, 1990). O CDC traz as informações veiculadas em pré-contratos também para a obrigação contratual com o consumidor. Para Cláudia Lima Marques, "o CDC amplia a noção de oferta no art. 30, inclui todas as informações suficientemente precisas, mas, principalmente, regula a **fase pré-negocial** no art. 48 do Código" (MARQUES, 2019, p. 863). Assim, os avisos de *cookies* são exibidos durante o acesso do usuário ao *website*, e têm natureza de pré-contrato. Por exemplo, ao entrar em um *site* de cursos *online*, o indivíduo se depara com um *banner* de *cookies* (pré-contrato), e então realiza a compra de um curso *online* (contrato principal). Neste caso, o pré-contrato vincula o fornecedor para todos os efeitos.

A **nulidade** de cláusulas contratuais – e pré-contratuais, logicamente – é prevista no art. 51 do CDC, como as que não se coadunam com os princípios da boa fé e da equidade. O artigo 54, § 3º do CDC estabelece critérios para os **contratos de adesão**, indicando características de **ostensividade** e **legibilidade**; isto se aplica aos pré-contratos também, e assim os avisos de *cookies* que servem para informar e obter autorização do consumidor devem atender a esses preceitos. Outro ponto relevante da referida lei consumerista é o artigo 66, que comina **sanção penal** para **omissões relevantes** ou **afirmações enganosas** sobre aspectos dos serviços prestados.

3.5.1 Dados pessoais do consumidor *standard* e por equiparação

O CDC conceitua o consumidor no artigo 2º: "é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final". Este é o conceito de consumidor *standard*. O consumidor padrão é, assim, aquele que necessariamente realiza algum tipo de comércio ou contratação de serviço junto ao prestador de serviços ou

fornecedor de produtos. O referido dispositivo indica ainda que a aquisição ou uso do produto ou serviço deve ser feita no caráter de destinatário final; isto é, se o vínculo o objeto é apenas meio para atingir outro objetivo intermediário e não final, como a contratação de um serviço ou produto de meio para posterior entrega de um serviço ou produto final, então não se caracteriza relação de consumo. O objeto deve se esvair após a sua fruição, sem etapa posterior. Por fim, a pessoa contratante pode ser natural ou jurídica. Há discussão doutrinária acerca da caracterização de pessoa jurídica como consumidora, porém não será abordado neste trabalho, pois o foco da proteção de dados pessoais é na pessoa natural. E ainda para o objetivo desta pesquisa, deve-se olhar tanto para esta qualidade de consumidor *standard* quanto para aquele que se equipara a consumidor.

O artigo 29 do CDC introduz o conceito de consumidor por equiparação, ou consumidor *bystander*: "[p]ara os fins deste Capítulo e do seguinte, equiparam-se aos consumidores todas as pessoas determináveis ou não, expostas às práticas nele previstas". Grinover e outros afirmam não ser simples definir o que é prática comercial, mas fazem uma diferenciação desta com prática de produção – produzir algo – argumentando que a prática comercial acontece em momento distinto da produção, e exemplificam como sendo o *marketing* uma prática comercial (GRINOVER *et. al.,* 2019). Do conteúdo positivado nos Capítulos V e VI do CDC, contudo, depreende-se que possíveis práticas comerciais são: oferta, publicidade, práticas abusivas, cobrança de dívidas, cláusulas abusivas e contratos de adesão (BRASIL, 1990). Assim, a exibição de avisos de *cookies* poderia ser entendida como uma aplicação do conceito de prática comercial, por exemplo com objetivo de *marketing*, mas não limitado a este.

Enquanto para o consumidor *standard* a contratação do bem ou serviço já ocorreu ou esteja em vias de acontecer, apenas o fato de expor o indivíduo às práticas comerciais já é suficiente para equipará-lo à condição de consumidor – e classificá-lo então como consumidor *bystander* ou equiparado. Então, mesmo aquela pessoa que não tem vínculo contratual ativo ou sua expectativa no futuro próximo pode ser considerada como consumidora – por equiparação. Este ponto interessa a este estudo, pois muitos indivíduos que interagem com os *websites* não realizam necessariamente contratos de consumo, mas apenas visitam os respectivos endereços na *Internet*.

Para esta pesquisa, interessa o consumidor que é pessoa natural, determinado ou indeterminado, *standard* ou equiparado, pois é titular de dados pessoais, assim conjugando os conceitos do CDC e da LGPD.

3.5.2 O fornecedor de serviços *online*.

Feitas as considerações anteriores sobre o enquadramento do consumidor nas relações consumeristas, é chegado o momento de caracterizar o fornecedor, e isto pode ser feito inicialmente visitando a letra da lei. O artigo 3º do CDC define fornecedor nos seguintes termos:

> Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.
> § 1° Produto é qualquer bem, móvel ou imóvel, material ou imaterial.
> § 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista. (BRASIL, 1990).

A lei é bem ampla na conceituação de fornecedor, restringindo o prestador de serviços, porém, com os termos "mediante remuneração" e "salvo as decorrentes das relações de caráter trabalhista". Como esta pesquisa não enfoca nas relações trabalhistas, observar-se-á apenas o aspecto mencionado sobre remuneração. Acerca da obrigatoriedade de remuneração, a posição doutrinária e jurisprudencial – apesar de não consolidada – sobre a prestação de serviços na *Internet* é no sentido de considerar que, mesmo quem fornece serviços gratuitamente na rede, pode ser considerado fornecedor; e o exemplo é que a prestação de serviços *online*, como redes sociais, *e-mails* e outros pode lançar mão de publicidade *online* para se remunerar (BLUM, 2018).

A publicidade *online*, nesses casos, seria então um meio de obter uma remuneração indireta, a partir do pagamento feito por anunciantes que usam espaços publicitários em *websites* dos fornecedores, acessados então pelos consumidores. Os usuários de *websites* seriam, nesses casos, consumidores diretos ou ainda consumidores equiparados, caso apenas visitassem os locais na *Internet*.

Para este trabalho, também é interessante notar que, além do fornecedor do serviço *online* por meio do *site*, há o caso daqueles que desenvolvem e fornecem produtos de *software* para coleta e gestão do consentimento, sistemas esses que são implantados nos *website*s. Esses sistemas de gestão de consentimento também são denominados CMPs – *Consent Management Platforms* – e se prestam às atividades de coletar, processar, registrar, armazenar e transmitir o consentimento obtido – ou não – dos usuários desses *sites*. A maioria desses CMPs são *software*s pagos, sendo alguns inclusive no modelo

SaaS (*Software as a Service*). Os CMPs não existem por si só, mas fazem parte de parcela significativa dos *sites* em geral nos dias atuais. Assim, os CMPs prestam serviço *online* agregado diretamente aos *website*s, e se indaga se também podem ser considerados fornecedores do ponto de vista do direito do consumidor.

Outro caso é o das plataformas de navegação – os navegadores, ou *browsers*, cujas licenças de uso atualmente não têm custo, via de regra. A posição dos navegadores do Google e da Microsoft são interessantes, pois essas empresas são fabricantes de sistemas operacionais utilizados em dispositivos móveis ou computadores pessoais; uma parcela da sua receita, especialmente do Google, advém da gestão do maior sistema de publicidade *online* direcionada em escala mundial, o Google Ads. Este sistema, que utiliza *big data* como insumo, coleta dados de pessoas durante sua interação com o ambiente *online*. Esses dados, que são então processados, enriquecidos, agregados ou não, armazenados e compartilhados com outros terceiros agentes do arcabouço de publicidade digital, formam então os perfis pessoais. O processo descrito também é denominado *profiling*, ou perfilização. Os perfis pessoais contêm identificadores únicos de redes sociais, assim como outras características pessoais, de gênero sexual, renda, escolaridade, localização geográfica, além de características dos dispositivos usados para navegar na *Internet*, como versão de sistemas, aplicativos usados, resolução de tela, situação da bateria e outros mais. Tais perfis são parte do lastro, do combustível, do insumo usado para movimentar o sistema de publicidade digital. A questão é que essas mesmas *big techs* fornecem os sistemas operacionais que dão suporte a tudo isso, os sistemas navegadores usados para acessar ambientes *online*, e ainda as tecnologias com as quais são produzidos os *website*s. Além do fornecimento dessa série de produtos de *software*, essas mesmas empresas atuam diretamente na gestão de sistemas de publicidade digital, como o Google Ads ou o Microsoft Advertising. Assim, outra indagação é se os fornecedores de sistemas de navegação, no contexto aqui explicado, poderiam ser considerados também fornecedores sob o ponto de vista do direito do consumidor em relação à proteção de seus dados pessoais.

3.5.3 Espécies de vulnerabilidade do consumidor no meio digital

Os estudos da doutrina acerca da tipificação da vulnerabilidade levaram à criação da conhecida classificação de Cláudia Lima Marques, segundo a qual a vulnerabilidade

pode ser técnica, jurídica ou científica, fática ou socioeconômica, e informacional (MARQUES, 2019, p. 312).

A vulnerabilidade técnica se dá em relação ao consumidor e ao produto ou serviço: o consumidor não tem conhecimento suficiente sobre o produto ou serviço ofertado (MARQUES, 2019, pp. 313-314). O consumidor não possui, neste caso, o embasamento cognitivo suficiente para avaliar os riscos técnicos daquilo que está contratando ou àquilo que está se expondo. Veja-se o exemplo de um *website* de notícias, que coleta informações do navegador para identificar o usuário com o objetivo de entregar publicidade direcionada ao seu perfil de consumo. Nesta situação, o consumidor internauta é tecnicamente vulnerável porque não conhece os meandros da implementação e da tecnologia que está por trás do *website*, que pode capturar seus dados pessoais de modo sorrateiro sem a autorização respectiva e criar um banco de dados com o perfil do consumidor. O dever de informar, que o fornecedor tem referente ao consumidor, deve ser exercido para reequilibrar as forças das partes e assim mitigar os riscos desta vulnerabilidade.

A vulnerabilidade jurídica ou científica acontece na perspectiva das consequências jurídicas das decisões tomadas pelo consumidor em relação ao fornecedor, o que toma relevância num contexto de massificação dos contratos de adesão, que podem ter cláusulas abusivas, e a única alternativa que resta ao consumidor é acatar ou desistir. Esta espécie de vulnerabilidade cuida dos reflexos quanto aos direitos e obrigações do consumidor. No uso de *websites*, por exemplo, o consumidor pode ser enquadrado como juridicamente vulnerável se for instado a fornecer seu consentimento para tratamento de dados pessoais sem ao menos entender das consequências jurídicas de tal ato.

A vulnerabilidade fática ou socioeconômica acontece com a assimetria de poder do fornecedor em relação ao consumidor: a relação consumerista, que é estruturalmente desigual, pode ser caracterizada pela disparidade da capacidade socioeconômica entre as partes. Por exemplo, a multiplicação dos contratos de adesão reflete a dificuldade ou impossibilidade de atendimento da autonomia da vontade por parte do consumidor, que é obrigado a pegar ou largar; neste contexto, em que o consumidor não tem outra alternativa senão aceitar os termos dos contratos ou então ficar sem o produto ou serviço, a vulnerabilidade do indivíduo se acentua, *de fato*. Quando há um produto muito exclusivo ou essencial no mercado – com monopólio, por exemplo – e cuja dependência do consumidor para com o fornecedor seja relevante, também ocorre a vulnerabilidade fática (MARQUES, 2019, pp. 320-324).

Cláudia Lima Marques introduz a vulnerabilidade informacional, e afirma que esta decorre do natural déficit informacional que caracteriza o consumidor - pois os fornecedores são os reais detentores da informação – e pode ser entendida como uma espécie de vulnerabilidade técnica (MARQUES, 2019). A vulnerabilidade informacional é inerente à relação consumerista, e por isso deve haver compensação pela presença de riscos decorrentes da oferta do produto ou serviço, tais como a ameaça ao direito de escolha do consumidor, os direitos fundamentais da dignidade da pessoa humana, o direito à vida, à liberdade, à informação e a proteção dos interesses do consumidor (MARQUES, 2019). A vulnerabilidade informacional é entendida, assim, como a possibilidade de exposição a riscos decorrentes da ausência de informação ou informação incompleta, do excesso de informação, da informação manipulada, informação inútil ao consumidor, ou ainda da informação enganosa que visa a dissuadir o indivíduo em prol dos interesses do fornecedor. Também na vulnerabilidade informacional, assim como na vulnerabilidade técnica, é relevante o dever de informar para trazer mais igualdade à relação consumerista por via da equidade informacional (MIRAGEM, 2021).

O Decreto 7962/2013 estabelece critérios sobre o provimento de informações no meio eletrônico. O Decreto 5903/2006 traz critérios sobre a apresentação de informações ao consumidor

Além da classificação quadripartite de Cláudia Lima Marques, outras vulnerabilidades são relevantes para este estudo, tais como a vulnerabilidade neuropsicológica e a vulnerabilidade digital. O uso do ambiente digital para fomentar o aumento do consumo traz novos desafios à interpretação do direito, e então é necessário recorrer a outras lentes para reconhecer a vulnerabilidade do consumidor. No ambiente *online*, a perfilização dos consumidores tem se mostrado eficiente para a análise comportamental e criação de publicidade direcionada. Também o emprego de *nudges* e *dark patterns*, oriundos da economia comportamental (MIRAGEM, 2021), aumenta o potencial de assertividade das práticas comerciais. Não obstante a racionalidade limitada ser característica do *homo economicus*, aquele ser teórico que toma decisões ótimas puramente baseadas na racionalidade, a vulnerabilidade neuropsicológica adiciona mais uma dimensão a ser considerada no âmbito consumerista: ela enfatiza a desproporcionalidade de forças entre fornecedores e consumidores, à medida que os incentivos sensoriais – com cores, destaques e formas estimulantes – visam ao aumento do consumo. Do mesmo modo, os estímulos emocionais podem incutir, nas mentes dos consumidores, necessidades até então não percebidas ou não existentes, naturais ou

induzidas – que eles realmente tinham e das quais apenas não haviam tomado consciência, ou aquelas cujo surgimento se deu única e exclusivamente por estímulo externo, proveniente do marketing com o uso de *dark patterns*; assim, os consumidores são vulneráveis neuropsicologicamente porque são expostos a práticas vindas da economia comportamental e que afetam a sua liberdade de escolha.

A vulnerabilidade neuropsicológica também pode ser explorada pelo emprego de mensagens subliminares, que influenciam fortemente o comportamento humano, e viciam o requisito de validade dos negócios jurídicos, pois afastam a decisão consciente que decorre da manifestação da vontade livre e verdadeira (FRANCO, 2018). As mensagens subliminares atuam no nível inconsciente da mente humana, e por agirem de forma manipulativa são completamente reprováveis pelo ordenamento jurídico (FRANCO, 2018). Por exemplo, a publicidade indireta, cuja intenção escapa ao nível consciente, é considerada prática abusiva pela legislação, pois do consumidor é subtraída a capacidade de identificar tal prática comercial – publicidade, conforme o artigo 36 do CDC: "[a] publicidade deve ser veiculada de tal forma que o consumidor, fácil e imediatamente, a identifique como tal" (BRASIL, 1990).

Bruno Miragem indica a existência de outra espécie de vulnerabilidade: a vulnerabilidade digital, pois novos riscos tomaram forma no ambiente eletrônico, a exemplo do tratamento ilícito de dados e das fraudes de todo o tipo, devido ao surgimento de novas formas de contratação e das características inerentes ao objeto digital de consumo (MIRAGEM, 2021), que pode não se encaixar nem como produto físico e muito menos como serviço. A vulnerabilidade digital é, assim, resultante do próprio meio digital, o ambiente eletrônico.

Laura Schertel Mendes discorreu sobre a vulnerabilidade do consumidor quanto à proteção de seus dados pessoais (MENDES, 2015). Segundo a autora, a evolução da economia de mercados de massa para um modelo de produção customizado exigiu também que o marketing de massa fosse substituído pelo marketing individualizado, que usa perfil de consumidor, com dados específicos de cada indivíduo. Essa perfilização é feita com a contínua vigilância, sendo os dados são utilizados como insumo do processo produtivo customizado. Todavia, essa vigilância incorre em riscos como a supressão da autonomia do consumidor e a discriminação da pessoa. Como consequência, as empresas sabem muito sobre seus consumidores, e estes por sua vez desconhecem essas empresas.

Para aquela autora, no âmbito da vulnerabilidade, tem-se o problema do consentimento aparente: *take it or leave it*, pegar ou largar, quando é obrigatório consentir

para acessar produtos ou serviços. Também na vulnerabilidade, há risco da falta de transparência no tratamento de dados, como por exemplo no *credit scoring*. A falta de transparência no tratamento de dados se revela como prática abusiva: sem transparência, não há controle pelo consumidor, nem controle externo por quem fiscaliza. A falta de transparência dificulta o controle e a fiscalização do fluxo de dados, tanto pelo consumidor ou titular quanto pelo fornecedor ou agente de tratamento.

Ressalta-se ainda que o CDC, art. 6º, inc. III atribui ao consumidor o direito de ser informado. Para Mendes (2015), no âmbito de proteção de dados pessoais do consumidor, esse direito de ser informado abrange informações sobre quais dados e finalidades, sobre compartilhamento de dados com terceiros e quais países, sobre prazo de guarda, e sobre como a segurança é garantida. Além disso, conforme o CDC, art., 46, não há obrigação ao consumidor sem prévio aviso sobre os termos contratuais.

Mendes afirma que, no direito alemão, o consentimento tem a natureza de um ato jurídico similar ao de um negócio jurídico, e que assim o consentimento pode ser enxergado do prisma de negócios jurídicos e de contratos. Ela argumenta também que a análise de casos de obtenção de consentimento para tratamento de dados pessoais pode ser feita com enfoque na boa-fé objetiva, conforme positivado no CDC, art. 4º, inc. III, e art. 51, inc. IV. Por meio da boa-fé, é possível identificar práticas abusivas, que ignoram o dever de lealdade e as expectativas razoáveis dos consumidores, e que desequilibram demasiadamente a balança de poder entre as partes.

Laura Schertel Mendes (2015) também discorre sobre outro critério para identificar a violação da privacidade: a expectativa legítima do consumidor quanto à segurança esperada, consubstanciada na "responsabilidade pelo fato do produto e do serviço" (BRASIL, 1990). Além disso, segundo a autora, o consumidor também é vulnerável quanto aos seus dados pessoais em razão de riscos de discriminação, pela oferta de preços diferenciados em razão de algum critério, como a geolocalização, prática conhecida como *geopricing*. Por fim, a autora argumenta que o Estado tem o dever constitucional de proteger o consumidor quanto aos seus dados pessoais, conforme o art. 5º, XXXII para garantir a liberdade material, ou liberdade efetiva do consumidor, à luz da boa-fé objetiva e do atendimento das legítimas expectativas dos consumidores.

3.5.4 A vulnerabilidade do consumidor quanto à proteção de dados

Em estudo sobre a vulnerabilidade aplicada à proteção de dados pessoais, Malgieria e Niklas propõem usar a teoria de camadas de vulnerabilidade proposta por Florencia Luna, segundo a qual a vulnerabilidade tem tanto o caráter universal quanto o particular: ela é uma condição que afeta os seres humanos como um todo, mas que também se manifesta com diferentes intensidades em cada pessoa (LUNA, 2009). Assim, os pesquisadores apresentam a ideia de que no campo de proteção de dados a vulnerabilidade é característica intrínseca a todas as pessoas – caráter universal –, e que algumas delas têm situações de maior vulnerabilidade – caráter particular (MALGIERIA; NIKLAS, 2020).

Numa abordagem de riscos, os mesmos pesquisadores discutem a vulnerabilidade quanto aos riscos referentes ao tratamento de dados – **antes** do tratamento –, e aos riscos referentes ao resultado do tratamento de dados – **após** o tratamento. No primeiro caso, os riscos quanto ao tratamento de dados são atrelados ao campo dos direitos, e são devidos à capacidade de fornecer consentimento, de compreender o funcionamento do tratamento – efetividade do cumprimento do dever de informar – e de exercer os direitos de titulares de dados previstos na legislação. No segundo caso, os riscos são pertinentes aos possíveis danos causados por discriminação de toda natureza, manipulação, danos físicos e psicológicos. Os pesquisadores também observam que as discussões sobre os riscos do resultado do tratamento de dados se concentram no estudo sobe vieses de algoritmos e decisões automatizadas (MALGIERIA; NIKLAS, 2020).

Sob o enfoque de proteção de dados e vulnerabilidades, pode-se entender: que a **vulnerabilidade técnica** diz respeito à falta de conhecimento aprofundado sobre como é implementado o tratamento de dados; que a **vulnerabilidade jurídica** é representada pela dificuldade de dominar as consequências das decisões tomadas no ambiente eletrônico; que a **vulnerabilidade fática** decorre da massificação dos contratos de adesão – e em especial do *framework notice and consent*; que a **vulnerabilidade informacional** é devida à assimetria da informação que caracteriza as relações na *Internet* – em que os *players* detêm verdadeiros dossiês com perfis dos usuários, e em cujos *websites* por vezes há falta ou excesso de informação; que a **vulnerabilidade neuropsicológica** se consubstancia no emprego de *dark patterns* para influenciar as decisões *online* dos titulares quanto aos dados pessoais; que a **vulnerabilidade digital** se refere aos tratamentos ilícitos de dados e às fraudes na *Internet*; que o campo de proteção de dados também tem um elemento de vulnerabilidade, segundo o qual todas as pessoas estão expostas a riscos, umas mais e outras menos, e que há riscos antes do tratamento de dados

e após ele, sendo a vulnerabilidade do consumidor em relação à proteção de seus dados pessoais.

Então, com base nessas vulnerabilidades estudadas, é possível reconhecer para ampla área do direito da proteção de dados, a existência de uma vulnerabilidade mais específica, que é a **vulnerabilidade de proteção de dados**, derivada da vulnerabilidade digital e da vulnerabilidade do consumidor quanto à proteção de seus dados, e que carrega em si um pouco dos aspectos das demais vulnerabilidades descritas anteriormente. Esta vulnerabilidade de proteção de dados é asseverada também pela impossibilidade de o sujeito ter acesso à real implementação do tratamento de dados pessoais, pois este é feito remotamente na maioria das vezes, e pela impossibilidade de controle da atuação do agente de tratamento, como na implementação da arquitetura de escolhas que influencia as tomadas de decisão. Tal vulnerabilidade se assenta, ainda, na extrema dependência do titular de dados quanto à aplicação dos princípios da confiança e da boa fé por parte dos agentes de tratamento. Por exemplo, como visto na pesquisa de campo desta investigação científica, existem riscos quanto à legalidade do tratamento de dados pessoais dos *cookies* frente à informação prestada nos avisos de *cookies*. Assim, como resta ao titular simplesmente a *esperança* de que os agentes de tratamento atuem eticamente e de boa fé no seu *métier*, e que honrem a confiança que neles foi depositada, o titular é claramente vulnerável quanto à proteção de seus dados pessoais, ante as inúmeras formas de tratamento de dados, a racionalidade limitada do ser humano, a dificuldade de tomar decisões locais que podem ter impacto significativo no futuro distante, dentre outros fatores.

Esta vulnerabilidade de proteção de dados acontece **antes** e **depois** do tratamento de dados, assim como apresentado por Malgieria e Niklas (2020). Contudo, a abordagem proposta aqui é a de incluir também a vulnerabilidade existente **durante** o tratamento de dados, e que pode ter consequências não aparentes ao titular, tais como a permanente vigilância que decorre de compartilhamentos de dados indevidos e outros tratamentos indevidos, as consequências latentes e potenciais como a possibilidade de desanonimização empregando novas tecnologias ou por agregação de outros dados, a materialização da teoria do mosaico pela construção de conhecimento futuro sobre os titulares como nas análises preditivas, deduções ou inferências sobre características humanas comuns ou sensíveis, e uma série de efeitos colaterais obscuros, invisíveis, imperceptíveis e ubíquos que podem nunca ser detectados, mas que de fato podem existir.

Sobre a vulnerabilidade digital, o surgimento de novos ambientes virtuais que proporcionam experiências imersivas de realidade virtual e realidade aumentada podem fazer uso ainda mais intensivo de dados pessoais, pois o aumento da interação do indivíduo com esses mundos virtuais apresenta riscos à proteção de dados pessoais sensíveis, e também porque a vulnerabilidade neuropsicológica é potencializada neste tipo de ambiente.

A análise preditiva decorrente de técnicas de mineração de dados, assim como de técnicas de aprendizado de máquina, ou *machine learning*, permite a exploração de novas formas de produção de conhecimento sobre a pessoa humana. Usando a análise preditiva, é possível realizar deduções até sobre as características mais íntimas das pessoas. Por exemplo, analisando alguns dados básicos de um indivíduo, pode-se deduzir outros dados derivados destes. Famoso é o caso em que uma empresa farmacêutica começou a enviar para uma mulher, que ainda não havia atingido a maioridade, algumas ofertas de produtos para gestantes, e após o pai ter reclamado junto ao ofertante sobre tais recebimentos, a filha contou que estava grávida. Naquela situação, o fornecedor analisou o histórico de compras da adolescente, e assim inferiu o estado gravídico da consumidora (VASCONCELOS CAMURÇA; NOGUEIRA MATIAS, 2021).

A conjugação da vulnerabilidade neuropsicológica com a vulnerabilidade digital, nas acepções respectivas, leva a crer que existe o risco aumentado de tratamento indevido de dados pessoais sensíveis por parte dos fornecedores. Há variáveis que se comportam como *proxies*, isto é, são variáveis que "representam" outras ou que com elas têm forte correlação.

Por exemplo, no caso Cambridge Analytica, os pesquisadores fizeram perguntas simples e "inocentes" para os respondentes, e assim conseguiram mapear o perfil de preferência política das pessoas. As perguntas feitas no aplicativo *This Is Your Digital Life*, através do Facebook, eram parte de uma suposta pesquisa científica liderada pelo psicólogo Aleksandr Kogan da Universidade de Cambridge. Por meio deste aplicativo, os dados pessoais de 270 mil respondentes diretos – além de seus perfis psicológicos traçados por meio da pesquisa – e os dados pessoais de todos os contatos dos respondentes (cerca de 87 milhões de pessoas) foram indevidamente coletados e compartilhados sem consentimento com a consultoria Cambridge Analytica que fazia mineração de dados e atuava com consultoria eleitoral. As perguntas tinham natureza aparentemente ingênua, como por exemplo: se a pessoa executa o que planeja, se tem dificuldade de entender ideias abstratas, se frequentemente perde a compostura, se gosta de ser o centro das

atenções e outras desse estilo. O objetivo das perguntas foi o de identificar o perfil psicológico dos respondentes, de acordo com o modelo Big Five que classifica as personalidades humanas em cinco tipos: extroversão, socialização, realização, neuroticismo e abertura (GUERRA *et. al.*, 2017).

Estudos apontam que há grande correlação entre os tipos de personalidades e a escolha por certos produtos ou marcas (GUERRA *et. al.,* 2017); assim, é mister prestar atenção na identificação do perfil psicológico do consumidor, pois a sua personalidade influencia nas escolhas que normalmente faz. Outros estudos relacionam os tipos de personalidades mais propensos a realizar compras impulsivas (GUERRA *et. al.,* 2017). Da mesma forma que perfis psicológicos foram identificados por meio de perguntas simples no caso Cambridge Analytica, o perfil psicológico-comportamental pode ser deduzido a partir do *user profiling*: hábitos de consumo e outras características pessoais coletadas de fontes esparsas na *Internet* ligadas à pessoa natural – em combinação com bases de dados que já tenham mapeadas as relações entre perfis psicológicos e preferências dos consumidores. Em última análise, e no limite, existe a possibilidade de se deduzir – por exemplo – as preferências políticas, sexuais, religiosas e outras mais, classificadas como dados pessoais sensíveis, a partir de perfis psicológicos previamente traçados e então conjugados perfis dos mesmos indivíduos que contenham dados pessoais e dados de consumo coletados de inúmeras fontes.

Tal possibilidade de inferência de dados pessoais sensíveis a partir de outras fontes, ainda que remota – ou nem tanto assim – existe, e pode ser corroborada pelo uso de *big data* em conjunto com tecnologias de inteligência artificial. Isto pode representar risco às liberdades individuais, ressaltando ainda o risco de discriminação. Uma reportagem do *website* Computer Weekly, do ano de 2020, retrata a tentativa de realizar exatamente isto: no Reino Unido, os três maiores partidos políticos se empenharam em coletar dados pessoais de eleitores para inferir os dados pessoais e dados pessoais sensíveis, tais como religião, opiniões políticas, nacionalidade e renda; posteriormente, verificou-se que o *data enrichment* – que é o enriquecimento dos perfis individuais com processamentos adicionais e dados de outras fontes – não foi efetivo, isto é, a tentativa de deduzir tais dados pessoais não foi bem sucedida pois não correspondia à realidade das pessoas (COMPUTER WEEKLY, 2020).

Em 2012, pesquisadores da Universidade de Cambridge e da Microsoft estudaram a relação entre as características da personalidade e as preferências de navegação em *websites*, e identificaram que é possível deduzir quais *websites* as pessoas têm maior

tendência a acessar conforme a sua classificação psicométrica. Foi utilizado o modelo *Five Factor Model – Big Five* – que categoriza as personalidades humanas em 5 *clusters* – agrupamentos – de maior densidade, e com base em dados psicométricos de 160 mil pessoas e respectivas preferências de *websites*, os pesquisadores concluíram que é possível deduzir qual é o perfil psicométrico das pessoas com base no seu histórico de navegação (KOSINSKI *et. al.,* 2012). Esta pesquisa é relevante porque demonstra que o escrutínio do histórico de navegação de uma pessoa natural, acumulado ao longo de um certo tempo, pode revelar os traços da sua personalidade. O uso do perfil psicométrico, junto com outros dados, pode também ser usado em favor do marketing comportamental, personalizando ofertas e influenciando assim na capacidade decisória das pessoas.

Um subgrupo dos mesmos pesquisadores do estudo anterior também investigou o nível de dificuldade de realizar predições sobre os seguintes caracteres humanos: orientação sexual, estado civil, preferências políticas, orientação religiosa, etnicidade, traços de personalidade, inteligência, grau de felicidade, uso de substâncias viciantes, separação dos pais, idade e gênero. Para o estudo publicado em 2013, mais de 58 mil pessoas forneceram os dados dos *likes* dos seus perfis do Facebook, responderam a questionário sobre perfil demográfico e realizaram vários testes psicométricos. A pesquisa se apoiou também no modelo dos cinco fatores (*Big Five Model*) para identificar o perfil psicológico. Utilizando os dados anteriormente descritos que foram fornecidos pelas pessoas que participaram da pesquisa, foi possível elaborar um modelo computacional com técnicas de *machine learning*, que na fase de treino aprendeu com o *dataset* de treino – isto é, os dados de *likes*, dados demográficos e dados psicométricos – para realizar as predições na fase de teste. Os resultados da pesquisa demonstraram que, em certos casos, a identificação correta das características pessoais chegou até a 95%, como na identificação sobre a etnicidade – se a pessoa tem origem caucasiana ou americana. O gênero sexual foi identificado corretamente em 93% das vezes, os homossexuais do sexo masculino 88% das vezes, a preferência política entre democratas ou republicanos em 85% das vezes, e a preferência religiosa entre cristianismo e islamismo em 82% dos casos avaliados. As demais características, como elencadas anteriormente, também puderam ser inferidas corretamente no espectro de 60% a 75% das vezes. O mote da pesquisa foi o de demonstrar o quão acertadamente é possível fazer previsões sobre características humanas tão relevantes – muitas delas sensíveis, que podem levar a discriminações, tais como preferências políticas, sexuais e religiosas –

utilizando dados que estão tão facilmente disponíveis nas redes sociais, tais como os registros de *likes* do Facebook (GRAEPEL; KOSINSKI; STILLWELL, 2013).

A realização de inferências de características humanas – dados pessoais sensíveis ou não – a partir de dados pessoais dispersos e aparentemente inofensivos é a materialização da teoria do mosaico. Segundo a teoria do mosaico, a coleta de dados pessoais dispersos e aparentemente sem relevância, feita em grande escala, pode revelar conhecimento sobre os indivíduos que não seriam possíveis de se obter caso os dados pessoais fossem avaliados separadamente. David Pozen explica que esta teoria surgiu nos Estados Unidos da América e tem sido usada como forma de negar pedidos de informação feitos ao governo com base no *Freedom of Information Act* (FOIA), lei que prioriza a transparência no governo estadunidense. O primeiro caso de uso da teoria do mosaico aconteceu em 1972, no caso United States v. Marchetti, quando o Poder Judiciário norte-americano impediu um ex-funcionário da Central Intelligence Agency (CIA) de publicar um documento intitulado "A CIA e o Culto da Inteligência" (POZEN, 2005). Apesar de este primeiro caso não ter sido ainda baseado em pedidos de acesso a informação com base no FOIA – tais como os pedidos feitos no Brasil com base na Lei de Acesso à Informação (LAI) – a sentença judicial exarada pelo então juiz de direito Clement Haynsworth inaugurou a teoria do mosaico, segundo o qual o significado de uma informação pode depender do seu contexto, e a informação que aparenta ser irrelevante pode ter enorme importância para aquele que tem uma visão mais ampla do panorama e que consegue encaixar o dado no contexto correto (HAYNSWORTH *apud* POZEN, 2005).

Uma das possíveis soluções para os problemas decorrentes da vulnerabilidade do consumidor está na recomendação da OCDE sobre proteção do consumidor no comércio eletrônico: educar os consumidores sobre os seus direitos e obrigações previstos na legislação consumerista, e também capacitá-los para que adquiram habilidades suficientes para interagir com a tecnologia voltada ao comércio eletrônico (FROTA; RAMOS, 2018).

Outra possível solução para a vulnerabilidade informacional é alterar a linguagem utilizada nas comunicações com o consumidor feitas de forma *online*. Ramos e Frota exemplificam o caso da oferta de artigos digitais como livros eletrônicos: ao invés de os *websites* utilizarem botões com os dizeres "Compre", ou "Compre Agora", poderiam ser empregados os termos "Adquira Sua Licença", ou "Licencie Agora", pois verdadeiramente os consumidores nestes casos não adquirem o produto para si, apenas

meramente adquirem uma licença de uso de um artigo que é disponibilizado virtualmente no próprio ambiente do fornecedor (FROTA; RAMOS, 2018).

Os *websites* empregam *nudges* e *dark patterns* para se comunicar com os usuários quando desejam que estes aceitem seus termos, forneçam consentimento, adquiram produtos ou serviços. Ao mesmo tempo, os mesmos *websites* empregam linguagens técnicas e jurídicas intrincadas, complexas, que dificultam sobremaneira a leitura dos termos de uso e políticas de privacidade. Nos avisos de *cookies*, por exemplo, o objetivo principal dos responsáveis pelos *websites* é o de obter o consentimento destes, além de atender de certa forma ao dever de informar imposto pela legislação. Já nas políticas de privacidade e nos termos de uso, o maior objetivo dos mesmos atores é o de preservar os seus próprios direitos, prevenindo qualquer tipo de questionamento quanto ao dever de informar, pois está tudo lá escrito; o conteúdo de tais documentos serve, ainda, ao cumprimento do dever de informar, de maneira bem mais detalhada.

O que fica claro, nesta análise, é que há uma enorme distância entre a informação apresentada – ao consumidor, titular de dados pessoais ou usuário de *Internet* – e o seu objetivo real. De um lado, nos avisos de *cookies*, por trás da expressão "usamos *cookies* para melhorar a experiência do usuário", com a aparência de cumprir com o dever de informação e de obter o consentimento, está a indiscriminada e generalizada coleta de dados pessoais e compartilhamento com diversos outros atores do cenário do comércio eletrônico, da publicidade digital, e do sistema de vigilância cibernético implantado. E por outro lado, nos termos de uso e políticas de privacidade, está a dificuldade decorrente da vulnerabilidade técnica, jurídica e também informacional que caracteriza os consumidores e titulares de dados pessoais de modo geral, que impõe barreiras linguísticas à compreensão dos termos, ou que simplesmente desmotivam a apreciação de longos textos detalhados – sobre assuntos que as pessoas comuns desconhecem ou pelos quais não se interessam à primeira vista – por conta do tempo necessário para empreender a leitura, ou pelo cansaço que tal desafio representa.

Para além da fadiga do consentimento – proporcionada pelo fator da constante e reiterada solicitação de autorização para coleta de dados pessoais por parte dos usuários nos avisos de *cookies*, e asseverada pelo outro fator da quilométrica e pedregosa via de leitura dos termos de uso e políticas de privacidade – está o próprio emprego desses dois fatores como um padrão obscuro que induz o titular de dados pessoais a fazer exatamente aquilo que o responsável pelo *website* deseja: aceitar os termos e as políticas de privacidade, fornecer seus dados, comprar aquilo que está sendo ofertado, e não criar caso

com os detalhes da implementação de toda esta operação, evitando assim questionamentos sobre o amplo tratamento e compartilhamento de dados pessoais e os reais significados dos termos da contratação que realizara. Esta prática, à vista do Código de Defesa do Consumidor, pode ser considerada prática comercial abusiva.

Para realizar uma ponte entre a comunicação dos avisos de *cookies* e os conteúdos das políticas de privacidade, diminuindo assim o risco representado pela vulnerabilidade informacional, é possível criar uma camada informacional intermediária, que aplique elementos visuais, ícones e outros componentes para resumir os aspectos mais importantes sobre aquilo que se está autorizando. A recente área de estudo do *Visual Law* trabalha com este assunto. Um exemplo disto é o emprego de indicadores visuais inspirados em tabelas ou rótulos de informações alimentares, tais como os sugeridos nas pesquisas de Lorrie Cranor (2012).

No caso dos avisos de *cookies*, o dever de informação impõe a necessidade de informar claramente sobre a possibilidade de rastreamento do usuário por terceiros com quem o *website* se comunica, assim como é preciso comunicar a possibilidade de formação de perfil de consumo e perfil comportamental que poderá ser usado por terceiros para finalidades específicas. O rastreamento fomenta a formação de perfil, e também aumenta o risco de vigilância indevida. Também neste ponto, é importante informar sobre a possibilidade – ou não – de existir o risco de inferência de dados pessoais sensíveis que possam ser causa de discriminação pessoal e representar risco às liberdades individuais da pessoa natural.

Na hipótese de formação do perfil do titular de dados pessoais por parte do *website*, caso contenha dados pessoais sensíveis, e na hipótese da inferência de dados pessoais sensíveis, é necessário obter o consentimento específico com cláusula em destacado, nos termos do artigo 11, inciso I da Lei Geral de Proteção de Dados: "quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas" (BRASIL, 2018). E na hipótese da formação de perfil de consumidor, também é importante obter a autorização do consumidor – *standard* ou equiparado – para a criação de registro de banco de dados em seu nome que contenha seus dados pessoais e dados de consumo, ou a comunicação à pessoa sobre a abertura de tal registro, nos exatos termos do artigo 43, §2º do Código de Defesa do Consumidor: "[a] abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele" (BRASIL, 1990).

No comércio eletrônico, outra sugestão – para diminuir o risco de desinformação do consumidor usando a mesma lógica de salientar pontos mais importantes de forma simplificada, e para fazer a mesma ponte entre a superficialidade da informação da oferta e a profundidade real de eventuais limitações da contratação – é apresentar de forma ostensiva, em linguagem simples, clara, acessível e facilmente visível, as mais relevantes limitações ao uso dos produtos ou serviços contratados em formato digital – como o exemplo dos livros eletrônicos mencionado alhures (FROTA; RAMOS, 2018).

3.5.5 Autodeterminação informativa

Laura Schertel Mendes apresenta o surgimento e a evolução do conceito de autodeterminação informativa no contexto alemão. A ideia de identificação das esferas íntima, privada e individual-social para proteger o indivíduo, segundo a qual as esferas íntima e privada seriam mais protegidas e a esfera individual menos, evoluiu para o reconhecimento de um direito geral da personalidade. Para a jurisprudência germânica, é por meio do direito geral da personalidade que o próprio indivíduo determina (autodeterminação) como ele se apresenta ao público, abrangendo toda a personalidade e não somente a esfera privada (ampliação da abrangência do conceito). Outro caractere importante do direito geral da personalidade reside na ideia de abstração, para fazer frente a futuras ameaças ao indivíduo: é nesse caminho que o desdobramento do direito geral da personalidade ocorreu em relação ao aspecto informacional do indivíduo (MENDES, 2020, pp. 2-10).

Assim, como corolário do direito geral da personalidade, e usando a abstração, a autodeterminação da pessoa foi estendida ao âmbito informacional, dando origem ao conceito de autodeterminação informativa com a decisão do Tribunal Constitucional Alemão sobre o recenseamento em 1983 (MENDES, 2020, p. 10).

Apoiado na ideia de autodeterminação e na necessidade de restringir o processamento de dados para reconhecer a autodeterminação informativa como direito fundamental, o tribunal alemão entendeu ser necessário criar limites, devido à falta de transparência, à grande quantidade de informações coletadas sobre os indivíduos e à suposta enorme capacidade de processamento do Estado, tratando possíveis riscos aos direitos individuais (MENDES, 2020, p. 10)

Identificando que os cidadãos poderiam não mais ter liberdade para tomar suas próprias decisões em relação a possíveis pressões estatais, por exemplo com a criação de

perfis; e percebendo que a incapacidade de as pessoas controlarem - dentre outros aspectos - **quem** tem **quais** informações prejudicaria os direitos individuais, a democracia e o próprio direito à autodeterminação informativa, o tribunal alemão também entendeu que todos os dados pessoais, independentemente de tipo, estariam abarcados por tal direito, não existindo dados insignificantes. E assim, para a corte constitucional germânica, o direito à autodeterminação informativa garante que a própria pessoa pode decidir sobre as condições de coleta e uso de seus dados (MENDES, 2020, pp. 10-11).

3.5.6 O Código de Defesa do Consumidor e a Lei de Defesa dos Usuários dos Serviços Públicos: Lei 13.460/2017

O artigo 3º do CDC também considera que o fornecedor pode ser pessoa jurídica pública ou privada, nacional ou estrangeira. No caso da pessoa jurídica pública ou privada nacional vinculada à administração pública brasileira, desde o ano de 2017 está em vigor no Brasil a Lei 13.460, que "[d]ispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública" (BRASIL, 2017), também conhecida como Lei de Defesa dos Usuários de Serviços Públicos. Para os fins deste trabalho, os aspectos legais da referida lei que rege a qualidade dos serviços públicos serão abordados apenas superficialmente neste tópico.

Apesar de haver poucos estudos doutrinários sobre este tema, a referida lei se aplica à administração pública direta e indireta de todos os entes da federação, portanto é uma lei ampla e importante também do ponto de vista dos sistemas públicos de controle interno e externo. Observa-se já no artigo 1º, §2º que o Código de Defesa do Consumidor deve ser usado conjuntamente com esta Lei de Defesa dos Usuários dos Serviços Públicos:

> § 2º A aplicação desta Lei não afasta a necessidade de cumprimento do disposto:
> I - em normas regulamentadoras específicas, quando se tratar de serviço ou atividade sujeitos a regulação ou supervisão; e
> II - na Lei nº 8.078, de 11 de setembro de 1990, quando caracterizada relação de consumo. (BRASIL, 2017).

Apesar de ter uma base privatista em contraponto ao regime juspublicista dos serviços públicos, era o CDC o principal diploma legal utilizado no lugar da Lei 13.460 antes de esta existir (JURUENA; VALLE, 2021). Esta lei, que traz na sua essência a proteção aos usuários dos serviços públicos, atendeu ao comando constitucional do artigo

37, §3º para a edição de lei para disciplinar "as formas de participação do usuário na administração pública direta e indireta" (BRASIL, 2017; JURUENA; VALLE, 2021).

Da mesma forma que o CDC conceitua consumidor e fornecedor, a Lei 13.460 apresenta os critérios para identificar quem pode ser considerado usuário do serviço público – "pessoa física ou jurídica que se beneficia ou utiliza, efetiva ou potencialmente, de serviço público" – e quem é entendido como administração pública: "órgão ou entidade integrante da administração pública de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios, a Advocacia Pública e a Defensoria Pública" (BRASIL, 2017). A abrangência tanto dos usuários quanto da administração pública é bem ampla, como é possível perceber.

Os incisos dos artigos 5º e 6º da Lei 13.460 enumeram direitos dos usuários dos serviços públicos. Para fins deste estudo, salienta-se os seguintes direitos: acessibilidade, "presunção de boa-fé do usuário", "adequação entre meios e fins", publicidade, "adoção de medidas visando a proteção à saúde e a segurança dos usuários", uso de soluções tecnológicas para melhor atendimento aos usuários, "utilização de linguagem simples e compreensível, evitando o uso de siglas, jargões e estrangeirismos", "obtenção e utilização dos serviços com liberdade de escolha entre os meios oferecidos e sem discriminação", "acesso e obtenção de informações relativas à sua pessoa constantes de registros ou bancos de dados", "proteção de suas informações pessoais", e "obtenção de informações precisas e de fácil acesso nos locais de prestação do serviço, assim como sua disponibilização na *Internet*" (BRASIL, 2017).

Os direitos supramencionados têm relação direta ou indireta com a gestão de dados pessoais realizada pelos *websites* disponibilizados pela administração pública, especialmente quanto à coleta, processamento e compartilhamento de dados por meio de *cookies* e *websites* de terceiros, e também sobre a forma de apresentação dos avisos de *cookies*. Por exemplo, o direito de proteção dos dados pessoais que consta no artigo 6º do referido diploma suporta esta afirmação, assim como o emprego de linguagem simples, a acessibilidade, o emprego de soluções tecnológicas que garantam a segurança dos usuários, a preservação da liberdade de escolha dos cidadãos e a publicidade.

4 ANÁLISE DE *COOKIES* E DE AVISOS DE *COOKIES*: METODOLOGIA

Este capítulo apresenta detalhadamente a metodologia utilizada durante a pesquisa, que foi conduzida com o objetivo de avaliar o impacto da vigência da LGPD sobre os *websites* brasileiros. Para isto, investigou-se a construção dos *websites* com respeito ao atendimento do direito à proteção de dados pessoais dos usuários de *Internet*, observando-se aspectos que tenham relação com proteção de dados pessoais.

É possível verificar, a partir da analise de *websites* brasileiros, o nível de conformidade desses sistemas em relação à Lei Geral de Proteção de Dados sobre a obtenção de consentimento dos titulares de dados pessoais (usuários dos *websites*) para operações de captura e tratamento de dados, e então comparar entre os resultados de antes e depois da vigência da LGPD.

Esta pesquisa foi conduzida para analisar os *cookies*, os *banners* e as politicas de privacidade, que são os meios de informação, interação e captura de dados mais comumente empregadas em *websites*. A pesquisa se voltou para *websites* brasileiros, com o objetivo de analisar as características sobre captura e tratamento de dados pessoais, verificando o comportamento dos *websites* em relação aos avisos sobre *cookies* e políticas de privacidade, e a sua evolução ao longo do tempo.

Para melhor didática, a metodologia empregada na pesquisa pode ser dividida em fases, correspondente a conjuntos de atividades carreadas durante a pesquisa. As fases foram realizadas conforme a Figura 5 que esboça de forma ampla as partes da pesquisa. É importante ressaltar que algumas fases se sobrepõem no tempo, isto é, algumas atividades de fases posteriores foram realizadas antes do fim das fases anteriores.

Na primeira fase, correspondente ao planejamento da pesquisa, foram definidos os elementos que seriam analisados. Os elementos escolhidos foram: os *cookies*, os avisos de *cookies* (*banners*) e as políticas de privacidade. Neste ponto, outras tecnologias de rastreamento de pessoas na *Internet*, tais como identificação de geolocalização, *web*

fingerprinting[5], *web pixels*[6], *web beacons* ou *web bugs*, rastreamento por ultrassom[7], *watermarking*[8], não foram selecionadas para análise.

Nesta fase, foi definido que a pesquisa abrangeria no mínimo dois momentos diferentes do tempo, de forma que os dados seriam coletados antes e depois da vigência da LGPD. Assim, o primeiro momento de captura escolhido foi o de maio de 2020, pois a LGPD entraria em vigor em 16 de agosto de 2020[9]. O segundo momento de captura foi planejado para ocorrer em maio de 2022, porém foi postergado para setembro de 2022, dois anos após a vigência da referida lei. A primeira captura feita pelo robô iniciou em 03 de junho e terminou em 05 de junho de 2020, e a segunda captura iniciou em 01 de setembro de 2022 e terminou em 02 de setembro de 2022. Para a execução do robô em 2020, foi utilizado um MacBook Pro 2012 com 16 GB de memória principal (memória RAM), 2 TB de armazenamento secundário e sistema operacional Mac OSX. O dispositivo com o robô estava ligado a uma conexão de *Internet* de 15 Mbps. O robô rodou em 2022 usando um MacBook Pro 2015 com 16 GB de memória principal, 250 GB de memória secundária, sistema operacional Mac OSX e uma conexão de *Internet* de 300 Mbps.

Ainda na primeira fase da pesquisa, também foram definidas as fontes de dados. As fontes de dados de *cookies*, avisos de *cookies* e políticas de privacidade poderiam ter

---

[5] *Web fingerprinting* é uma das técnicas de rastreamento mais utilizadas na *Internet*. É um processo que envolve a obtenção de diversas características do navegador e do próprio dispositivo eletrônico do usuário, como um *laptop* um *smartphone* ou computador de mesa. As características obtidas podem ser, por exemplo: nome e versão do navegador, extensões instaladas no navegador; resolução de tela usada pelo dispositivo, quantidade de bateria, geolocalização, configurações de teclado e outras informações. O *website* https://amiunique.org/ demonstra bem o quanto uma pessoa é identificável na *Internet*.

[6] *Web pixels* ou *web beacons* são pequenas imagens, geralmente na dimensão de 1 *pixel* de largura e 1 *pixel* de altura, usadas para enviar informações da estação do usuário para o servidor onde está o *pixel*. Por exemplo, se um *website* exibe um *banner* de publicidade que está armazenado em um domínio de terceiro, no carregamento deste *banner* para o computador local, pode ser enviado também o *pixel*. A URL para carregamento deste *pixel* é montada de forma que, ao solicitar o *download* da imagem, o sistema local do usuário encaminha diversas informações que podem caracterizar o indivíduo – e até individualizá-lo, assim como as demais técnicas descritas nesta seção.

[7] O rastreamento por ultrassom é feito por aplicativos instalados em *smartphones*, que se comunicam com outros aplicativos, por meio da emissão de ondas ultrassônicas imperceptíveis ao ouvido humano, mas que podem ser detectadas por outros dispositivos. Tais sons podem carregar informações sobre o dispositivo do usuário, bem como quaisquer outros dados, permitindo assim o rastreamento das atividades usando o aparelho móvel. Para mais informações, ver: https://www.comparitech.com/blog/information-security/block-ultrasonic-tracking-apps/

[8] *Watermarking* corresponde ao processo de inserção de marcas d'água digitais em imagens, vídeos ou outros recursos. As marcas d'água podem ser visíveis, ou então invisíveis pela marcação do recurso digital com algum identificador de rastreio. As marcas d'água servem para identificar quem compartilhou o conteúdo com terceiros, e assim permite o rastreamento de atividades *online*.

[9] O início de vigência da LGPD sofreu alterações, decorrentes de pressão política, sendo inclusive justificada pela pandemia de coronavírus, além de outros motivos políticos. Foi também por este motivo que alguns artigos da LGPD entraram em vigor em 2020, sendo que a vigência dos artigos que tratavam das penalidades administrativas foi postergada para 2021.

vindo de aplicativos de dispositivos móveis como *smartphones* ou *tablets*, ou ainda outros aparelhos conectados à *Internet*, como aparelhos de televisão e outros, ou ainda de outros programas de computador. Neste ponto, foram escolhidos os *websites*. Optou-se por *websites* porque eles uma fonte rica de dados, e também porque seria possível fazer comparações com outras pesquisas científicas correlatas, além de haver mais facilidade para automatizar as coletas de dados.

Especificamente sobre os *websites*, ficou decidido que apenas os *websites* brasileiros seriam analisados. Identificou-se que algumas pesquisas correlatas estudaram *websites* do mundo inteiro de forma ampla, indistintamente, e outros estudos focavam apenas em *websites* de alguns países ou continentes, sendo que não havia estudo para o Brasil que avaliasse efeitos da Lei Geral de Proteção de Dados comparando a situação anterior e posterior à sua vigência.

Foi definido também que não seria feita restrição sobre o perfil dos *websites* brasileiros na análise, isto é, que seria feito um estudo sobre *websites* de diversas áreas. Assim, não foi escolhido um setor econômico específico, como o setor financeiro, de comércio eletrônico ou de turismo. Optou-se por aumentar a escala do conjunto de dados, e desta forma quanto à quantidade de fontes de dados pesquisadas, estimou-se que seriam analisados no mínimo 1.000 *websites*.

Na seguinte fase, foi elaborada a lista de *websites* que serviriam de fonte de dados para a pesquisa. Neste ponto, aquilo que parecia mais simples se mostrou mais complexo: como obter uma lista de *websites* brasileiros? A primeira tentativa foi buscar no *website* do Comitê Gestor da *Internet* no Brasil (CGI.BR), e posteriormente no *website* do Registro.br, que é a entidade que organiza o registro de nomes de domínios que utilizam o sufixo ".br". Como o *website* do Registro.br não foi disponibilizava uma lista dos *websites* brasileiros, então foi avaliada a possibilidade de usar o serviço Alexa[10] da Amazon, que fornecia listas de nomes de domínios com vários detalhes. Este serviço estava disponível no endereço www.alexa.com à época da primeira captura de dados, e foi desativado em 01 de maio de 2022. Foi descoberto, ainda, um serviço *online* de geração de listas de nomes de domínios, denominado Tranco, disponível no endereço www.tranco-list.eu. Como algumas pesquisas sobre *cookies* feitas em 2020 e 2019 usaram esta fonte de dados, ela foi a escolhida para fornecer a lista de *sites*.

[10] Para os fins desta pesquisa, as menções a Alexa referem-se a um serviço *online* vendido pela empresa Amazon, e que foi descontinuado em 01 de maio de 2022. Este serviço *online* é diferente da assistente virtual homônima, Amazon Alexa, que por sua vez é um produto de *hardware* com tecnologia embarcada.

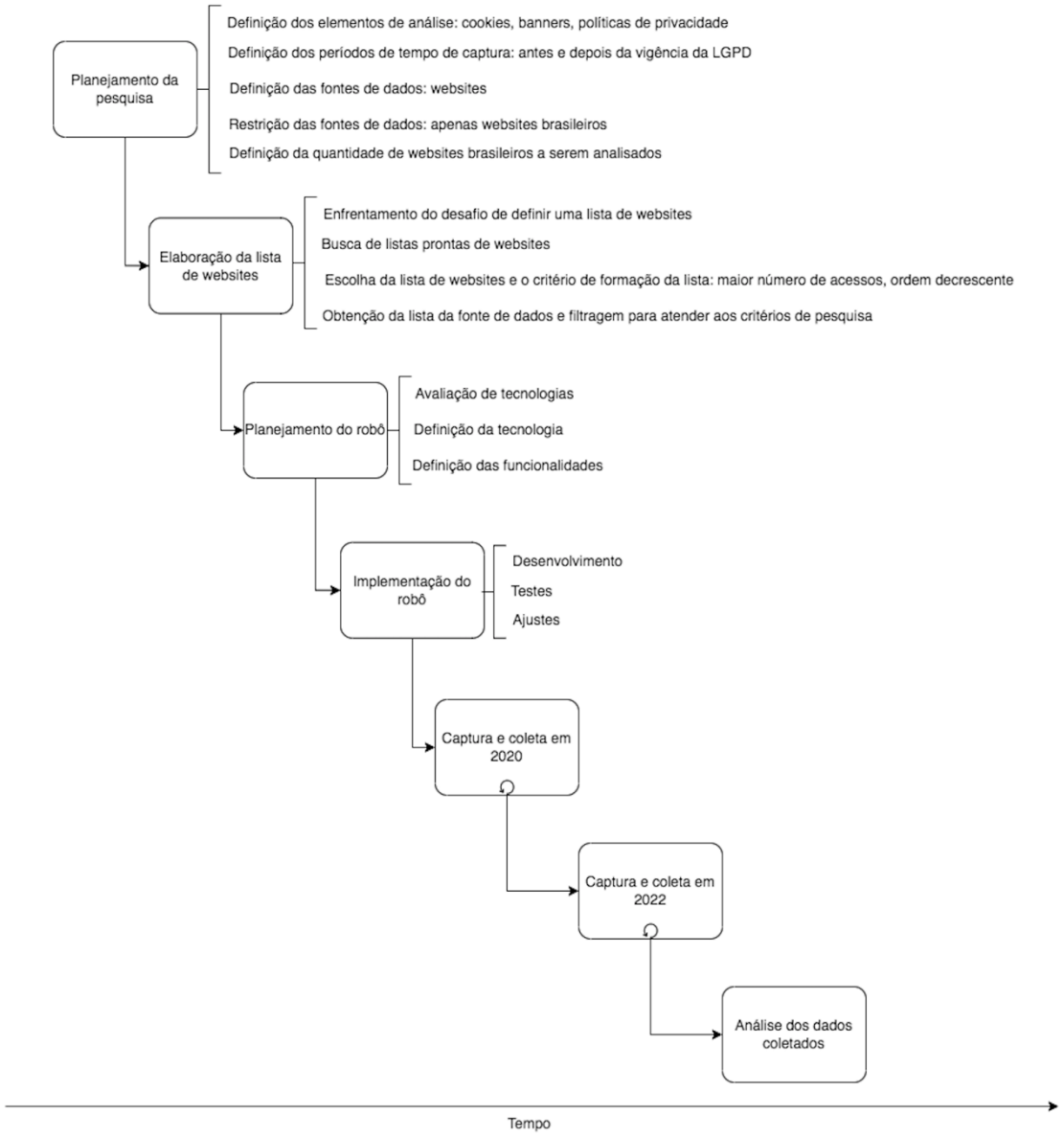


Figura 5: Fases da pesquisa
Fonte: elaborado pelo autor.

O serviço *online* Tranco é produto de um projeto de pesquisa cujo nome é: *Tranco: a research-oriented top sites ranking hardened against manipulation* (LE POCHAT *et. al.,* 2019). Em 2020, este serviço utilizava quatro fontes de dados distintas para gerar uma lista de nomes de domínio ordenadas por quantidade de acesso: Alexa, Umbrella, Quantcast e Majestic[11], e é implementado com um algoritmo que diminui a probabilidade de manipulação da quantidade de acessos dos *websites*, pois um dos problemas

[11] Alexa, Umbrella, Quantcast e Majestic eram fontes de dados que, à época, forneciam listas de nomes de domínios de *websites* mais acessados.

enfrentados pelos pesquisadores era a baixa confiabilidade dos rankings de *websites* mais acessados obtida simplesmente acessando algum dos quatro serviços acima – Alexa e outros. Assim, foi realizado um estudo e concebido um serviço *online*, além de um artigo científico, para gerar listas confiáveis de rankings de *websites* ordenados por quantidades de acessos. Então, após avaliar este serviço e o respectivo artigo, foi decidido usar o serviço *online* Tranco para gerar a lista de *websites* necessária.

Além disso, para obter a lista de *websites* brasileiros, preferiu-se obter dados de alguma fonte que usasse algum critério relevante para sua geração: maior quantidade de acessos, *websites* mais antigos ou outro critério. No caso da lista do serviço Tranco, o critério de maior quantidade de acessos foi utilizado. Como foi tomada a decisão de usar a lista Tranco, então o critério de quantidade de acessos estava implicitamente escolhido também, assim como a ordenação decrescente, em que o *website* mais acessado aparecia no início da lista, e o *website* menos acessado estava no final da lista.

A lista foi obtida em maio de 2020, com os seguintes parâmetros selecionando inicialmente a lista completa de 1 milhão de *websites* mais acessados no mundo. Obtida esta lista, o arquivo que possuía apenas duas colunas e que estava em formato CSV (*comma-separated values*) foi aberto em um editor de planilhas. Então, foi criado um filtro para separar somente aqueles *websites* que tinham a extensão ".br". A coluna que indicava a posição no ranking de *websites* também foi removida do arquivo. Assim, o arquivo ficou com apenas uma coluna e com muitas linhas, apenas com *websites* brasileiros. A nova lista, com os *websites* brasileiros já filtrados, foi armazenada em um novo arquivo em formato de texto simples. Apesar de o arquivo com a lista de *websites* não indicar a posição no ranking, os *websites* brasileiros mais acessados estavam em primeiro lugar desta lista, e os menos acessados estavam no fim do arquivo. Este arquivo, então, serviu de parâmetro para todo o restante do projeto.

A próxima fase da pesquisa serviu para o planejamento do robô de captura dos dados dos *websites* brasileiros. Duas escolhas importantes foram feitas nesta fase: sobre a tecnologia de implementação do robô, e sobre as suas funcionalidades. O robô[12], em sua essência, é um programa de computador que automatiza ações do navegador de *Internet*. Assim, o robô simula ações como se fosse um usuário humano.

[12] Um robô também é conhecido como *bot*.

Quanto às tecnologias para implementação do robô, algumas alternativas estavam disponíveis, tais como o Projeto Selenium[13] (https://www.selenium.dev), o Projeto OpenWPM[14] (https://github.com/openwpm/OpenWPM) e a biblioteca[15] Puppeteer[16] (https://pptr.dev). Como os dados de participação no mercado do *website* Statcounter indicaram que o navegador de *Internet* mais utilizado em março de 2020 no Brasil era o Google Chrome conforme a Figura 6 (STATCOUNTER, 2022), então foi descartada a possibilidade de usar o Projeto OpenWPM, pois este utilizava o navegador Firefox. E como a biblioteca Puppeteer parecia estar mais atualizada que o Projeto Selenium, então ela foi escolhida para a implementação.

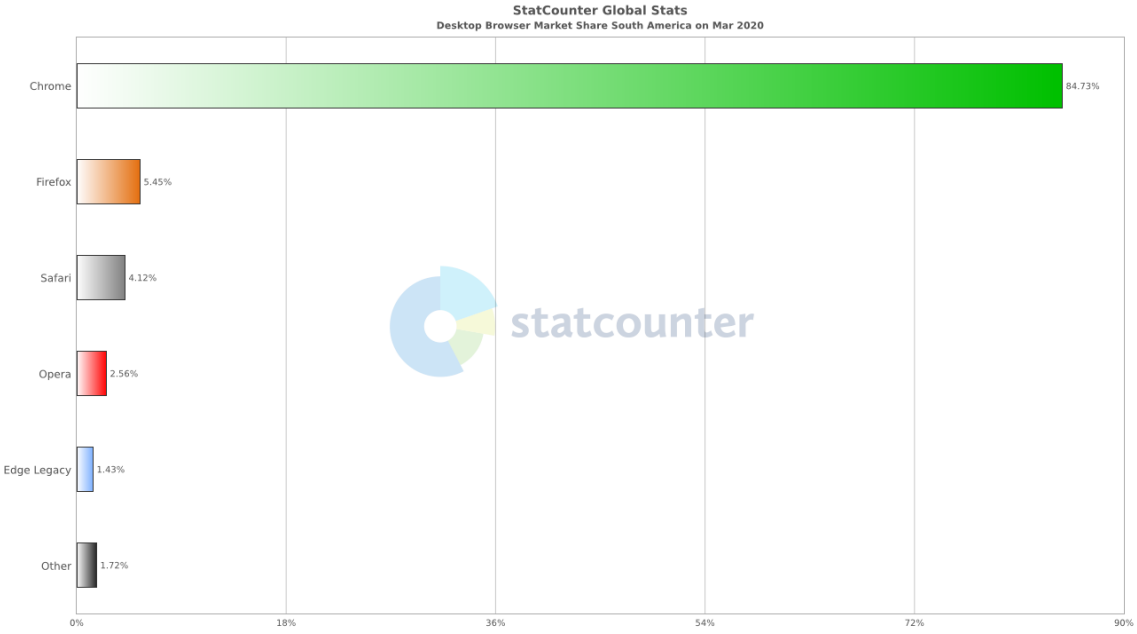


Figura 6: Participação no mercado dos principais navegadores de *Internet* em março de 2020
Fonte: STATCOUNTER, 2022.

A biblioteca Puppeteer é um conjunto de programas escritos em Javascript[17]. Os programas escritos em Javascript e que utilizam esta biblioteca Puppeteer são executados

[13] "Selenium é um projeto que abrange uma variedade de ferramentas e bibliotecas que permitem e suportam a automação de navegadores da web" (SELENIUM, 2022).
[14] "O OpenWPM é uma estrutura de medição de privacidade na Web que facilita a coleta de dados para estudos de privacidade em uma escala de milhares a milhões de *sites*. O OpenWPM é construído em cima do Firefox, com automação fornecida pelo Selenium. Inclui vários mecanismos para coleta de dados" (OPENWPM, 2022, tradução livre).
[15] Uma biblioteca é um conjunto de programas de computador prontos que podem ser facilmente executados para compor outros programas, viabilizando o reuso de código de *software*.
[16] "Puppeteer é uma biblioteca desenvolvida em tecnologia Node que fornece uma API de alto nível para controlar o Chrome ou o Chromium" (PUPPETEER, 2022, tradução livre).
[17] "JavaScript é uma linguagem de programação que permite a você implementar itens complexos em páginas web — toda vez que uma página da web faz mais do que simplesmente mostrar a você informação

em um ambiente de execução denominado Node.JS[18]. A biblioteca Puppeteer foi concebida para manipular o comportamento de dois navegadores de *Internet*, o Google Chrome e o Google Chromium. O navegador Google Chrome é o mais conhecido, porém é derivado do projeto precursor Google Chromium. Enquanto o Chrome possui tecnologia proprietária, o Chromium tem seu código aberto. Para a implementação do projeto, foi decidido que o navegador com o qual o robô interagiria seria o Chromium, pois a biblioteca Puppeteer já vem com este navegador integrado nela. Como os navegadores Chrome e Chromium são muito semelhantes, então entendeu-se mais seguro usar o Chromium durante as capturas dos *websites*.

Em seguida, as funcionalidades do robô, ou *bot*, precisavam ser especificadas. Foi definido que o robô precisaria executar atividades de *web crawling*[19] e de *web scrapping*[20]: simular a visita aos *websites*, um por vez, e esperar pelo carregamento completo do *website*, assim como capturar todos os *cookies* que foram armazenados no navegador, e ainda capturar todo o leiaute da tela exibida no navegador e as políticas de privacidade.

A próxima fase da pesquisa consistiu no desenvolvimento do robô, com atividades de programação e testes. Ao final, foram feitos ajustes para que o robô aguardasse uma quantidade máxima de segundos para a carga do *website* e então passasse para a próxima atividade. Esta fase levou em torno de 3 meses para ser executada.

Assim, a implementação do projeto foi aplicada para cada um dos *websites* presentes na lista. Passa-se agora a descrever o funcionamento do programa de computador (robô, ou *web crawler*) durante as iterações nos itens da lista de *websites* que implementou as funcionalidades necessárias.

---

estática — mostrando conteúdo que se atualiza em um intervalo de tempo, mapas interativos ou gráficos 2D/3D animados, etc. — você pode apostar que o JavaScript provavelmente está envolvido." (MOZILLA, 2022).

[18] "Como um ambiente de execução JavaScript assíncrono orientado a eventos, o Node.js é projetado para desenvolvimento de aplicações escaláveis de rede." (NODEJS, 2022).

[19] *Web crawling* é a expressão mais comumente utilizada para definir as atividades de rastreamento de *websites* que são realizadas por robôs. Por exemplo, quando um programa de computador acessa de forma automatizada um *website* por meio de um *link* de *Internet*, e depois acessa outro *link* que está dentro deste *website*, e assim por diante, então isto é uma atividade de rastreamento, ou de *crawling*. No caso desta pesquisa, quando o robô acessa um *website* e depois acessa um certo tipo de *link* dentro deste *website* em busca de informações específicas, então este robô está praticando *crawling*.

[20] *Web scrapping* é a expressão mais comumente utilizada para definir as atividades de "raspagem" de *websites*, e que também são realizadas por robôs. Um exemplo de raspagem de dados, ou *scrapping*, ocorre quando um robô acessa um *website* e captura todas as imagens e todos os textos deste *website*, armazenando em local diverso para posterior processamento.

Descrevendo de forma ampla seu funcionamento, o robô abre o arquivo que contém a lista dos *websites*. Esta lista foi criada em fase anterior, filtrando-se apenas os *websites* brasileiros a partir da lista original de *websites* mais acessados obtida do Projeto Tranco, conforme já detalhado. Após abrir o arquivo, o programa acessa cada linha da lista e, para cada nome de domínio desta lista, monta a URL[21,22] respectiva e executa o processamento individual completo que foi projetado para cada *website*. Ao atingir o final da lista, o robô simplesmente termina.

Os parágrafos seguintes detalham a metodologia de processamento adotada pelo robô para cada *website*, conforme ilustrada pela Figura 7.

No processamento individual completo projetado para cada *website*, o robô primeiro cria uma pasta com o nome do domínio do *website* a ser visitado. Em seguida, o programa robô cria uma instância do navegador Chromium para controle automatizado[23]. O robô comanda o início da captura de *cookies* que começarão a ser registrados na instância do navegador. Depois, o robô envia o comando para que o navegador acesse o *website* indicado na URL. Então, o *website* é acessado, e o programa aguarda um tempo fixo para carregamento ou um evento que identifique que a carga do *website* está completa. Isto é especialmente relevante nos *websites* que possuem páginas de rolagem contínua, como por exemplo os *websites* de notícias que vão carregando novos itens à medida que os usuários rolam as páginas para baixo. Para o objetivo deste projeto, é importante que o *website* seja carregado completamente. Carregar completamente, nos termos deste projeto, significa que não ocorre mais o fluxo de dados entre o navegador e o *website*; assim, não deve haver mais *download* de novo conteúdo, para que então o rodapé do *website* seja exibido e a captura possa ser realizada conforme planejado.

---

[21] *Uniform Resource Locator*.

[22] De forma simplificada, uma URL identifica um endereço de *Internet* para acessar um recurso disponível na rede. Para os fins desta pesquisa, uma URL pode ser construída com um protocolo de acesso ao recurso da rede e com o nome do domínio dos *websites* analisados. Por exemplo, dado o protocolo "https" e o nome de domínio "www.brasil.gov.br", então a URL será "http://www.brasil.gov.br". A especificação técnica apropriada sobre as regras de formação dos nomes de URLs pode ser acessada por meio da seguinte URL: https://datatracker.ietf.org/doc/html/rfc3986.

[23] O navegador de *Internet* é instanciado usando a biblioteca Puppeteer com o parâmetro "headless: false", o que significa que a janela do navegador será exibida na tela do computador. Isto é importante de ser observado, pois a biblioteca Puppeteer permite que o navegador seja executado sem exibir nenhuma janela para o usuário. Como será feita captura de tela posteriormente, então é fundamental que a janela do navegador seja exibida.

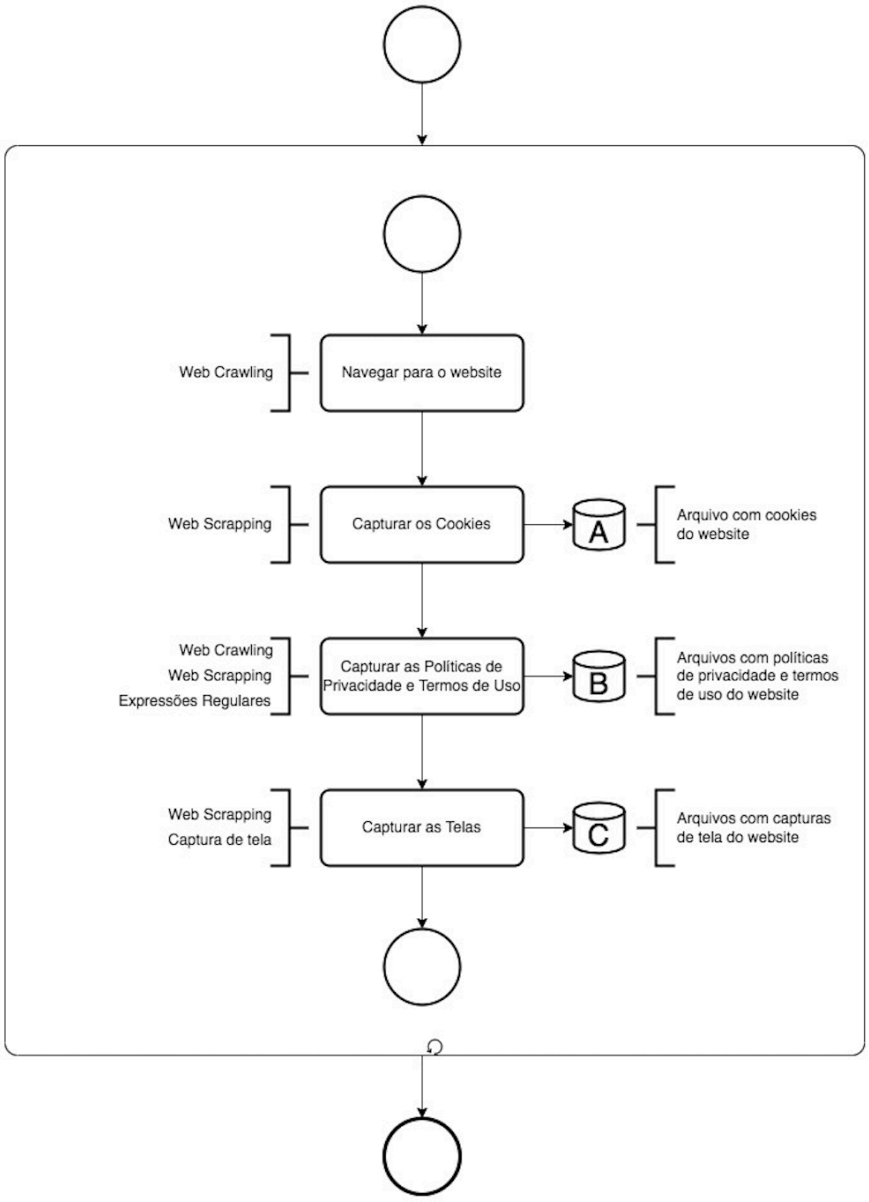


Figura 7: Esboço do fluxo do processamento individual completo para cada *website*
Fonte: Elaborado pelo autor.

Concomitantemente ao carregamento do *website*, e de forma assíncrona, o programa executa a captura dos *cookies* que são disponibilizados pelo *website* e carregados no navegador. Após o final do carregamento do *website*, por decurso do tempo ou por ocorrência do evento de fim de carga do *website*, a captura dos *cookies* para aquele *website* visitado é encerrada pelo robô. Então, os *cookies* são armazenados em uma base de dados de *cookies*, Base A[24]. A base de dados de *cookies* nada mais é do que um arquivo

[24] Para fins deste projeto, as bases que armazenam dados produzidos ou utilizados pelo programa têm identificação com letras alfabéticas, com o intuito de facilitar a compreensão.

de texto que contém todos os dados dos *cookies* que foram recebidos pelo navegador durante o carregamento do *website*.

Após navegar até o *website*, aguardar o seu carregamento completo e capturar todos os *cookies*, então o robô captura a tela que está sendo exibida no computador utilizado para a atividade. O *software* foi programado para que, no momento da captura, esteja sendo exibida somente uma aba do navegador, que é a página principal do *website* que foi carregado. A captura é feita de duas formas distintas: primeiro, é feita uma captura de tela simples, com a tela do navegador maximizada, correspondente à dimensão inteira do monitor então configurado para o computador, resultando em uma imagem de captura de tela completa convencional, em formato retangular, com as dimensões do monitor utilizado no dispositivo. Esta captura é feita para registrar exatamente aquilo que os desenvolvedores do *website* projetaram para a experiência do usuário final: o mais comum é encontrar um *website* com um cabeçalho, alguns elementos textuais e outros elementos de imagens, e na parte inferior do navegador é exibida, ou não, alguma mensagem, algum aviso, que pode ser sobre política de privacidade, *cookies* ou nenhum. A imagem gerada e capturada é então coletada pelo robô e armazenada na pasta com resultados da coleta do respectivo *website*, na Base B.

A segunda captura de tela é a captura da página inicial do *website* como um todo, uma captura de tela ampliada: neste caso, é gerada uma imagem da página inicial completa do *website*, com dimensão vertical em geral muito maior que apenas a altura do próprio monitor. Esta segunda captura de tela contém a página inteira, com toda a sua extensão de rolagem, até o rodapé do *website*. Note-se que a primeira captura, apenas daquilo que é visível para o usuário, não necessariamente contenha o rodapé – onde em geral estão contidos os *links* para a política de privacidade e outros elementos, e por este motivo foi realizada a segunda captura, que também é armazenada na base B, que fica na pasta que contém os arquivos coletados para o *website* pesquisado.

Por fim, depois de capturar as telas do *website*, o robô captura as politicas de privacidade, as politicas de *cookies* e os termos de uso dos *websites*. É comum que as politicas de privacidade sejam utilizadas para informar aos usuários quais dados pessoais são tratados e quais são as finalidades destes tratamentos. Os dados coletados podem ser dados pessoais ou não. Também é usual que as politicas de privacidade informem acerca do uso de *cookies* pelos *websites*. Há também casos em que a documentação sobre os *cookies* fica separada da política de privacidade, mantida em uma política de *cookies*, em documento apartado, ou no mesmo documento ou página do *website*. Em outros casos,

há somente o documento de política de privacidade, ou ainda apenas o documento de termos de uso ou termos de serviço, mas o conteúdo desses documentos trata de diversos assuntos separados por tópicos, ou mistura todos os assuntos indistintamente. Os termos de uso, por sua vez, têm o objetivo de apresentar os objetivos do *website* e as regras de uso que seus criadores esperam que os usuários observem, evitando assim o abuso por parte dos usuários.

Para capturar as políticas de privacidade, termos de uso e eventuais políticas de *cookies*, após o carregamento completo do *website*, o programa lê todos os *links* da página principal. Cada *link* é composto de duas informações básicas: o texto do *link* que é exibido para o usuário, e a URL que indica o caminho para o recurso que será acessado. Após a identificação de todos os *links*, o programa filtra apenas aqueles que tenham relação com políticas de privacidade, políticas de *cookies* e termos de uso. Para isto, o robô aplica um filtro criado com termos derivados de: "política de privacidade", "termos de uso" e "política de *cookies*". Também são usados nas expressões regulares criadas os termos em inglês "*privacy policy*", "*cookie policy*" e "*terms of use*" e suas derivações na forma de expressões regulares. A elaboração correta das expressões é capaz de selecionar *links* que tenham literalmente os textos acima indicados, bem como textos como "Sobre a Nossa Política", "Nossos Termos", "Nossas Regras", "Privacidade", "Sobre *Cookies*", "*About Cookies*", "*Our Policy*" e outros. O programa não diferencia letras maiúsculas de letras minúsculas e desconsidera letras acentuadas, portanto "Política de Privacidade" e "politica de privacidade" são reduzidas para a mesma expressão. Apesar de as políticas de privacidade e documentos similares terem sido coletados, eles não foram objeto de análise nesta pesquisa e serão usados em trabalho futuro.

Após aplicar o filtro, o programa cria uma nova lista com os *links* selecionados. Para cada *link* com possível política de privacidade, política de *cookies* ou termos de uso, o robô abre uma nova aba na mesma janela do navegador, acessa o *link* nesta aba, e aguarda o carregamento completo do conteúdo da nova aba ou o decurso do tempo limite definido no programa. Ao identificar o fim da carga do conteúdo da aba, o programa captura o conteúdo da aba, e o armazena em uma base de dados de políticas de privacidade, Base C. Depois do armazenamento, o robô fecha a aba do *link* respectivo e segue para o próximo *link*, se houver. Se não houver mais *links*, então encerra a tarefa de captura e coleta dos textos das políticas de privacidade. No fim desta captura textual, a Base C é formada por zero, um ou mais arquivos no formato de texto e que contêm o conteúdo textual completo das páginas dos *websites* relacionadas a políticas de

privacidade e assemelhados. Esta atividade de implementação do robô para a captura das políticas de privacidade encerrou a quarta fase da pesquisa. Ao todo, a quarta fase da pesquisa levou três meses para ser concluída, de março a maio de 2020.

A fase seguinte da pesquisa foi realizada em junho de 2020, logo após a finalização do desenvolvimento, testes e ajustes do *software*, e consistiu na execução do robô que foi programado na fase anterior.

Após a coleta dos dados de 2020, seguiu-se à próxima fase, que foi a coleta dos dados de 2022. O robô foi executado novamente em agosto de 2022, com base na mesma lista de *websites* de 2020, desta vez com um MacBook Pro Retina 2015 com 16 GB de memória principal e 250 GB de memória secundária.

Finalizada a captura dos dados de 2022, foi iniciada seguinte fase de produção de dados da pesquisa. As atividades foram as seguintes: a) categorização manual da lista dos *websites* visitados, identificando o setor de atuação a que pertenciam, como: comércio eletrônico, viagens e turismo, governo, educação, serviços, veículos e outros; b) identificação e análise das características dos *cookies* coletados; c) identificação e análise de características de avisos de *cookies* nos *website*s e nas capturas de tela; d) identificação de *websites* cuja captura ocorreu em 2020 e que não ocorreu em 2022; e) identificação do uso de sistema de gestão de consentimento nos *banners* de *cookies*; e f) cruzamento de dados entre os avisos de *cookies* e os próprios *cookies* capturados nos respectivos *sites*.

Para dar mais relevância à análise dos dados que foram coletados, os *websites* visitados precisaram ser categorizados. A categorização foi manual, foi aquela indicada anteriormente que considerava o setor de atuação do *website*.

Em busca de possíveis classificações para uso neste trabalho, identificou-se que a categorização de *websites* utilizada por Urban *et. al.* (2020) utilizou a nomenclatura fornecida pelo serviço *McAfee SmartFilter Internet Database*[25], agregando as categorias dos *website*s segundo esta base de dados. A pesquisa de Buckler *et. al.* (2020) classifica os *websites* por domínios de segundo nível, consolidando domínios em quatro categorias: *websites* governamentais pelos domínios **.gov** e **.int**, *websites* comerciais pelos domínios **.com**, **.net** e **.info**, *websites* de organizações sem fins lucrativos pelo domínio **.org** e *websites* educacionais pelo domínio **.edu**. A pesquisa de Kosta e Sørensen (2019, p. 1592) utilizou categorias com base no serviço *online* ***whois***: entretenimento, governo, serviços jurídicos, jornalismo privado, jornalismo público, serviços postais, transporte público,

[25] Este serviço estava disponível no endereço https://trustedsource.org/ e foi movido para o endereço https://sitelookup.mcafee.com/, e informa a categoria do *website* conforme a respectiva URL.

compras e viagens, universidades, previsão do tempo privada e previsão do tempo pública.

Por fim, foi definido que a forma de categorização básica escolhida para esta pesquisa foi por categorias conforme o assunto, sendo uma categorização personalizada, criada especificamente para esta pesquisa. As seguintes categorias foram identificadas no *corpus* da pesquisa e então identificadas conforme o assunto principal do *site*: Adulto, Automotivo, Comércio Eletrônico, Educação, Entretenimento, Esportes, Estilo de vida, Finanças, Governo, Imóveis, Negócios, Notícias, ONGs e outros, Pessoal, Portal de Busca, Rede Social, Religião, Saúde, Tecnologia, Transporte e Viagens.

Depois que as categorias dos *websites* foram definidas, então foi feita a categorização, tanto automática quanto manual.

O próximo passo foi a inspeção manual de todas as telas capturadas para os *websites* de 2020. A inspeção das telas capturadas em 2022 foi feita de forma semiautomatizada, da seguinte forma: os avisos de *cookies* dos *websites* consultados foram analisados individualmente em uma etapa posterior à captura dos *cookies*. Para isto, o robô foi programado para acessar cada *website* e aguardar até que o navegador fosse fechado para aquele *website*; então, após o carregamento do *site*, procedeu-se à análise visual e manual dos avisos de *cookies*. As seguintes perguntas foram respondidas: 1) o *website* possui *banner* de aviso de *cookies*? 2) se o *website* possui *banner* de aviso de *cookies*, há elementos afirmativos, negativos, informacionais e gerenciais? As telas foram avaliadas em relação ao *banner* de *cookies*, ou aviso de privacidade. A avaliação gerou planilhas contendo detalhes sobre os *banners*, utilizando critérios da pesquisa desenvolvida por Kampanos e Shahandashti (2021) e identificando se o componente tinha elementos das seguintes categorias: a) positivos; b) negativos; c) informativos; d) gerenciais. Elementos positivos são representados por botões ou outros componentes com dizeres positivos, tais como: “ok”, “sim”, “aceito”, “concordo”, “li e aceito” e similares. Elementos negativos são relacionados a itens com mensagens negativas, tais como “não aceito”, “não concordo”, “dispensar” e outros. Elementos informativos são aqueles que levam a detalhes sobre termos de uso ou políticas de privacidade, tais como os *links* que permitem o acesso a tais documentos informativos. Elementos gerenciais, por sua vez, permitem que o usuário escolha quais *cookies* ou categorias de *cookies* ele aceita ou não, dentre outras funcionalidades se existentes.

Os resultados das capturas de 2022 também foram comparados com os de 2020 para identificar quais *websites* de 2020 não estavam mais acessíveis em 2022.

Ao final, o projeto pode usar as bases de dados anteriores para produzir novos dados estatísticos como tempo médio e complexidade de leitura das políticas de privacidade. Outras perguntas que podem ser respondidas a partir dos dados capturados são, por exemplo: se as políticas de privacidade e os termos de uso estão acessíveis para os usuários na página principal dos *websites*; que tipos de dados pessoais são capturados através de *cookies* próprios e de *cookies* de terceiros; quais são os domínios dos *websites* dos *cookies* de terceiros utilizados nos *websites* brasileiros; e quais são as finalidades dos *cookies* utilizados nos *websites* brasileiros, dentre outros. Os dados produzidos podem ser armazenados na Base E.

A classificação de elementos afirmativos, negativos, informacionais e gerenciais seguiu o mesmo trabalho desenvolvido por Kampanos e Shahandashti (2021) e publicado no artigo *Accept All: The Landscape of Cookie Banners in Greece and the UK*. Tal pesquisa identificou se esses elementos estavam presentes nos avisos de *cookies* no contexto britânico e helênico.

A Tabela 1 apresenta o que são os elementos afirmativos, negativos, informacionais e gerenciais presentes nos *banners*. Os elementos encontrados foram enquadrados conforme a tabela abaixo exemplifica.

Elemento	Apresentações possíveis
Afirmativo	Botões que apresentam opção para aceitar o uso de *cookies*, como "Ok", "Sim", "Aceito", "Continuar", "Fechar", "X", "Continuar navegando", "Aceito os termos", "Aceito os *cookies*", etc.
Negativo	Botões que apresentam opção para rejeitar o uso de *cookies*, como "Não", "Não aceito os termos", "Não concordo", "Discordo", "Rejeitar", "Rejeitar todos os *cookies* não necessários", "Rejeitar todos os *cookies*", "Não permitir rastreamento" e outros.
Informacional	Botões ou *links* que levem a outro elemento que tenha informações adicionais: "Política de privacidade", "Política de *cookies*", "Clique aqui para saber mais", "Acesse nossa política de *cookies*", "Saber mais", "Nossos termos", "Mais informações" e outros.
Gerencial	Botões ou *links* que levam para o segundo nível do *banner* de *cookies* para detalhar as opções: "Gerenciar", "Preferências", "Configurações de *cookies*", "Gerenciar *cookies*" e outros.

Tabela 1: Exemplos de elementos afirmativos, negativos, informacionais e gerenciais
Fonte: elaborada pelo autor.

Esta etapa do trabalho foi feita manualmente, por inspeção visual. Nas três semanas após a coleta dos dados dos *website*s, como capturas de telas e de *cookies*, a classificação foi feita de forma manual, *site* a *site*: acessando cada um deles, avaliando os *banners*

individualmente, comparando com as possíveis apresentações acima, e tabulando os dados em uma planilha. Este trabalho foi realizado apenas por 1 pessoa, o próprio pesquisador. Posteriormente, nas duas semanas seguintes ao fim da tabulação, os dados foram integralmente revisados mais duas vezes, para identificar inconsistências. Assim, cada *website* foi visitado no mínimo 3 vezes em busca das informações sobre o primeiro nível dos avisos de *cookies*. Este trabalho sobre os elementos de primeiro nível foi feito nos dois momentos, em 2020 e 2022.

No escrutínio, foram avaliados dois níveis dos elementos dos avisos de *cookies*: inicialmente, sobre os componentes de primeiro nível, conforme acima explicado; e caso o *banner* possuísse elemento gerencial, então o segundo nível também foi analisado visualmente e os dados também foram inseridos na planilha respectiva. Para o segundo nível, três características foram buscadas: a) se havia elemento afirmativo que permitia aceitar todos os *cookies*; b) se havia elemento negativo que permitia rejeitar todos os *cookies* não necessários; e c) se os *cookies* não necessários estavam desativados por padrão. Somente foram analisados os avisos de *cookies* de 2022, pois a decisão de escopo da pesquisa à época não abrangia os avisos de *cookies* no segundo nível.

Os avisos de *cookies* que possuem elemento gerencial mostram um segundo nível de interação com o usuário, para que as opções de rastreadores de *cookies* sejam apresentadas de forma mais detalhada e assim a pessoa possa escolher o que deseja. O Guia orientativo sobre *cookies* publicado pela ANPD em 2022, que não possui caráter cogente apesar de levemente balizar práticas nesse *métier*, recomenda a implementação deste segundo nível (BRASIL, 2022d).

Cumpre ressaltar que o elemento negativo procurado foi algum mecanismo que permitisse ao usuário rejeitar *cookies* não necessários, e que o componente afirmativo deveria aceitar todos os rastreadores. Para esta pesquisa, assumiu-se ainda que as finalidades dos *cookies* necessários podem ser baseadas no legítimo interesse, mas é importante lembrar que há outras hipóteses legais que podem justificar o tratamento de dados pelo controlador, fornecedor do *website*, conforme a lei geral de proteção de dados define. Apesar de o Guia orientativo da ANPD sobre o tema apenas sugerir que *cookies* funcionais cujas funções não sejam essenciais ao funcionamento do serviço também se enquadrem como *cookies* não necessários (BRASIL, 2022d, p. 10), não há como identificar de forma simples quais rastreadores de *cookies* de finalidade funcional são ou não necessários. Por este motivo, a decisão metodológica foi a de contabilizar como não-necessários apenas os rastreadores de publicidade e os analíticos, desconsiderando os

funcionais e os necessários, obviamente. Estas últimas considerações se aplicam às três características investigadas nesta seção da pesquisa.

Durante a inspeção visual dos avisos de *cookies* nos dois níveis, a pesquisa avaliou se os avisos de *cookies* usavam língua estrangeira, tanto no primeiro quanto no segundo nível. Para indicar o uso de língua estrangeira, foi usado como critério a presença de sentenças de textos em outras línguas tanto no primeiro quanto no segundo nível, e a disponibilização de *links*, nos dois níveis, para recursos externos em língua estrangeira. Pequenos estrangeirismos, como "Ok" ou "*cookies*" foram desconsiderados. Nos casos de emprego de outro idioma, o item foi contabilizado na planilha.

Em seguida, os avisos de *cookies* também foram avaliados na sua implementação quanto ao uso de CMPs (*Consent Management Platforms*), e os dados foram tabulados na planilha respectiva.

5 RESULTADOS DA PESQUISA EMPÍRICA

Este capítulo apresenta os resultados das capturas de dados dos *website*s que foram realizadas em 2020 e em 2022. A primeira captura ocorreu em junho de 2020, portanto antes do início da vigência da Lei Geral de Proteção de Dados, agosto de 2020. A segunda captura foi feita em setembro de 2022, dois anos após a vigência do referido diploma legal. A lista de *website*s utilizada nas duas capturas foi a mesma, obtida do *website Tranco Project* em maio de 2020. Nos dois casos, o robô capturou os *cookies*, tirou fotografia das telas dos *website*s, identificou coletou e armazenou os textos das políticas de privacidade, políticas de *cookies* e termos de uso, e também obteve arquivo de *log* – gerado pelo navegador – sobre a conexão feita entre o computador de pesquisa e os *website*s investigados. Em seguida, foi feita a análise manual das capturas de tela do ano de 2020 em busca de informações sobre os avisos de *cookies* nelas presentes. E após a captura automática dos dados dos *website*s de 2022, foi feita uma análise manual de cada *website* quanto aos avisos de *cookies*, conforme já explicado no capítulo sobre metodologia.

Inicialmente, serão apresentados os dados de pesquisa relacionados aos *cookies* dos *website*s pesquisados, e ao longo do texto também serão apresentados comentários sobre os achados de pesquisa. Da mesma forma, os dados produzidos sobre os avisos de *cookies* serão apresentados assim como os respectivos comentários. Conforme já explicado, apesar de ter sido feita a captura, as políticas de privacidade, as políticas de *cookies* e os termos de uso estão fora do escopo desta pesquisa.

Ao longo dos três dias em que o robô foi executado, foram visitados ao todo 1.282 *website*s. Destes, 94 *website*s não foram encontrados por diversas razões por exemplo: *website* com mensagem “em construção” ou “fora do ar”, *website* indisponível com erro HTTP 404 (mensagem padrão do protocolo HTTP que informa que o recurso não foi encontrado, que não existe), *website* inacessível por outro motivo, como acesso proibido com erro 403 (outra mensagem padrão que indica que o agente não possui permissão para acessar aquele recurso), e diversos outros motivos, tais como *website* inacessível, suspenso, sem acesso, *website* que exigia senha ou ainda que redirecionava para conta de rede social. Uma razão peculiar para alguns *website*s não terem sido encontrados foi a detecção, por parte do sistema, que o agente que estava realizando o acesso era controlado por um robô. O acesso também foi feito com o protocolo HTTP (*e.g.*:

http://www.*website*A.com.br), e não com o protocolo HTTPS (*e.g.*: https://www.*website*A.com.br), porém este aspecto não foi avaliado no trabalho. Também não foi avaliado se o *website* redirecionava para o mesmo endereço com o protocolo HTTPS.

Por estas justificativas, em 2020 não foram encontrados 94 *website*s, e em 2022 não foram encontrados 122 *website*s. Uma razão natural para o aumento de *website*s que não foram encontrados é a simples desativação dos endereços, por motivos diversos atinentes ao domínio do respectivo negócio. Apesar disto, houve alguns casos em que os *website*s foram encontrados em 2022, mas não em 2020, e provavelmente isto se deve a uma indisponibilidade momentânea do sistema.

Assim, em 2020 foram encontrados 1.188 *website*s, e 1.160 em 2022, totalizando 2.348 *website*s encontrados, e que compõem integralmente o *corpus* desta pesquisa. Ao longo dos dois anos de pesquisa, foram então visitados 2.564 endereços.

***Website* encontrado?**	**2020**	**2022**	**Total Geral**
Não	94	122	216
Sim	1188	1160	2348
Total Geral	1282	1282	2564

Tabela 2: Tamanho do *corpus* de pesquisa quanto ao número de *websites*
Fonte: elaborada pelo autor.

A Tabela 2 mostra o perfil dos *website*s pesquisados quanto à categoria em que foram classificados. Foi utilizada a lista de *website*s fornecida pelo Tranco Project, que cria um *ranking* dos *website*s mais acessados no mundo. Como foi feita uma filtragem por TLD[26] (*Top-Level Domain*) com extensão ".br", outros endereços que possivelmente eram mais acessados no Brasil e que terminavam em ".com", por exemplo, ficaram de fora da análise. Percebe-se que, assim, a maior parte dos *website*s acessados que têm extensão ".br" são *sites* de notícias, em seguida vêm os de educação, os de governo e assim por diante.

Conforme a Tabela 3, os *website*s da categoria Notícias dominam o *corpus* da pesquisa dos *sites* mais acessados, seguidos pelos de Educação, Governo, Negócios e

[26] TLD é o acrônimo para *Top Level Domain*. Na url https://www.google.com.br, o TLD é ".br", o *hostname* é "www.google", e o TLD+1 é "google". Da mesma forma, no endereço https://app.ieee.org, o TLD é ".org", o *hostname* é "app.ieee", e o TLD+1 é "ieee". TLD indica o primeiro nível (mais alto) na hierarquia da nomenclatura, e TLD+1 se refere ao segundo nível do domínio.

Comércio Eletrônico. Juntas, estas 5 categorias representam mais de 50% de toda a massa de pesquisa.

Categoria do *website*	2020	2022
Notícias	217	217
Educação	158	160
Governo	153	146
Negócios	130	123
Comércio Eletrônico	128	121
Finanças	82	83
Tecnologia	80	77
Entretenimento	56	53
ONGs e outros	42	40
Saúde	21	20
Viagens	21	20
Portal de Busca	17	17
Estilo de vida	16	16
Automotivo	15	16
Religião	11	11
Imóveis	9	10
Adulto	8	8
Esportes	8	7
Rede Social	8	8
Transporte	6	5
Pessoal	2	2
Total Geral	1188	1160

Tabela 3: Tamanho do *corpus* de pesquisa considerando apenas *websites* encontrados
Fonte: elaborada pelo autor.

5.1 Resultados sobre os avisos de *cookies*

Este tópico apresenta os resultados da pesquisa empírica dos dois momentos da coleta de dados, tais como a prevalência de avisos de *cookies* nos *sites*, a estratificação dessa prevalência por categoria de *website* e a presença de certos elementos que compõem os avisos. Também descreve os perfis de avisos que foram identificados nos dados coletados, mostra os percentuais de *website*s que adotam determinadas práticas como *cookie wall*, consentimento tácito, manipulação de elementos visuais para conferir destaques, uso de língua estrangeira nos avisos de rastreadores de *cookies*, percentuais de interfaces que apresentam segundo nível para ajustar preferências de rastreamento e respectivas características, como a pré-seleção de rastreadores não essenciais, e também

apresenta a participação de CMPs nos *website*s brasileiros. Por fim, o tópico também mostra o cruzamento entre os perfis de primeiro e segundo nível, para identificar o grau de conformidade dos *website*s com boas práticas relacionadas aos avisos de *cookies*.

A Tabela 4 mostra, em valores absolutos e percentuais, as quantidades de *website*s que têm avisos de *cookies* durante os dois períodos de captura dos dados. Em 2020, apenas 6,9% dos *website*s pesquisados apresentavam avisos de *cookies*; este número subiu para 55,17% em 2022. Então, nota-se que houve aumento significativo no emprego deste tipo de recurso para o usuário da *Internet*.

Há aviso de *cookies*	**2020**	**2022**	**%2020**	**%2022**
Não	1106	520	93,10%	44,83%
Sim	82	640	6,90%	55,17%

Tabela 4: *Websites* com aviso de *cookies* por ano
Fonte: elaborada pelo autor.

A pesquisa desenvolvida por Kampanos e Shahandashti (2021), feita num *corpus* de 17.737 *websites*, apontou que 48% dos *sites* pesquisados da Grécia e 44% dos *sites* do Reino Unido apresentavam avisos de *cookies*, totalizando algo próximo de 45% considerando os dois países analisados.

Degeling *et. al.* (2018), no artigo *We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy*, estudaram 6.759 *website*s de 28 países da União Europeia para descobrir se houve mudanças no ambiente *online* após a vigência da GDPR, comparando os períodos de janeiro de 2018 (antes) e maio de 2018 (depois da GDPR). Em janeiro daquele ano, 46,1% dos *sites* pesquisados tinham aviso de *cookies*, e em maio de 2018 o percentual subiu para 62,1%.

Klein *et. al.* (2022) criaram um mecanismo de identificação de avisos de *cookies* e de consentimento automático para testar ataques de "roubo de sessão". Foram visitados 23.113 *website*s com TLD de países da União Europeia, além dos TLDs **.uk**, **.com**, **.net** e **.org**. Avisos de *cookies* foram identificados em 8.149 *sites*, resultando em 35,26% de *sites* com esses *banners*.

Khandelwal *et. al.* (2022) desenvolveram um sistema de detecção automática de avisos de *cookies* que desabilita aqueles não-essenciais. Usando os 5.000 *website*s mais populares conforme lista obtida do projeto Tranco, a pesquisa avaliou 3.547 endereços acessíveis a partir do Reino Unido e dos Estados Unidos, e identificou a presença de *banners* de marcadores de *cookies* e outras características desses *banners*. Foram

escolhidos os primeiros 5.000 *sites* da lista da Tranco – que estima os endereços mais acessados no mundo – dos quais 3.547 estavam disponíveis. Os pesquisadores ressaltaram que, quando visitados a partir do Reino Unido e dos Estados Unidos, os avisos de *cookies* foram apresentados em 53% e 25% dos *sites*, respectivamente.

Krisam *et. al.* (2021) analisaram 500 *website*s da Alemanha em busca de informações sobre os padrões de avisos de *cookies* e identificaram que 65,6% dos *sites* apresentavam aviso de *cookies*.

Uma das razões de o percentual brasileiro ter sido maior do que o resultado de Kampanos e Shahandashti (2021) é o tamanho da amostra: nesta pesquisa brasileira, foram avaliados 1.282 *website*s, e naquela pesquisa foram 17.737 *sites*, razão inclusive aventada por aqueles pesquisadores quando compararam com outros estudos da mesma natureza.

No caso da pesquisa de Klein *et. al.* (2022), o percentual de *sites* com aviso de *cookies* pode ter sido mais baixo porque foi desenvolvido focado em *banners* do tipo CMP (*Consent Management Platform*), que implementam o protocolo TCF (*Transparency Consent Framework*) proposto pela IAB (*Interactive Advertising Bureau*).

O trabalho de Khandelwal *et. al.* (2022) apresentou 53% de avisos de *cookies* nos 3.547 *sites* mais procurados no mundo, quando o acesso foi feito a partir do Reino Unido, que – assim como a União Europeia – tem um *enforcement* maior do que em outros países.

O resultado de Krisam *et. al.* (2021) segundo o qual 65,6% dos *sites* apresentam avisos de *cookies*, pode ter sido mais alto porque foram visitados apenas 500 *websites*, e também porque eram os mais acessados segundo o *ranking* organizado por Alexa Top *sites*.

A Tabela 5 estratifica os totais acima apresentados por categoria de *website*. De 2020 a 2022, houve mudança em todas as categorias, com destaque para portais de busca que não apresentaram mais os avisos, e os *website*s de governo que empregaram proporcionalmente menos avisos – em comparação às outras categorias que têm proporcionalmente mais *website*s, com 39,84%. Exceto para portais de busca, todas as outras categorias aumentaram a aplicação de avisos de *cookies*.

Para fins de comparação com outras pesquisas, a análise dos elementos dos avisos de *cookies* foi realizada de forma a permitir algumas comparações com outros trabalhos, tais como aquele desenvolvido por Kampanos e Shahandashti (2021), conforme descrito no capítulo de metodologia. Nele, os pesquisadores identificaram elementos afirmativos,

negativos, informacionais e gerenciais. Da mesma forma, a presente pesquisa utilizou os mesmos parâmetros para permitir medir as diferenças entre os estudos.

	2020					2022				
	Tem *banner*?					Tem *banner*?				
Categoria	**Não**	**Sim**	**% Não**	**% Sim**	**Total**	**Não**	**Sim**	**% Não**	**% Sim**	**Total**
Notícias	203	14	93,55%	6,45%	217	114	103	52,53%	47,47%	217
Educação	153	5	96,84%	3,16%	158	55	91	55,00%	45,00%	146
Governo	151	2	98,69%	1,31%	153	30	91	60,16%	39,84%	121
Comércio Eletrônico	122	6	95,31%	4,69%	128	88	72	37,67%	62,33%	160
Negócios	120	10	92,31%	7,69%	130	18	65	41,56%	58,44%	83
Tecnologia	72	8	90,00%	10,00%	80	74	49	24,79%	75,21%	123
Finanças	70	12	85,37%	14,63%	82	32	45	54,72%	45,28%	77
Entretenimento	50	6	89,29%	10,71%	56	29	24	21,69%	78,31%	53
ONGs e outros	39	3	92,86%	7,14%	42	17	23	42,50%	57,50%	40
Saúde	19	2	90,48%	9,52%	21	3	13	45,00%	55,00%	16
Viagens	18	3	85,71%	14,29%	21	5	12	56,25%	43,75%	17
Portal de Busca	14	3	82,35%	17,65%	17	8	12	100,00%	0,00%	20
Automotivo	12	3	80,00%	20,00%	15	9	11	40,00%	60,00%	20
Estilo de vida	12	4	75,00%	25,00%	16	9	7	62,50%	37,50%	16
Religião	11		100,00%	0,00%	11	5	6	45,45%	54,55%	11
Imóveis	9		100,00%	0,00%	9	5	5	50,00%	50,00%	10
Esportes	8		100,00%	0,00%	8	3	4	29,41%	70,59%	7
Adulto	8		100,00%	0,00%	8	2	3	18,75%	81,25%	5
Rede Social	7	1	87,50%	12,50%	8	5	3	42,86%	57,14%	8
Transporte	6		100,00%	0,00%	6	1	1	40,00%	60,00%	2
Pessoal	2		100,00%	0,00%	2	8		50,00%	50,00%	8
Total Geral	1106	82	93,10%	6,90%	1188	520	640	44,83%	55,17%	1160

Tabela 5: *Websites* com aviso de *cookies* por ano e categoria
Fonte: elaborada pelo autor.

O gráfico mostra a presença individual dos elementos afirmativos, negativos, informacionais e gerenciais nos avisos de *cookies*, ou *banners* de *cookies*. Como já apresentado, elementos afirmativos servem para que o usuário comunique a intenção de concordar com o conteúdo apresentado no aviso, elementos negativos existem para rejeitar opção trazida pelo *site*, elementos informativos fornecem mais transparência sobre políticas de privacidade, políticas de *cookies* e outros; e os elementos gerenciais permitem que o usuário configure o que ele quer aceitar ou rejeitar individualmente, com maior granularidade.

Conforme as informações da Figura 8, todos os *website*s apresentavam elementos afirmativos (100%) nos avisos de *cookies* capturados no ano de 2022. Elementos

informativos também estavam presentes na grande maioria dos avisos (86,41%). Elementos gerenciais foram encontrados em menor quantidade nos *banners* dos *sites* (32,19%), e apenas 21,25% deles tinham elementos negativos.

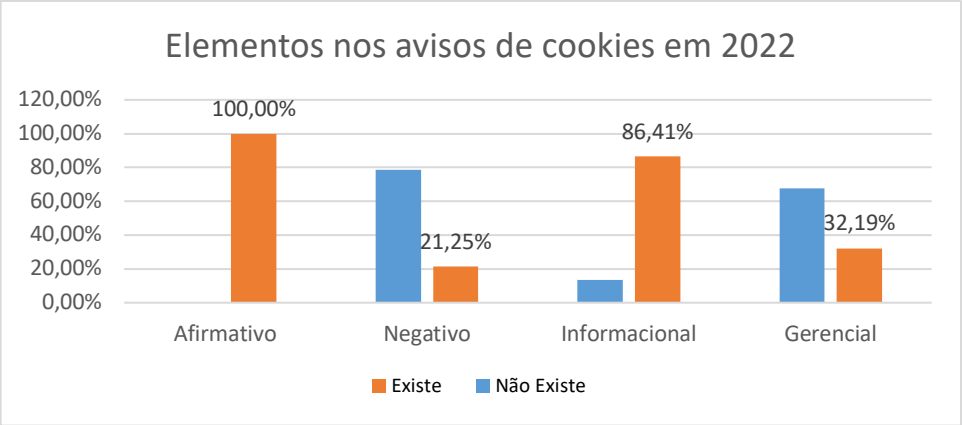


Figura 8: Elementos de primeiro nível nos avisos de *cookies* em 2022
Fonte: elaborada pelo autor.

Na pesquisa de Kampanos e Shahandashti (2021), os percentuais de presença dos mesmos elementos na Grécia e Reino Unido foram de: 95 e 88% (afirmativo), 20 e 6% (Negativo), 40 e 20% (Informacional), e 50 e 69% (Gerencial). A Tabela 6 mostra semelhança no elemento afirmativo entre Brasil e Grécia e no elemento negativo entre Brasil e Reino Unido. Os elementos informacional e gerencial têm maior discrepância entre as duas pesquisas.

Elemento	Brasil	Grécia	Reino Unido
Afirmativo	100%	95%	88%
Negativo	21,25%	20%	6%
Informacional	86,41%	40%	20%
Gerencial	32,19%	50%	69%

Tabela 6: Comparação com os resultados da presente pesquisa (Brasil) com aqueles obtidos por Kampanos e Shahandashti (2021) sobre Grécia e Reino Unido
Fonte: elaborado pelo autor e utilizando dados de Kampanos e Shahandashti (2021)

Segundo Kampanos e Shahandashti (2021), na Grécia e no Reino Unido é mais fácil ajustar as preferências de *cookies* do que rejeitar o rastreamento, pois 59% e 69% têm opção gerencial, e 20% e 6% têm opção negativa, respectivamente. No Brasil, modificar as configurações de *cookies* é um pouco mais fácil do que rejeitar o rastreamento (32,19% e 21,25%). Todavia, modificar essas preferências no Brasil é bem mais difícil do que na Grécia e no Reino Unido (32,19%, 50% e 69%). Para Nouwens *et.*

al. (2020), permitir gerenciar preferências de *cookies* no primeiro nível diminui o consentimento entre 8% e 20%.

Nouwens *et. al.* (2020) também analisaram o design dos avisos de *cookies* do tipo CMP dos 10.000 *website*s mais populares do Reino Unido. A ferramenta construída durante aquela pesquisa conseguiu identificar automaticamente CMPs em 680 desses *sites* (6,8% do total), e foi contabilizado que 74,3% dos botões de rejeitar tudo estavam no segundo nível; assim, complementarmente 25,7% (100% - 74,3%) é o limite máximo de presença dos botões de rejeitar tudo no primeiro nível, pois há casos em que não há botões de rejeição. Este percentual de 25,7% se aproxima do que foi medido na presente pesquisa (21,25%).

Na pesquisa, Nouwens *et. al.* (2020) identificaram que 50,1% dos *banners* não tinham botão para rejeitar. A pesquisa brasileira por sua vez computou que, no primeiro e segundo níveis, 75,00% dos avisos não tinham elemento negativo, conforme a Tabela 7, correspondentes aos avisos que não tem elemento negativo no primeiro nível, e nos quais não há segundo nível, ou se houver então não têm o elemento no segundo nível. Assim, o caso brasileiro tem percentuais piores que o britânico.

Elemento negativo no primeiro nível	**Elemento negativo no segundo nível**		**Tem segundo nível**
	Não	**Sim**	
Não	12,19%	3,75%	62,81%
Sim	3,91%	12,34%	5,00%

Tabela 7: Avisos de *cookies* que têm elemento negativo
Fonte: elaborada pelo autor.

Ainda na pesquisa de Nouwens *et. al.* (2020): em 93,1% dos casos, somente o primeiro nível do aviso foi visitado, significando que o nível gerencial é pouco usado; 89,3% dos participantes optou por aceitar tudo ou rejeitar tudo, sem mudar preferências e sem apenas aceitar ou rejeitar a configuração padrão; 55,2% aceitaram todos os rastreadores, 34,1% rejeitaram todos, e 0,9% não interagiram com o aviso. Tais percentuais expõem a preferência dos usuários pela menor interação com a interface e o baixo uso dos recursos postos à disposição. A partir disto, é possível compreender a importância do *Privacy by Default*, por configurações padrão que privilegiem a privacidade. Para os mesmos autores, avisos de *cookies* que não têm o elemento negativo no primeiro nível (botão para rejeitar o rastreamento) contribuem para o aumento do consentimento entre 22% e 23.

Com base na existência dos elementos anteriormente indicados em cada aviso de *banner*, foi possível criar combinações entre eles, criando assim perfis dos avisos de *cookies*. Na Tabela 8, as letras das combinações são formadas como explicado aqui. “A”: existe elemento afirmativo; “N”: existe elemento negativo; “G”: existe elemento gerencial; “I”: existe elemento informacional; “x”: não existe o elemento respectivo. Como são 4 tipos de elementos que podem ter apenas 2 tipos de valores, “sim” ou “não”, então o número máximo de combinações possíveis é 2^4, totalizando até 16 combinações possíveis. Ao todo, porém, foram encontradas 10 combinações entre os elementos, que permitiram analisar a prática da adoção de avisos de *cookies* no Brasil para os *website*s deste trabalho. Nas análises a seguir que envolvem os perfis de *banners*, é utilizado o identificador “?” para indicar que, naquela posição, qualquer valor pode estar presente. Por exemplo, A-N-?-I significa que na posição “?” podem estar presentes os valores “G” ou “x”.

Combinação dos elementos de primeiro nível	2020	2022
A-N-G-I	0,00%	13,44%
A-N-G-x	1,22%	2,81%
A-N-x-I	3,66%	3,44%
A-N-x-x	1,22%	1,56%
A-x-G-I	15,85%	11,41%
A-x-G-x	6,10%	4,53%
A-x-x-I	63,41%	58,12%
A-x-x-x	6,10%	4,69%
x-x-x-I	2,44%	0,00%

Tabela 8: Distribuição das combinações de elementos de primeiro nível dos avisos de *cookies*
Fonte: elaborada pelo autor.

A combinação ideal de avisos de *cookies* é a da primeira linha da tabela: A-N-G-I, que apresenta todos os elementos que permitem que o usuário aceite ou rejeite as condições do aviso de *cookies*, informe-se mais a respeito para decidir sobre isto, ou configure suas preferências sobre o assunto trazido no aviso de *cookies*. Esta é a segunda combinação mais popular, pois estava presente em 13,44% dos avisos encontrados em 2022, sendo que em 2020 este perfil de aviso não existia nos mesmos *website*s. O Guia orientativo sobre *cookies* e proteção de dados pessoais publicado pela ANPD, inclusive, faz recomendações neste sentido para que os componentes dos avisos tenham todas essas

funcionalidades, de modo que os direitos dos titulares de dados pessoais possam ser exercidos mais plenamente (BRASIL, 2022d).

O perfil de *banner* que tem maior prevalência dentre os avisos analisados é aquele que apresenta dois elementos: o afirmativo e o informativo, A-x-x-I. Este perfil também era o mais comum em 2020, e continua sendo em 2022: 58,12% dos *website*s usam este modelo. Do ponto de vista de implementação do componente de *software*, é o mais simples de ser desenvolvido, pois o intuito maior deste perfil é o de comunicar o usuário sobre o uso de *cookies* – elemento informativo – fornecendo um *link* ou um botão para navegar até alguma política de *cookies* ou de privacidade antes de decidir. Neste perfil, o elemento afirmativo tem mais o objetivo de retirar o aviso exibido do que propriamente de registrar o aceite.

No artigo de Nouwens *et. al.* (2020), foi identificado que quanto mais possibilidades de escolha em relação ao consentimento (preferências) no primeiro nível, o consentimento cai de 8 a 20%. Também foi contabilizado que somente 12,6% tinham um botão para rejeitar com a mesma ou melhor acessibilidade (número de cliques igual ou menor) que o botão de aceitar. Na presente pesquisa, esta métrica corresponde a todos os perfis que têm A-N-?-?, onde "?" corresponde a G, I ou x neste caso, e o percentual aqui medido é de 11,72%. Assim, os valores identificados no Brasil em 2022 são muito próximos àqueles medidos no Reino Unido em 2020.

Para Kampanos e Shahandashti (2021), grande parte dos avisos influencia o comportamento dos usuários em desfavor da privacidade na Grécia e Reino Unido, sendo que respectivamente: o perfil A-M- está presente em 32% e 47% dos casos naqueles países (corresponde a A-x-G-x no Brasil, com 6,10% e 4,53% em 2020 e 2022); o padrão que influencia o comportamento para consentimento, sem elemento negativo, ou ?-??, é encontrado em 75% e 82% dos casos (corresponde a ?-x-?-? no Brasil, com); e 75% e 84% dos avisos não têm opção negativa em igualdade com a afirmativa (uma das opções não existe ou não está no mesmo nível).

A pesquisa de Khandelwal *et. al.* (2022) para Reino Unido e Estados Unidos mostrou que os avisos de *cookies* não disponibilizavam opções de escolha ao usuário em 18% e 31% dos casos respectivamente, mostrando apenas um botão para aceitar o rastreamento. No Brasil, a situação é pior: pela Tabela 9, a impossibilidade de escolha afeta 78,75% dos casos. Esta tabela também compara os estudos de Degeling *et. al.* (2018), Kampanos e Shahandashti (2021) e esta pesquisa do Brasil, por meio de

correspondências entre perfis identificados: dentre os perfis trazidos acima, os prevalentes em todas as pesquisas são aqueles que apenas permitem confirmação do rastreamento, sem possibilidade de *opt-out*. Apesar de no caso brasileiro terem sido avaliados 640 avisos de *cookies*, o percentual de 78,75% encontrado se aproxima dos resultados de Kampanos e Shahandashti (2021), que ficam entre 75% e 82%, calculados com base em aproximadamente 8 mil *website*s (aproximadamente 45% de 17.787 tinham *banners* de rastreamento).

Degeling *et. al.*	**Grécia**	**Reino Unido**	**Kampanos e Shahandashti**	**Grécia**	**Reino Unido**	**Pesquisa Atual**	**2020**	**2022**
No Option	20%	40%	--??	5%	12%	x-x-?-?	2,44%	0,00%
Confirmation Only	65%	35%	A-??	75%	82%	A-x-?-?	91,46%	78,75%
Binary	4%	5%	AN??	20%	5%	A-N-?-?	6,10%	21,25%

Tabela 9: Comparação com os resultados da pesquisa atual (2020 e 2022) para o Brasil com aqueles obtidos por Kampanos e Shahandashti (2021) e Degeling *et. al.* (2018) sobre Grécia e Reino Unido
Fonte: elaborado pelo autor e utilizando dados de Kampanos e Shahandashti (2021) e Degeling *et. al.* (2018)

Nouwens *et. al*. (2020) encontraram 75% de casos que atendem ao critério *Reject as easy as accept* (mesmo número de cliques para as duas opções); Kampanos e Shahandashti (2021) encontraram 84%, e nesta pesquisa do Brasil, 16,25% dos avisos de *cookies* têm igualdade nas opções de aceitar e rejeitar rastreamento para suprir o critério de comparação.

Quantidade de elementos do aviso de *cookies*	**Kampanos e Shahandashti**		**Pesquisa Atual**	
	Grécia	**Reino Unido**	**2020**	**2022**
Sem elementos	0,3%	1%	0,00%	0,00%
1 elemento	22%	29%	8,54%	4,69%
2 elementos	57%	58%	70,73%	64,21%
3 elementos	20%	12%	20,73%	17,66%
4 elementos	4%	0,7%	0,00%	13,44%

Tabela 10: Comparação da quantidade de elementos com os resultados da pesquisa atual (2020 e 2022) para o Brasil com aqueles obtidos por Kampanos e Shahandashti (2021)
Fonte: elaborado pelo autor e utilizando dados de Kampanos e Shahandashti (2021)

Para Kampanos e Shahandashti (2021), a média de quantidade de elementos nos *banners* era de 2,1 na Grécia e 1,8 no Reino Unido, respectivamente. No caso do Brasil, em 2020 a média era de 2,1 e em 2022 subiu para 2,4. A Tabela 10 mostra que nas duas

pesquisas os avisos de *cookies* com 2 opções prevalecem; na pesquisa atual, aumentou o número de componentes de 2020 para 2022.

A Tabela 11 apresenta alguns dos perfis de *banners* de *cookies* identificados na pesquisa.

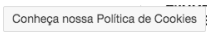
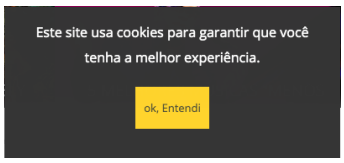
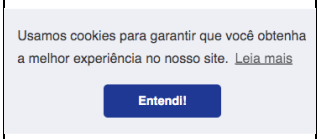
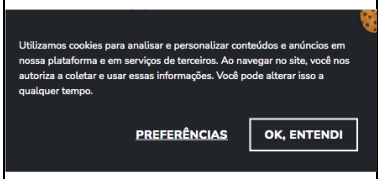
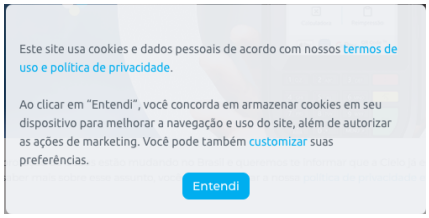
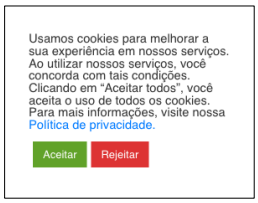
Perfil 1: x-x-x-I	Perfil 2: A-x-x-x	Perfil 3: A-x-x-I
		
Perfil 4: A-x-G-x	**Perfil 5: A-x-G-I**	**Perfil 6: A-N-x-x**
		
Perfil 7: A-N-x-I	**Perfil 8: A-N-G-x**	**Perfil 9: A-N-G-I**
		

Tabela 11: Perfis de avisos de *cookies* dos *websites* brasileiros
Fonte: elaborada pelo autor.

O próximo perfil mais frequente nos *sites* tem a combinação A-x-G-I: tem elementos afirmativos, informativos e gerenciais, e só não fornece a opção negativa. A implementação de um componente gerencial de consentimento é muito mais complexa do que o fornecimento de uma opção direta para rejeitar o consentimento. Com base nisto, é interessante notar que o controlador do *website* decidiu, no mínimo, dificultar que o usuário rejeite o emprego de *cookies* na sua visita ao *website*.

O perfil A-x-x-x, presente em 2,59% dos *sites*, apenas comunica ao usuário que o *website* utiliza *cookies*, e não fornece mais informações sobre o assunto, nem indica algum *link* para isto. O perfil A-x-G-x também dificulta a escolha do usuário do *website*, pois não fornece opção para rejeitar *cookies*, nem opção para ter mais informações sobre o assunto, a não ser que se adentre na opção gerencial. Por fim, avisos de *cookies* que apresentam elementos afirmativos, negativos e informativos, sem elementos gerenciais – perfil A-N-x-I, ao menos aparentemente fornecem ferramentas básicas, necessárias, mas não suficientes, para que o usuário exerça suas escolhas.

Kulyk *et. al.* (2018) agruparam os perfis de *banners* de *cookies* em 5 (cinco) grupos – denominados *Group* 1 a *Group* 5 – também de acordo com os seus conteúdos, porém focando mais na mensagem contida no primeiro nível, de acordo com a profundidade da mensagem, desde o *banner* que apenas informava sobre o uso de *cookies*, passando por aquele que mencionava as finalidades de uso dos rastreadores – analíticos ou publicidade – até aqueles que apresentavam detalhes sobre os propósitos dos *cookies* e que também comunicavam sobre o compartilhamento desses dados com terceiros.

Degeling *et. al.* (2018), no artigo *We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy*, identificaram os seguintes perfis de *banners*: *No Option*, *Confirmation*, *Binary*, *Slider*, *Checkbox-based* e *Other*. Esta categorização levou em consideração os tipos de componentes visuais de interface, tais como botões, caixas de verificação (*checkboxes*), barras de rolagem (*sliders*) e outros. *No Option* não possibilitava aceitar ou rejeitar; *Confirmation* permitia somente aceitar; *Binary* mostrava duas opções, aceitar e rejeitar; *Slider* criava uma hierarquia entre as finalidades de *cookies*, permitindo a seleção cumulativa; e *Checkbox-based* mostrava finalidades de uso dos rastreadores, que poderiam ser escolhidas uma a uma; e *Vendor* permitia a seleção de *cookies* com base no fornecedor do *cookie*, como pelo nome da empresa que faz o rastreamento (Google, Facebook *et cettera*).

O trabalho de Degeling *et. al.* (2018, p. 11) mostra que o perfil de *banner* prevalente é *Confirmation Only*, seguido por *No Option* e *Checkbox-based* em terceiro. Nesta pesquisa brasileira, *No Option* equivale ao padrão x-x-x-I, e a comparação é intrigante, pois enquanto na União Europeia este era o padrão mais popular na época, no Brasil era o menos utilizado em 2020, e não foi identificado em 2022.

Kampanos e Shahandashti (2021) examinaram os avisos de *cookies* com base na presença de elementos afirmativos, negativos, gerenciais e informativos, tal qual a pesquisa aqui apresentada, que usou os mesmos critérios de Kampanos e Shahandashti

(2021) para permitir comparações. Ao total, foram identificadas 16 combinações, provenientes de é 2^4, pois são 4 elementos com dois valores possíveis cada (existe ou não existe). Ao todo, Kampanos e Shahandashti (2021) avaliaram 17.737 *website*s do Reino Unido e da Grécia.

A pesquisa de Krisam *et. al.* (2021) também catalogou 13 categorias de avisos de *cookies* conforme o conteúdo apresentado, com mais ou menos botões, funcionalidades e informações nas mensagens dos *banners*. Foram 6 categorias principais e outras 7 subcategorias. A categoria mais frequente, com 27,8%, foi a que apresentava no primeiro nível um botão para aceitar os *cookies* e outro para configurar, sendo que apenas no segundo nível seria possível rejeitar os rastreadores. O segundo tipo de *banner* mais aplicado estava em 17,7% dos *sites*, nos quais havia apenas um botão para aceitar e uma mensagem indicando mais informações em outro local.

A Tabela 12 mostra o percentual de *website*s que empregam *cookie wall* nos avisos de *cookies*. Nesta pesquisa, o termo *cookie wall* refere-se aos avisos de *cookies* que bloqueiam a ação do usuário, à espera de uma ação sobre o componente exibido. Quando um indivíduo acessa um *site* e é apresentado a um aviso de *cookies* no estilo de *cookie wall*, ele é obrigado pelo sistema a decidir sobre a aceitação ou não dos termos apresentados no *banner*. Se a pessoa nada fizer, o acesso ao *site* é impedido. Os dados abaixo mostram que o emprego de *cookie wall* diminuiu percentualmente de 2020 para 2022, chegando a 2,03% em 2022; apesar disto, devido ao aumento da adoção de avisos de *cookies*, em 2020 só 2 *website*s usavam *cookie wall* e 13 *sites* adotaram tal prática em 2022. A figura abaixo demonstra o funcionamento do *cookie wall*: ao acessar, o *website*, é mostrado ao fundo, e na frente dele fica uma caixa com uma mensagem solicitando uma ação do usuário; no caso apresentado, as únicas opções disponíveis são clicar no botão "Entendi", customizar as preferências sobre *cookies*, ou obter mais informações nos termos de uso e políticas de privacidade. Não importa o que o visitante faça, ele é obrigado a fazer uma escolha, ou então precisa abandonar o *website*.

Usa *cookie wall*?	**% 2020**	**% 2022**	**Quantidade 2020**	**Quantidade 2022**
Não	97,56%	98,12%	80	627
Sim	2,44%	1,88%	2	12

Tabela 12: *Website*s que empregam *cookie wall*
Fonte: elaborada pelo autor.

As figuras que seguem apresentam *cookie walls* diferentes: ambos demandam a ação do usuário, porém um deles obriga a aceitar os termos para continuar usando o *site*, e o outro permite configurar as preferências que serão aceitas.

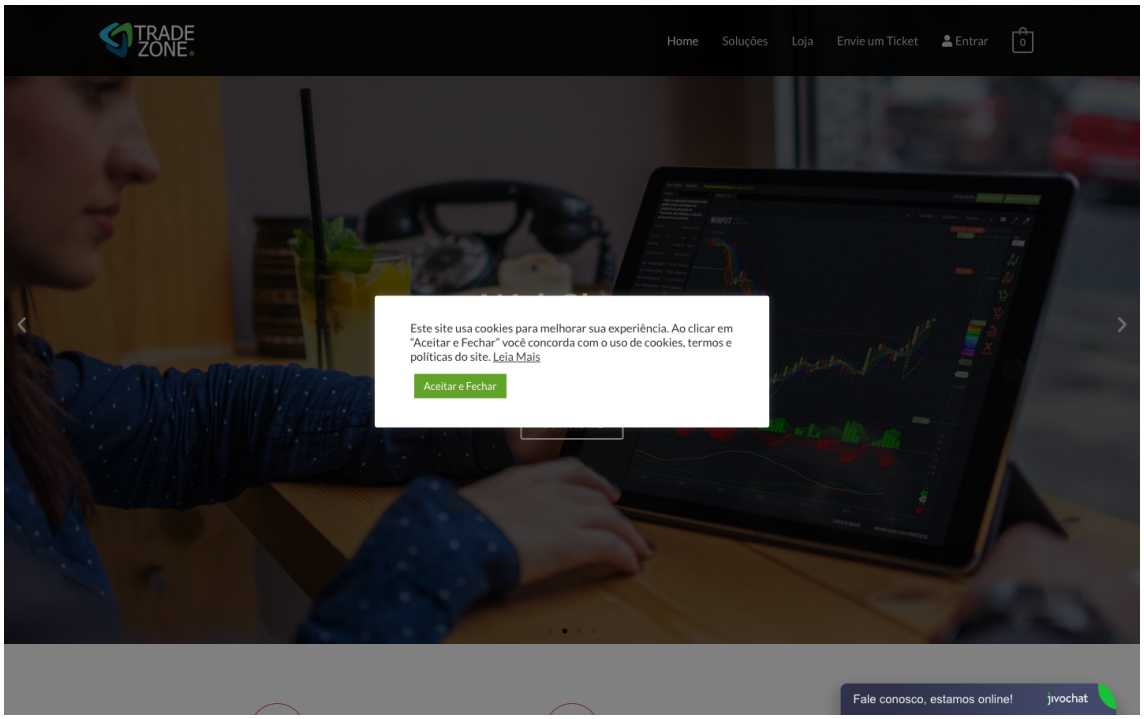


Figura 9: *Cookie Wall* que força a aceitação dos termos do aviso de *cookies*
Fonte: TRADEZONE, 2022.

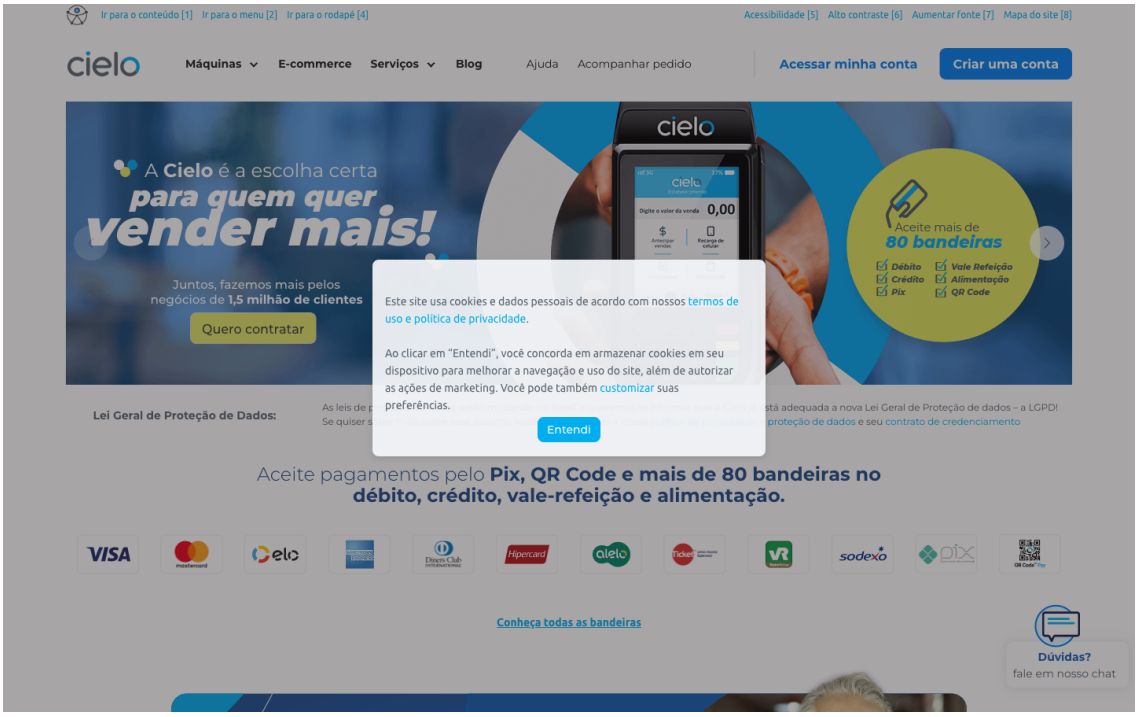


Figura 10: *Cookie Wall* que permite configurar preferências de *cookies* no segundo nível
Fonte: CIELO, 2022.

No estudo de Nouwens *et. al.*, (2020) foi descoberto que o emprego de aviso não bloqueante ou bloqueante (*cookie wall*) não influencia na tomada de decisão do usuário; além disso, também ficou evidenciado que o estilo de notificação (com ou sem barreira de acesso) não alterou a frequência de consentimento;

Nouwens *et. al.* (2020) encontraram também avisos bloqueantes em 234 *sites*, e não bloqueantes em 446 ocasiões; dos *banners* com consentimento explícito, 50,3% usavam bloqueios e 49,7% não. No caso brasileiro, de 2020 para 2022 houve queda de 2,44% para 1,88% no emprego de avisos bloqueantes.

Na criação de critérios de validade de consentimento segundo o regulamento europeu de proteção de dados, o trabalho desenvolvido por Bielova, Matte e Santos (2020) definiu o Requisito 20, *No "consent wall"*: ele se refere aos *cookie walls* (ou *tracking walls*) que obrigam o usuário a aceitar as condições de rastreamento sem outra opção, ou ainda os avisos bloqueantes, que obstruem a ação principal do usuário, obrigando-o a executar uma ação de aceitar ou rejeitar o consentimento.

Para Bielova, Matte e Santos (2020), é preferível usar o modo não bloqueante sempre que possível, e o serviço *online* deve estar disponível mesmo se for rejeitado o rastreamento. Este requisito requer que o aviso de *cookies* seja não bloqueante, não obstrua a ação principal do usuário, no sentido de não atrapalhar e assim não invalidar o consentimento, como nos casos em que os *banners* tomam toda a tela de um *smartphone*.

Consentimento tácito	% 2020	% 2022	Quantidade 2020	Quantidade 2022
Não	40,24%	53,75%	33	344
Sim	59,76%	46,25%	49	296

Tabela 13: *Websites* que presumem consentimento tácito
Fonte: elaborada pelo autor.

A Tabela 13 mostra os percentuais e quantidades de *sites* que presumem consentimento tácito do usuário quanto ao emprego de *cookies* conforme os avisos respectivos. Apesar de isto ter diminuído percentualmente entre 2020 e 2022, a realidade é que 46,25% dos *website*s pesquisados usam a presunção de consentimento tácito como justificativa para o emprego de rastreadores de *cookies*: dos 640 *website*s que têm o *banner*, 296 deles informam isto. A presunção de consentimento tácito acontece nestes

sites quando os respectivos avisos de *cookies* informam que, ao continuar navegando no *website*, o usuário aceita o uso de *cookies*.

Exemplo 1:

Exemplo 2:

Exemplo 3:

Tabela 14: Avisos de *cookies* com mensagens de consentimento tácito
Fonte: elaborada pelo autor.

Na pesquisa de Nouwens *et. al.* (2020), foi identificada a prática de consentimento implícito em avisos de *cookies* em 221 *sites* (32,5%), e explícito em 459. Para Kampanos e Shahandashti (2021), *banners* sem elemento afirmativo nem gerencial não permitem consentimento explícito: eram em torno de 2%. Apesar disso, os pesquisadores estimaram a ocorrência em torno de 15% de consentimento tácito, pois havia elementos afirmativos como “Fechar”, “Continuar” e outros. Na presente pesquisa, a determinação de consentimento tácito foi feita com base no texto da mensagem do aviso de *cookies*, nos

casos de textos que comunicavam que havia aceitação do uso de rastreadores apenas pelo uso do *site* ou fechamento do aviso respectivo.

Algumas das mensagens sobre presunção de consentimento tácito estão presentes na Tabela 14, retiradas de capturas de telas dos *website*s obtidas na coleta dos dados.

Essencialmente, os exemplos acima comunicam que o visitante aceita o uso de *cookies* com base nas seguintes hipóteses: "[a]o navegar em nosso serviço você aceita tal monitoramento"; "ao continuar navegando, você concorda com as condições de acordo com a nossa Política de Privacidade"; e "[v]ocê concorda com nossos *cookies* se continuar a usar o nosso *site*". Nos três exemplos apresentados, o controlador presume que o fato de navegar, continuar navegando ou continuar a usar o *site* é legítima manifestação do usuário em favor do consentimento.

De acordo com a tabela anterior, o percentual de avisos de *cookies* com mensagem que comunicava o consentimento tácito diminuiu de 59,76% para 46,25% na comparação entre antes e depois da LGPD. Porém, estes números, tanto em 2020 quanto em 2022, orbitam em torno da área de 50% nos dois casos.

Destaque Afirmativo	% 2020	% 2022	Quantidade 2020	Quantidade 2022
Não	6,10%	13,75%	5	88
Sim	93,90%	86,25%	77	552

Tabela 15: Avisos de *cookies* de *websites* com destaque para o elemento afirmativo
Fonte: elaborada pelo autor.

A Tabela 15 consolida as quantidades e os percentuais dos avisos de *cookies* que conferem destaque ao elemento afirmativo que os compõem. Como sabido, o elemento afirmativo é representado por botões com mensagens do tipo "Ok", "Sim", "Aceito", "Concordo", "Continuar", "Aceitar e Fechar", "Aceitar e Continuar" e outros similares. Os dados mostram que houve diminuição percentual do uso de destaque para os componentes afirmativos, de 93,90% para 86,25% de 2020 para 2022, porém devido ao aumento de adoção de *banners* que informam sobre o emprego dos marcadores de *cookies* após a vigência da LGPD, a quantidade absoluta de avisos que têm destaque também cresceu de 77 para 552 *website*s. Assim, dois anos após o início da vigência do referido diploma legal, somente 88 *website*s, ou 13,75%, deixam as opções afirmativas e negativas em pé de igualdade para a escolha do usuário. Conforme já explicado na metodologia, a avaliação do destaque entre as opções foi realizada por inspeção visual, manualmente,

site a *site*, e foi conferida outras duas vezes de forma integral. Assim, diferenças relevantes entre os elementos dos avisos de *cookies* foram contabilizadas como destaques.

Na Tabela 16, estão alguns exemplos de avisos com elementos afirmativos em destaque.

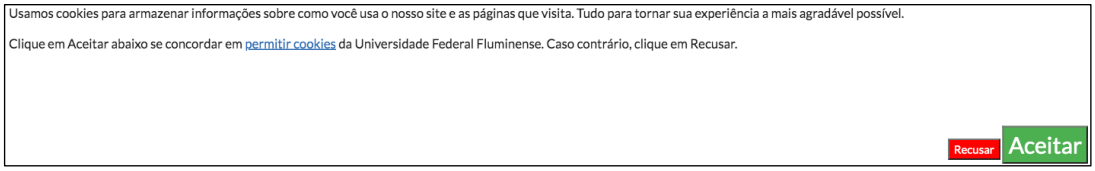
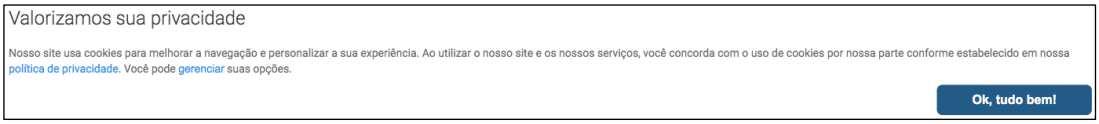
Exemplo 1: 
Exemplo 2: 
Exemplo 3: 

Tabela 16: Avisos de *cookies* com destaque para o elemento afirmativo
Fonte: elaborada pelo autor.

A análise dos elementos de segundo nível foi feita manualmente, por inspeção visual, como já apresentado na parte do trabalho sobre a metodologia. Nesta seção, serão apresentados os resultados desta análise que foi feita para o ano de 2022. A inspeção dos avisos de 2020 não foi realizada à época; apesar disto, os dados mais relevantes são os de 2022 neste ponto, por causa da relevância devido à maior quantidade de dados obtidos na segunda captura. Será com base nesse universo de 206 avisos que as próximas análises sobre o segundo nível serão feitas.

Há segundo nível	% 2022	Quantidade 2022
Não	67,81%	434
Sim	32,19%	206

Tabela 17: Avisos de *cookies* que têm segundo nível
Fonte: elaborada pelo autor.

Os dados da Tabela 17 demonstram que, dos *website*s que possuíam avisos de *cookies*, apenas 32,19% deles também disponibilizavam elemento gerencial que levava ao segundo nível. Então, 206 *sites* avaliados – quase um terço dos que tinham *banner* – forneceram ao usuário melhores ferramentas de controle dos seus dados pessoais com o advento da LGPD. Porém, será que disponibilizar uma camada gerencial é suficiente para garantir a proteção dos dados e os direitos dos visitantes? Isto será respondido posteriormente.

A Tabela 18 mostra que, em 2022, apenas 31,55% dos avisos com segundo nível possuíam um elemento afirmativo. No contexto do segundo nível, o elemento afirmativo corresponde a algum botão ou elemento que permita ao usuário aceitar todos os *cookies*, de todas as finalidades. No caso estudado, apenas 65 dos 206 *sites* com segundo nível tinham essa opção. O recurso que permite rapidamente aceitar todos os rastreadores melhora a usabilidade da interface para o usuário.

Há elemento afirmativo no segundo nível	% 2022	Quantidade 2022
Não	68,45%	141
Sim	31,55%	65

Tabela 18: Avisos de *cookies* com elemento afirmativo no segundo nível
Fonte: elaborada pelo autor.

Na pesquisa de Nouwens *et. al.* (2020), 9,7% dos usuários acessaram a interface de configurações de *cookies* (segundo nível); menos de 2% alteraram essas configurações para aceitar tudo; e 1,3% efetivamente fizeram configurações personalizadas sobre os *cookies*. Em 93,1% dos casos, somente o primeiro nível do aviso foi visitado. Isto demonstra a necessidade de privilegiar a privacidade logo no primeiro nível, asseverado pela baixa disponibilidade de elemento afirmativo no segundo nível (31,55% no presente trabalho) e baixo uso pelo usuário (2% no trabalho de Nouwens *et. al.*).

A Figura 11 mostra um exemplo de aviso de *cookies* com elemento afirmativo no segundo nível.

Figura 11: Aviso de *cookies* com elemento afirmativo no segundo nível
Fonte: elaborada pelo autor.

A análise do segundo nível também foi feita em busca de elemento negativo. Conforme a Tabela 19, exatamente 50%, ou 103 *website*s do total de 206 que tinham os *banners* em 2022, apresentavam opção para rejeitar todos os *cookies* não necessários no segundo nível.

A pesquisa de Nouwens *et. al.* (2020) identificou: que 50,1% dos *banners* não tinham botão para rejeitar todos os rastreadores não necessários; que somente 12,6% tinham um botão de rejeitar tudo com a mesma ou melhor acessibilidade (número de cliques igual ou menor) que o botão de aceitar tudo; e que 74,3% dos botões de rejeitar tudo estavam no segundo nível. O resultado da presente pesquisa quanto à existência de elemento negativo no segundo nível (50%) se aproxima daquele correspondente na pesquisa de Nouwens *et. al.* (50,1%).

Há elemento negativo no segundo nível	% 2022	Quantidade 2022
Não	50,00%	103
Sim	50,00%	103

Tabela 19: Avisos de *cookies* com elemento negativo no segundo nível
Fonte: elaborada pelo autor.

A Figura 12 mostra um exemplo de aviso de *cookies* com elemento negativo no segundo nível.

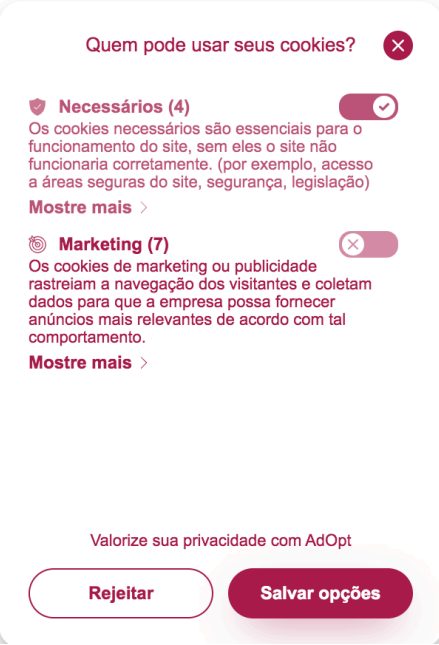


Figura 12: Aviso de *cookies* com elemento negativo no segundo nível
Fonte: elaborada pelo autor.

Os *cookies* apresentados no segundo nível também podem estar habilitados ou desabilitados por padrão, isto é, quando a interface gerencial é apresentada, as opções de *cookies* já estão ativadas. Assim, se o usuário não interagir e apenas fechar o segundo nível, aceitando as condições apresentadas no primeiro nível, então espera-se que todas as configurações pré-marcadas no nível gerencial serão utilizadas pelo sistema.

No estudo realizado conforme os dados apresentados na Tabela 20, a maior parte (75,73%) dos componentes gerenciais de segundo nível mantém os *cookies* não necessários desativados por padrão, enquanto que os *cookies* vêm ativados por padrão em 50 dos 206 *website*s analisados neste quesito.

A pesquisa de Khandelwal *et. al.* (2022) mostrou que os avisos de *cookies* não davam opções de escolha ao usuário em 18% e 31% (Grécia e Reino Unido respectivamente), mostrando apenas um botão para aceitar o rastreamento; e que os *cookies* não necessários estavam ativados por padrão em 16,7% e 22% respectivamente. O trabalho de Nouwens *et. al.* (2020) identificou que 56,2% dos avisos tinham *cookies* ativados por padrão no segundo nível, e que em 68,6% das situações a lista de finalidades de uso dos *cookies* foi ignorada pelos usuários. Neste quesito de *cookies* ativados por padrão no segundo nível, o percentual medido por Khandelwal *et. al.* (2022) para o Reino Unido (22%) se aproxima mais do valor medido na presente pesquisa (24,27%), e ambos se distanciam daquele observado por Nouwens *et. al* (2020), de 56,2%.

Cookies ativados por padrão no segundo nível	% 2022	Quantidade 2022
Não	75,73%	156
Sim	24,27%	50

Tabela 20: *Cookies* não necessários ativados por padrão no segundo nível
Fonte: elaborada pelo autor.

A Figura 13 mostra um exemplo de aviso de *cookies* com *cookies* não necessários desativados por no segundo nível.

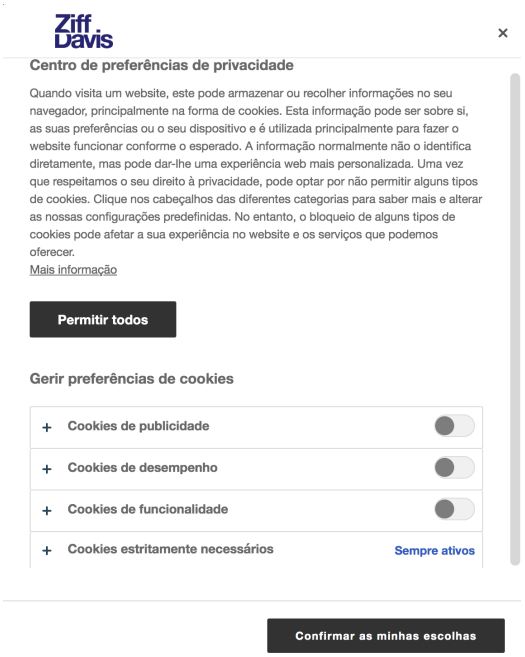


Figura 13: *Cookies* não necessários desativados por padrão no segundo nível
Fonte: elaborada pelo autor.

Analogamente à criação de perfis de *banners* de primeiro nível realizada anteriormente, foram identificados os perfis dos componentes de segundo nível usando 8 (oito) combinações possíveis, decorrentes de 2^3, pois são 3 elementos com 2 valores possíveis cada. Na Tabela 21, as combinações levaram em conta os seguintes itens, que significam, na ordem: "A": elemento afirmativo no segundo nível; "N": elemento negativo no segundo nível; "C": *cookies* desativados por padrão. O perfil ideal é A-N-C, que tem elementos afirmativos, negativos e nos quais os *cookies* estão inicialmente desativados; esta combinação está presente em 12,62% dos *website*s pesquisados que têm segundo nível. A combinação que prevalece na distribuição é x-N-C, com 32,04%, nas quais há apenas o elemento negativo, que pode ser um botão para rejeitar todos os *cookies* não necessários, e em que os *cookies* estão desativados por padrão. Por ordem de

frequência, a terceira combinação mais frequente, x-x-x, está presente em 18,93% não tem um botão para permitir todos os *cookies*, também não tem um botão para rejeitar todos os não necessários, e mantém todos os *cookies* ativos por padrão. Os outros itens são as combinações, com menores porcentagens.

Combinação do Segundo Nível	% 2022	Quantidade 2022
A-N-C	12,62%	26
A-N-x	2,43%	5
A-x-C	12,14%	25
A-x-x	4,37%	9
x-N-C	32,04%	66
x-N-x	2,91%	6
x-x-C	14,56%	30
x-x-x	18,93%	39

Tabela 21: Distribuição das combinações de elementos de segundo nível dos avisos de *cookies*
Fonte: elaborada pelo autor.

É possível encontrar as quantidades de *website*s cujos avisos de *cookies* atendem aos requisitos tidos como ideais tanto para o primeiro quanto para o segundo nível. Isto foi feito cruzando os dados das combinações dos dois perfis, o que resultou na Tabela 22. O ideal seria que, no primeiro nível, os *website*s tivessem a combinação A-N-G-I, tal como apresentado anteriormente, e que no segundo nível tivessem a combinação A-N-C, que também já foi mostrada. Após o cruzamento das informações conforme a tabela abaixo, foi possível identificar apenas 8 *website*s que atendem a todos os critérios supracitados.

		Combinações de primeiro nível				
Combinações de segundo nível		**A-x-G-x**	**A-x-G-I**	**A-N-G-x**	**A-N-G-I**	**Total Geral**
	x-x-x	6	18	6	9	39
	x-x-C	7	18	3	2	30
	x-N-x		4		2	6
	x-N-C		4		62	66
	A-x-x	4	3	1	1	9
	A-x-C	8	14	1	2	25
	A-N-x		4	1		5
	A-N-C	4	8	6	8	26
	Total Geral	**29**	**73**	**18**	**86**	**206**

Tabela 22: Cruzamento entre combinações de primeiro e segundo nível
Fonte: elaborada pelo autor.

Os oito *website*s referidos acima estão elencados na Tabela 23. Aplicando novo filtro para identificar aqueles que não apresentam informação sobe consentimento tácito, e que cumulativamente mantêm em pé de igualdade os elementos afirmativo e negativo, apenas quatro *sites* atendem aos critérios, e estão indicados com o valor "Sim" na coluna "Atende a todos os critérios?". Posteriormente, estes quatro endereços abaixo indicados com "Sim" na última coluna serão cruzados com os dados obtidos da captura de *cookies*, com o objetivo de verificar as características de implementação de tais *website*s.

Website	**Informação sobre consentimento tácito?**	**Tem destaque para elemento afirmativo?**	**Emprega *cookie wall*?**	**Usa língua estrangeira?**	**Atende a todos os critérios?**
cpfl.com.br	N	N	N	N	Sim
flamengo.com.br	N	S	N	N	Não
polishop.com.br	S	S	N	N	Não
pucminas.br	N	N	N	N	Sim
stone.com.br	N	S	N	N	Não
unimed.coop.br	N	S	N	N	Não
voegol.com.br	N	N	N	N	Sim
yelp.com.br	N	N	N	N	Sim

Tabela 23: *Websites* que atendem aos critérios de primeiro e segundo nível
Fonte: elaborada pelo autor.

Os resultados da pesquisa de Nouwens *et. al.* (2020) mostraram que apenas 11,8% dos *sites* atendiam aos requisitos conforme a GDPR: consentimento explícito, botões de aceitar e rejeitar todos os *cookies* com a mesma acessibilidade, e *cookies* não necessários ativados por padrão. Considerando o número total de *website*s encontrados na presente pesquisa, para o ano de 2022 apenas 0,69% dos *sites* atendem aos critérios de primeiro e segundo nível (8 *sites* de um total de 1.160), o que revela ser um número muito menor que o observado por Nouwens *et. al.* (2020), de 11,8%.

Emprego de língua estrangeira	**% 2020**	**% 2022**	**Quantidade 2020**	**Quantidade 2022**
Não	92,68%	96,25%	76	616
Sim	7,32%	3,75%	6	24

Tabela 24: Emprego de língua estrangeira em avisos de *cookies*
Fonte: elaborada pelo autor.

Quanto uso de língua estrangeira nos avisos de *cookies*, identificou-se que todos os casos positivos estavam em língua inglesa. A quantidade encontrada de *website*s com

avisos de *cookies* que empregam, de certa forma, alguma língua diferente do português foi baixa: 3,75% em 2022, correspondente a 24 casos conforme a Tabela 24.

Os resultados da avaliação dos avisos de *cookies* quanto ao emprego de *Consent Management Platforms* estão descritos na Tabela 25. Antes da vigência da LGPD, a medição feita identificou apenas 2 *website*s que utilizavam CMPs. Em 2022, a adoção de CMPs aumentou para 79 *sites*, que representa 12,34% de todos os 640 *website*s que exibiam avisos de *cookies*.

CMP	**Quantidade 2020**	**Quantidade 2022**
Adopt		15
Axeptio		1
***Cookie*bot**		1
Didomi		2
GDPR *Cookie* Compliance		2
Illow		1
OneTrust		36
ProvacyTools		14
Privally		3
Protegon		1
Quantcast	2	
Securiti		3
Total Geral	**2**	**79 (12,34%)**

Tabela 25: Avisos de *cookies* implementados por CMPs
Fonte: elaborada pelo autor.

Bielova, Matte e Santos (2020), no trabalho em que definiram 22 requisitos para considerar válido o consentimento à luz da GDPR, demonstraram de que forma eles podem ser usados para verificar a conformidade nesse tema, e investigaram a possibilidade de automatizar tal verificação. Ao final, concluíram que não é possível automatizar por completo este processo de verificação, pois há tarefas que dependem de inspeção manual, e em alguns casos esses estudos devem obter as respostas dos próprios usuários ou titulares de dados.

Também elaborado por Bielova, Matte e Santos (2020), o Requisito 13 – Escolha Balanceada – diz respeito a igualdade de condições nas escolhas, respeitando o direito a escolhas justas. As autoras relacionaram violações a esse requisito pela aplicação de *dark patterns*, tais como Falsa Hierarquia e Manipulação Estética.

Na Falsa Hierarquia, algumas opções ganham precedência ou vantagem sobre outras. Por exemplo, a) diferenças visuais de tamanhos, cores ou visibilidade entre os componentes, como botões e *links*: um botão maior que outro, uma opção com botão e outra em formato de *link* menos perceptível, ou um elemento afirmativo (de aceitação) com cor favorável e o botão de rejeição com cor que o prejudique; e b) opção de rejeitar consentimento presente apenas no segundo nível do aviso.

Na Manipulação Estética, a interface induz o usuário a aceitar o rastreamento. Neste item aplicam-se os mesmos exemplos de diferenças visuais de tamanhos, cores e visibilidade da Falsa Hierarquia, e também: a) tornar mais atraentes os elementos afirmativos; e b) opções pré-escolhidas.

O presente trabalho identificou a presença dos mesmos tipos de *dark patterns*, tais como as Figuras 14, 15 e 16.

Figura 14: *Dark pattern* Falsa Hierarquia entre elemento negativo e afirmativo
Fonte: elaborado pelo autor.

Figura 15: *Dark pattern* Falsa Hierarquia sem elemento negativo no primeiro nível
Fonte: elaborado pelo autor.

Figura 16: *Dark pattern* Manipulação Estética com opções pré-selecionadas
Fonte: elaborado pelo autor.

5.2 Discussões sobre os resultados da pesquisa empírica

Esta seção discute os resultados da pesquisa empírica com relação aos diversos aspectos já apresentados.

5.2.1 Quanto à presença de elementos afirmativos, negativos, gerenciais e informacionais

A presença de elementos negativos no primeiro nível dos avisos de *cookies* é importante. Segundo o trabalho de Nouwens *et. al.* (2020), avisos de *cookies* que não têm o elemento negativo no primeiro nível (botão para rejeitar o rastreamento) contribuem para o aumento do consentimento entre 22% e 23%. O presente estudo encontrou um percentual muito baixo de presença de elementos negativos no primeiro nível, na ordem de 21,25% de todos os *website*s pesquisados em 2022 (total de 1.160).

A arquitetura de escolhas apresentada pelos *banners* dos *website*s brasileiros privilegia o elemento afirmativo, presente em 100% dos casos após a vigência da LGPD conforme os dados apresentados anteriormente, indicando o emprego generalizado de *dark pattern* com o objetivo de capturar o consentimento dos usuários, em dissonância com os requisitos necessários da lei de proteção de dados para a formação de consentimento válido, por vício no aspecto da liberdade do consentimento que é correlacionada à liberdade de escolha.

Há também indícios de prática abusiva conforme a legislação consumerista, por desrespeito à mesma liberdade de escolha. O fato de não exibir certos elementos que

proporcionem igualdade entre controlador e titular de dados, ou entre prestador de serviços e consumidor, viola a liberdade de consentimento pois ocorre interferência no comportamento humano em favor da parte mais forte, num claro aproveitamento em relação à condição de vulnerabilidade do indivíduo.

5.2.2 Quanto aos perfis de avisos de *cookies* identificados

A presença de elementos afirmativos, negativos e gerenciais nos *banners* de rastreadores de *cookies* confere maior poder de escolha ao indivíduo, e a granularidade das decisões tende a aumentar indo ao segundo nível dos *banners*. O elemento informativo tem a função de aumentar o nível de transparência das práticas de tratamento de dados exercidas pelos controladores dos *website*s. Em suma, todos esses itens idealmente podem compor uma arquitetura de escolhas que favoreça o exercício do princípio da transparência, por conferir informação e propiciar que diferentes escolhas sejam feitas, em maior ou menor grau de detalhamento.

O Perfil 1 (x-x-x-I) está em uma das extremidades do espectro dos perfis identificados, e tem o foco em apenas informar a pessoa. Assim como os *sites* que não empregam *banners* de *cookies*, este perfil ignora a existência de direito à autodeterminação informativa. No instante da captura da fotografia do *website* no qual este perfil foi identificado, este tipo de aviso era quase imperceptível, pois pequeno demais e difícil de identificar. Tanto do ponto de vista da implantação de rastreadores quanto do ponto de vista da transparência, é o perfil de exibição de informação com menor efetividade. A adequação e a acessibilidade da informação provida estão completamente prejudicadas devido à falta de ostensividade do aviso. Não há possibilidade de o titular autorizar ou não o tratamento de dados.

Os Perfis 2 e 3 (A-x-x-x e A-x-x-I) também ignoram o direito de a pessoa decidir sobre o tratamento de seus dados pessoais. Ambos têm cunho mais informativo, no sentido de que até comunicam algo com mais ou menos detalhe, porém não permitem escolha, pois há apenas caminho único no fluxo da interação com o *site*: concordando ou não, haverá rastreamento. Aqui também não há possibilidade de escolha pelo indivíduo, seja ele consumidor tradicional ou *bystander*.

Em seguida, os Perfis 4 e 5 (A-x-G-x e A-x-G-I) permitem, de certa forma, a tomada de decisão; no perfil 5, por haver elemento informativo, a "decisão" é melhor informada do que no perfil 4. Todavia, a opção afirmativa é privilegiada pois está no

primeiro nível do *banner*, e para que a pessoa exerça o *opt-out* é necessário acessar o segundo nível e indicar suas preferências. Esta prática claramente cria dificuldades para rejeitar o monitoramento por *cookies*, e influencia o comportamento humano para que a decisão final seja aquela que o controlador do *website* deseja, aproveitando-se da vulnerabilidade neuropsicológica da pessoa. O perfil 5, ainda, em muitas situações identificadas durante a pesquisa despreza a importância do elemento gerencial, pois o mantém no meio de um texto, com grande desvantagem em relação ao elemento afirmativo, diferente de outros casos em que o acesso ao componente gerencial é exibido em um botão. Da mesma forma, o perfil 4 em muitos casos ressalta a opção positiva do botão "Ok, Entendi". Os perfis criam incentivos para uma determinada opção, e quase escondem ou minimizam o realce das demais opções, na tentativa de criar uma arquitetura de escolhas tendenciosa favorável ao *website*.

Quanto aos Perfis 6 e 7 (A-N-x-x e A-N-x-I), os elementos afirmativos e negativos estão presentes na arquitetura de escolhas de ambos, apesar de o perfil 7 qualificar melhor a decisão, com o fornecimento de informação sobre o que é apresentado. Nos dois casos identificados, porém, há diferença entre os elementos afirmativo e negativo, pretendendo direcionar o comportamento do indivíduo à opção afirmativa, para decidir favoravelmente ao rastreamento do usuário no ambiente *online*. Apesar disto, para identificação dos perfis não se considerou se há destaque ou não de algum elemento. As vulnerabilidades fática e informacional do consumidor ficam evidentes do ponto de vista do consumidor quando a ele é apresentado um aviso de *cookies*, instrumento pré-contratual, principalmente quando é necessária alguma decisão em cenários de pouca ou nenhuma informação.

Indo ao Perfil 8 (A-N-G-x) nota-se que o cardápio de opções para tomada de decisão melhora, à medida que os padrões de composição de elementos vão se localizando mais próximos à outra extremidade do espectro de perfis. Este padrão de aviso de *cookies* apresenta as opções afirmativa, negativa e gerencial, porém não entrega mais detalhes sobre a possível decisão, pois falta o elemento informativo. Neste ponto, a arquitetura de escolhas apresenta opções ao indivíduo que, tecnicamente vulnerável, não tem tanto conhecimento para saber o que fazer frente aos possíveis caminhos.

Por fim, o Perfil 9 (A-N-G-I) apresenta – logo no primeiro nível – os elementos afirmativo, negativo, gerencial e informacional. Trata-se de uma arquitetura de escolhas mais completa pois todos os elementos buscados foram encontrados. Na figura representativa do perfil exibida anteriormente, apesar de não ser a configuração ideal pelo

fato de o item afirmativo estar destacado dos demais, os elementos estão presentes de forma integral, o que é suficiente para caracterizar o padrão.

Este trabalho apresenta que os percentuais de elementos negativos, gerenciais e informacionais é bem menor que o percentual de elementos afirmativos. Tais percentuais são indicativos de aproveitamento, por parte dos controladores dos *website*s, das fragilidades dos titulares de dados e dos consumidores, quanto a diversas vulnerabilidades tais como: técnica, jurídica, fática, informacional, neuropsicológica, digital e de proteção de dados. A vulnerabilidade dos titulares de dados, dos consumidores em geral e equiparados, é largamente explorada mediante o uso de padrões obscuros – *dark patterns* – que direcionam as possibilidades de escolha no sentido da obtenção da autorização para tratamento de dados, nos casos em que o consentimento é necessário, e nas situações em que há alguma sorte de informação sobre rastreamento.

É baixa a procura por autorizar pontualmente ou negar de forma ampla o rastreio navegando em profundidade numa interface de *banner*, mostra-se ainda mais relevante a necessidade de apresentar as opções afirmativa e negativa no primeiro nível. Os estudos de Nouwens *et. al.* (2020) corroboram tal argumento, pois indicam que é baixo o número de indivíduos que busca o segundo nível de avisos de *cookies* para rejeitar o rastreamento. A fadiga do consentimento, fenômeno que tomou corpo frente às inúmeras solicitações de autorização para uso de *cookies*, pedidos de compartilhamento de localização e outros, junto com o baixo conhecimento das consequências jurídicas e de proteção de dados sobre fornecimento de dados pessoais, fundamentam ainda mais a necessidade de observação do dever de informação por parte dos controladores dos dados, fornecedores dos *website*s estudados.

5.2.3 Quanto aos *cookie walls*

Para ser considerado válido, o consentimento deve ser livre, nos termos da LGPD, art. 5º, XII (BRASIL, 2018) e do MCI, art. 7º, VII. Os componentes de *cookie walls* têm o mesmo comportamento: se apresentam como uma barreira entre o visitante e o *website*; entre eles, está um obstáculo que deve ser transposto com o fornecimento de uma resposta afirmativa ou negativa; caso a resposta não seja fornecida, o acesso ao recurso desejado poderá não ser concedido conforme explicado a seguir.

Há dois comportamentos possíveis para o *cookie wall*: o primeiro é aquele que fornece apenas caminho de aceitação obrigatória dos termos do aviso mostrado, com um

elemento afirmativo sendo a única opção. Esta situação é mostrada na primeira figura sobre *cookie walls*: a única saída para o visitante é clicar no botão "Aceitar e Fechar", ou então ir para outro *site*. O segundo comportamento possível é um pouco menos incisivo, mas nem por isso deixa de ser forçoso: o visitante até pode configurar as opções para rejeitar *cookies* não necessários no segundo nível, e então clicar no elemento afirmativo para confirmar as escolhas feitas, e assim o *banner* é fechado e o acesso ao *website* é liberado; ou então o visitante pode clicar diretamente no elemento negativo e rejeitar o uso de *cookies*, alterando ou não eventuais configurações se existirem, e ao final também consegue acessar o *site* desejado. No primeiro comportamento, o único caminho era aceitar as condições impostas; no segundo, poder-se-ia rejeitar as condições, mas mesmo assim era necessário, obrigatório, que o usuário fizesse alguma ação para isto.

Apesar de até ser possível rejeitar as condições apresentadas no *cookie wall* e então acessar o *site* no caso da segunda figura apresentada sobre *cookie walls*, na prática a situação não é tão simples assim: conforme mostrado na referida figura, para rejeitar os *cookies*, o usuário precisa ler as pequenas letras do aviso, identificar que aquela pequena palavra "customizar" na verdade significa uma opção que o levará a um segundo nível em que poderá rejeitar as condições apresentadas. E tudo isto deve ser feito com o botão "Entendi" destacado em azul pronto para ser clicado. Ou seja, o sistema de escolhas desenvolvido para o *website* atua para induzir o comportamento do usuário, com o objetivo de conseguir o que o controlador deseja: que o visitante clique em "Entendi", obtendo a autorização para tratamento dos dados pessoais capturados e trocados com terceiros por meio dos *cookies* e de outros recursos tecnológicos de rastreamento. As duas situações configuram claramente o emprego de *dark pattern*, como os denominados Dissimulação (*Sneaking*), Informações Ocultas, Manipulação Estética, pois configuram os elementos de forma a dificultar o acesso a certas informações, ou a mascarar a possibilidade de acessar funcionalidades que beneficiem o usuário, consumidor, titular de dados pessoais.

Com relação à prática de *cookie wall*, alguns padrões obscuros são usados, tais como: *Privacy Zuckering*, pois o indivíduo tem a impressão de poder exercer a autodeterminação informativa; *dark pattern* Obstrução, quando é imposta uma barreira para seguir ao próximo passo; e Ação Forçada, que obriga a pessoa a exercer certa ação que terá consequências decisórias frente àquela barreira imposta.

No caso de *website*s de pessoas jurídicas abrangidas pela Lei do Cadastro Positivo, argumenta-se neste trabalho que o simples fato de o usuário visitar o *website* de instituição

financeira, sem ter realizado qualquer tipo de cadastro, não autoriza o respectivo gestor a proceder conforme o art. 4º: "abrir cadastro em banco de dados" (BRASIL, 2011), "fazer anotações no cadastro", "compartilhar as informações cadastrais e de adimplemento", ou disponibilizar informações sobre *score* e histórico de crédito. Assim, seja em *website*s com *cookie walls* ou não, entende-se que é necessário para estes casos a autorização prévia dos visitantes dos *website*s para manipulação de cadastros com dados pessoais – capturados por meio dos identificadores de rastreamento *online*, ainda mais porque a simples visita ao *site* permite apenas o contato com termos pré-contratuais, e também porque não há como se diferenciar de antemão quem é consumidor efetivo – cliente – e quem é consumidor equiparado – um mero passante que visita o sítio eletrônico da instituição financeira.

A imposição de uma barreira para acesso ao *website* que macula a liberdade de escolha também pode ser vista como ilegal segundo a lei consumerista, pelo fato de que o CDC entende – como prática abusiva – negar a prestação de serviço, na medida em que ela poderia ser feita apenas com emprego de rastreadores de sessão (e os demais estritamente necessários).

Ainda quanto aos resultados encontrados na pesquisa em contraponto a outros, há diferenças significativas no emprego de bloqueios nos avisos de *cookies* brasileiros e do Reino Unido – conforme a pesquisa atual e aquela elaborada por Nouwens *et. al*. (2020): chama atenção o percentual de aproximadamente 1/3 (um terço) dos avisos britânicos serem bloqueantes e de no Brasil haver uma tendência a zero. As razões podem ser diversas, mas podem ser devidas ao maior *enforcement* naquela região, à adoção de lei de proteção de dados há mais tempo que no Brasil, e aos comandos existentes na diretiva *e-privacy*. Ademais, uma das conclusões a que Nouwens *et. al.* (2020) chegaram foi a de que, pela falta de obrigatoriedade de interação com os *banners*, tais avisos de *cookies* não bloqueantes possibilitam uma resposta neutra, vazia, diferente de sim ou não. Do ponto de vista brasileiro, como não há legislação que obrigue especificamente o emprego de avisos de *cookies*, esta também pode ser uma justificativa para o baixo índice de barreira nos *banners*. À parte do Requisito *No "consent walls"* trazido pelas autoras Bielova, Matte e Santos (2020), é possível também entender que é desnecessário impor uma ação ao usuário também por outro motivo: ele pode se sentir compelido a aceitar as condições, por pensar que se não o fizer não poderá acessar o serviço. Este também poderia ser entendido como os *dark patterns* de Obstrução e de Ação Forçada.

5.2.4 Quanto ao consentimento tácito

A legislação brasileira de proteção de dados define que o consentimento deve ser expresso: a LGPD, no art. 5º, XII adjetiva o consentimento como a "manifestação livre, informada e inequívoca" do titular de dados pessoais (BRASIL, 2018). Segundo o art. 7º, VII e IX do Marco Civil da *Internet*, para fornecimento de dados pessoais a terceiros, o consentimento deve ser "livre, expresso e informado" – à exceção de outras previsões legais – e ainda o consentimento deve ser expresso para "coleta, uso, armazenamento e tratamento de dados pessoais" (BRASIL, 2014). Ademais, entende-se que também aqui não cabe a autorização ao gestor de instituição financeira proceder ao tratamento de dados conforme o art. 4º da Lei do Cadastro Positivo por motivos já expostos. Assim, o arcabouço normativo respalda a exigência de consentimento expresso, invalidando ações tomadas com base em presunções, suposições, comunicações tácitas, mensagens de conteúdo implícito, não objetivas, obscuras, passíveis de largo espectro de interpretação.

A liberdade de escolha é também uma garantia do consumidor, nos termos do CDC, art. 6º, inc. II, assim como o direito a informações claras previsto no inc. III (BRASIL, 1990). Da mesma forma, o art. 4º, inc. I do Decreto 7.962/2013 que regulamenta as relações de consumo no comércio eletrônico alude ao respeito, pelo prestador de serviço, à liberdade de escolha do consumidor pela apresentação de informações necessárias, tanto quanto o art. 1º, inc. I, que também pugna por informações claras (BRASIL, 2013). O que for comunicado deve ser o mínimo necessário, e deve ser feito com clareza, sem cláusulas implícitas, sem suposições de autorizações tácitas, sem mensagens subentendidas em entrelinhas. Isto forma a base para a liberdade de escolha no exercício da autodeterminação informativa, tanto do ponto de vista do consumidor *standard* ou equiparado, do cidadão usuário de serviços públicos, quanto do titular de dados em geral. É de se lembrar que também a Lei 13.460/2017 define, no art. 6º, inc. II, a liberdade de escolha como direito básico do usuário de serviços públicos, da administração pública direta ou indireta de todas as esferas (BRASIL, 2017).

O CDC, no art. 51, ainda considera abusiva a cláusula contratual – e então a pré-contratual, no caso dos avisos de rastreadores – que for incompatível com a equidade (inc. IV), ou que estiver em desacordo com o sistema de proteção consumerista (inc. XV). Sendo assim, mensagens de cunho tácito quanto à concordância do usuário em relação ao emprego de *cookies* para tratamento de dados pessoais têm nulidade absoluta no sistema consumerista pátrio. A assimetria de poder entre o controlador do *website* e o seu visitante

não pode ser usada para captura de dados pessoais e compartilhamento com terceiros ou processamento próprio, senão para os exatos fins daqueles autorizados expressamente e de forma clara, objetiva. O mesmo se aplica para os usuários de serviços públicos, nos termos da Lei 13.460/2017, art. 1º, § 2º, inc. II, pois o CDC é aplicado de forma subsidiária à referida lei (BRASIL, 2017).

Os resultados observados na atual pesquisa empírica mostram que, com o advento da Lei Geral de Proteção de Dados, houve leve diminuição do emprego de mensagens que remetem ao consentimento tácito, quando o *website* está programado para instalar rastreadores no dispositivo do usuário simplesmente pelo fato de este acessar seu endereço eletrônico, continuar navegando desconsiderar ou fechar o aviso informativo. Apesar da diminuição, esta prática em desconformidade com a lei é uma das mais comuns encontradas nos sítios eletrônicos brasileiros estudados, presente em 59,76% dos casos em 2020, e em 46,25% após a vigência da LGPD.

Para além das mensagens sobre consentimento tácito, há ainda que se observar a existência de mensagens cujo conteúdo afirma que o usuário poderá ter dificuldades com o acesso ao *website* se não aceitar as condições apresentadas no aviso de rastreadores. Neste caso, estão presentes os *dark patterns ConfirmShaming* e Brincar com a Emoção, com teor negativo em relação ao comportamento do usuário que negar a autorização de tratamento de dados.

5.2.5 Destaque para o elemento afirmativo

Segundo conceitua a Lei Geral de Proteção de Dados, em seu art. 5º, inc. XII, o consentimento deve ser manifestado de forma livre, informada e inequívoca. Para o Marco Civil da *Internet*, art. 7º, VII, o consentimento também deve ser livre e informado. O quão livre é uma escolha quando há favorecimento de uma ou outra opção, se é que possa haver uma segunda opção? E quão inequívoca é a decisão tomada pelo usuário quanto à autorização de seu rastreamento numa situação de desigualdade entre os caminhos a seguir? Ser inequívoco é ser livre de erro, é ser livre de engano, é ser livre de ambiguidade. E a escolha feita quando só há um ou dois caminhos desiguais, e ainda sem possibilidade de obter maiores informações, também não é uma escolha informada, e que favorece ainda mais a opção ideal formulada pelo criador daquele sistema de escolhas. Uma decisão tomada num ambiente que favorece certa opção certamente não é livre, às vezes nem suficientemente informada, e muito menos isenta de equívocos.

Da mesma forma que os casos nos quais as opções de escolha ficam ocultas ou cujo acesso é desfavorecido, também quando se prestigia uma opção de escolha em relação às demais, em desfavor do usuário, consumidor ou titular de dados, possivelmente se está diante do emprego de *dark patterns*. Como já referido, os padrões de Manipulação Estética, de Falsa Hierarquia, de Brincar com a Emoção, e de Interferência de Interface. É interessante salientar que a LGPD, art. 9º, § 1º define que o consentimento é nulo sempre que for obtido por meios abusivos ou enganosos, ignorando o princípio da transparência.

Os dados colacionados na presente pesquisa exprimem que, em junho de 2020, 93,90% dos *website*s brasileiros estudados conferiam destaque ao elemento afirmativo. Os resultados também mostram que, em setembro de 2022, 86,25% dos mesmos *website*s tinham o elemento afirmativo em destaque. Apesar de ter diminuído, a incidência de tal prática ainda é alta nos *sites* brasileiros estudados, e assim apenas uma minoria deles confere igualdade de condições no sistema de escolhas.

Caso os elementos dos avisos de *cookies* fossem dispostos de forma a favorecer as escolhas feitas pelos usuários, então estar-se-ia na presença de *nudges*, e não de *dark patterns*. Um exemplo de *nudge* que poderia ser usado nesta situação é a aplicação de um assistente virtual que auxiliasse os usuários nas escolhas, diminuindo assim a assimetria e mitigando as vulnerabilidades existentes.

Para o caso de desconformidade apresentado, a solução ideal é a apresentação, em igualdade de condições, das opções de escolha, com todos os elementos na mesma formatação, tamanho e disposição, atendendo ainda aos critérios definidos no Decreto 7.962/2013 (BRASIL, 2013) quanto a legibilidade e em linha com as orientações do guia orientativo sobre *cookies* publicado pela ANPD (BRASIL, 2022d).

5.2.6 Emprego de língua estrangeira

Em que pese a baixa incidência de idioma diferente da língua pátria nos resultados encontrados por esta pesquisa acadêmica, é importante salientar que o uso de vernáculo estrangeiro dificulta sobremaneira o acesso à informação. O princípio da transparência que compõe a LGPD remete a "informações claras, precisas e facilmente acessíveis", (BRASIL, 2018); na mesma linha, o art. 7º, inc. VIII e XII do MCI também asseguram respectivamente que obter "informações claras e completas" e desfrutar de acessibilidade são direitos dos usuários (BRASIL, 2014); a lei 13.460/2017, art. 5º, inc. XIV, também

define que é direito básico dos usuários de serviços públicos o emprego de linguagem simples e sem estrangeirismos (BRASIL, 2017).

Os dados obtidos nesta pesquisa mostram que o uso de língua estrangeira diminuiu proporcionalmente de 7,32% para 3,75% de 2020 a 2022, apesar de o número absoluto de casos ter crescido de 6 para 24, conforme a tabela respectiva. Isto significa que houve maior cuidado no dever de informar por parte dos controladores dos *website*s, e que a tendência para este quesito é de diminuição ao longo do tempo.

5.2.7 Avisos de *cookies* com segundo nível: elementos afirmativos e negativos

O visitante do *website* pode ser entendido como titular de dados pessoais sob o ponto de vista da legislação de proteção de dados, como consumidor – equiparado ou não – à luz do direito consumerista, ou pode ainda ser visto como usuário, de acordo a lei de proteção e defesa dos direitos do usuário dos serviços públicos. Em todos os casos, o indivíduo tem direito à proteção de seus dados pessoais, do qual também faz parte o direito a exercer a sua autodeterminação informativa. No caso dos avisos de *cookies* que não têm elemento negativo no segundo nível, o direito de oposição ao tratamento de dados pessoais pode ficar prejudicado se não houver outro meio razoável para rejeitar o tratamento. Da mesma forma que o sistema oferece condições simples de aceitar o rastreamento de suas atividades para todas as finalidades, a rejeição de tratamento para finalidades não necessárias também deve ser facilitada.

O art. 8º, § 3º da LGPD veda o tratamento de dados com vício de consentimento. A falta de igualdade de condições para uma escolha ou outra, no contexto eletrônico abordado, pode caracterizar nulidade na obtenção da autorização do titular de dados pessoais.

O art. 18, *caput* e inc. VIII da LGPD afirma que é direito do titular obter "informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa" (BRASIL, 2018). Ademais, o art. 8º, § 3º do mesmo diploma estabelece que "[é] vedado o tratamento de dados pessoais mediante vício de consentimento" (BRASIL, 2018). Assim, a impossibilidade de rejeitar todos os dispositivos rastreadores de *cookies* – devido a falta de aparato tecnológico para tal – eiva de nulidade o tratamento de dados, já que foi construído todo o arcabouço para implantar componentes de monitoramento.

Também é evidente a vulnerabilidade do consumidor, que não tem outra opção senão aquiescer com o que lhe for apresentado, por conta da construção tecnológica que concretiza a assimetria de poder entre o vulnerável e o fornecedor do *website*, quando não há opção para rejeitar o monitoramento eletrônico exercido pelo controlador principal e por terceiros controladores com os quais os dados são eventualmente compartilhados.

5.2.8 *Cookies* ativados por padrão

O consentimento livre fica prejudicado quando há alguma forma de sugestão que favoreça a opção afirmativa, ou que aumente a quantidade de dados compartilhados pela pessoa com o controlador.

A figura apresentada anteriormente no tópico sobre *cookies* ativados por padrão continha uma interface que não trazia as configurações de interesse do fornecedor do *website*, e assim não sugeria algo que o usuário não quisesse. Este foi um bom exemplo de aplicação do princípio *Privacy by Default*, pois os controles estão, por padrão, protegendo a privacidade da pessoa. Quando apresentada a *Diretiva E-Privacy*, já foi mencionado sobre o caso Planet49, em que houve uma decisão no contexto europeu condenando o controlador de dados por entregar avisos de *cookies* com itens pré-selecionados, em desfavor da privacidade pessoal (UNIÃO EUROPEIA, 2019). Também em recente relatório publicado pela Federal Trade Comission (FTC) norteamericana, o documento afirma que a pré-seleção de opções num sistema de escolha pode ser entendido como *dark pattern* (FTC, 2022, p. 15).

Os dados compilados nesta pesquisa demonstram que, dos *sites* que tinham avisos de *cookies* com segundo nível (gerencial), 24,27% deles tinham os *cookies* ativados por padrão, ou seja, aproximadamente ¼ dos avisos de rastreadores não aplicavam a diretriz *privacy by default*, e empregavam o *dark pattern* Pré-Seleção, que é um tipo de padrão de Interferência de Interface, com o qual ficam previamente ativadas as opções que favorecem o arquiteto de escolhas, no caso o controlador dos dados, que é o fornecedor do *website*.

5.2.9 Atendimento dos critérios de primeiro e segundo nível

De todos os 640 *website*s que possuíam avisos de *cookies*, e que representavam 55,17% do total de 1.160 endereços que estavam acessíveis em 2022, apenas 21,25% –

de todos os 640 – possuíam no mínimo o padrão de perfil A-N-?-?, em que estavam presentes os elementos afirmativos e negativos. Ou seja, um baixo número de *sites* mostrava componentes de interface que permitiam a escolha pelo usuário.

Dentre esses 640 *sites*, foram encontrados 206 deles nos quais havia segundo nível nos avisos de *cookies*. E apenas 26 desses 206, ou 12,62% dos 206, atenderam a um conjunto mínimo de critérios no segundo nível, possuindo elemento afirmativo e também negativo, e ainda tendo os *cookies* não necessários desativados (isto é, com emprego de *privacy by default*). Ou seja, um número ainda menor de avisos de *cookies* com segundo nível atendia em certo grau tais requisitos.

No cruzamento realizado entre os perfis de primeiro e de segundo nível, foram encontrados apenas 8 (oito) *website*s que atendiam plenamente às condições aqui avaliadas, de um total de 640 *sites* que tinham avisos de *cookies*, e de um total global de 1.160 *website*s visitados durante a captura de dados de 2022. Ou seja, apenas 1,25% dos 640 avisos de *cookies* atenderam aos critérios, correspondendo a somente 0,69% de todo o *corpus* da pesquisa cujos endereços estavam acessíveis em 2022.

Ainda conforme o cruzamento feito, se forem usados outros critérios conforme descritos na respectiva tabela apresentada anteriormente, o número de *website*s que atendem a tais condições diminui ainda mais. Os outros critérios versam sobre consentimento tácito, destaque para elemento afirmativo, emprego de *cookie wall*, e uso de língua estrangeira. Conforme a mencionada tabela, apenas 4 dos 8 *website*s daquela lista efetivamente atende a todos os critérios. Assim, foi identificado que somente 0,63% dos avisos de *cookies* atendiam aos critérios todos, e que apenas 0,35% de todos os *website*s avaliados em 2022 correspondiam aos quesitos firmados na referida análise.

Assim, pode-se afirmar que o nível de atendimento aos critérios definidos nesta seção é extremamente baixo. Uma das razões pode ser a falta de norma legal no Brasil que imponha critérios mínimos para o emprego de rastreadores nos *website*s. De qualquer modo, apesar de não haver norma cogente específica para rastreadores de *website*s em relação a privacidade e proteção de dados, em que pese a existência de um guia orientativo sobre o tema publicado pela ANPD, é possível usar de critérios gerais, tanto da Lei Geral de Proteção de Dados, quanto do Marco Civil da *Internet*, e ainda do Código de Defesa do Consumidor, e também do próprio guia orientativo supramencionado, para avaliar o nível de conformidade desses avisos de *cookies*. E isto foi feito neste trabalho, pela concepção dos itens de verificação da forma como descritos nos perfis e demais pontos

que foram anteriormente apresentados e que permitiram comparação com outras pesquisas.

5.2.10 Emprego de CMPs

O uso de plataformas de gestão de consentimento cresceu em números percentuais e absolutos entre os anos de comparação da pesquisa, chegando a 12,34% dos *website*s que apresentavam *banners* de rastreamento (640 no total). No Brasil, não há obrigatoriedade legal de adoção de tais ferramentas, tampouco há padronização em relação a elas. Tais soluções tecnológicas – que são da classe das PETs, ou *Privacy Enhancing Technologies* – não são garantia de conformidade com os ditames principiológicos das normas que regem a legalidade do tratamento de dados pessoais. Apesar disso, percebe-se o avanço dessas tecnologias, oriundas de um outro contexto normativo, o contexto europeu, que possui norma específica sobre o assunto e que exerce o *enforcement* de maneira muito ativa em relação a este assunto.

No Brasil, a questão sobre quem é o controlador dos dados gerenciados pelas plataformas de gestão de consentimento não foi – ainda – discutida diretamente em sede administrativa ou judicial. É interessante notar o crescimento da adoção deste tipo de solução tecnológica padronizada, derivada de autorregulação, e que já rendeu discussões no contexto da GDPR, com decisões que entenderam para aquele contexto jurídico: que tanto o órgão que organizou a autorregulação é controlador de dados; e que quanto os identificadores únicos utilizados pelos CMPs são considerados dados pessoais pois permitem a identificação, a individualização da pessoa que acessa o *website* que simplesmente exibe o *banner*.

5.2.11 Emprego de *dark patterns*

O emprego de *dark patterns* é generalizado nos *website*s brasileiros pesquisados. Dentre os padrões identificados, alguns são como seguem. ***Roach Motel***: na quase totalidade dos *website*s, não é possível retirar o consentimento em momento posterior à respectiva autorização. **Ilusão de Controle**, ***Privacy Zuckering***: ocorre sempre que os *website*s capturam ainda mais dados pessoais do usuário, enriquecendo os respectivos perfis armazenados por esses *sites*; o indivíduo até pensa que tem o controle sobre seus dados, o que é uma falácia. ***Misdirection***: acontece quando o aviso de *cookies* não fica

tão visível quanto outros elementos do *site* visitado, e assim o usuário é distraído para outros componentes. ***Bait and Switch***: se dá quando os rastreadores são instalados mesmo que o usuário não aponha sua autorização para tratamento de dados. ***Confirmshaming***: é empregado por meio de mensagens que constrangem o usuário a fazer o que o controlador do *site* deseja. ***Nagging***: quando há excesso de outros elementos que pedem a atenção do usuário e o desfocam de cuidar do aviso sobre rastreamento. **Obstrução**: é usado quando o processo de gestão do consentimento é complicado, nas situações em que deveria ser simples. **Dissimulação**: acontece quando as informações prestadas pelo *website* são mascaradas por algum outro componente ou característica da interface, bem como por mensagens de incentivo ao usuário fazer aquilo que é benéfico ao controlador do *website*. **Interferência de Interface**: é um padrão amplo que altera a comunicação entre o *website* e o usuário, também em favor do controlador do *site*. **Informações Ocultas**: acontece quando há dificuldade de acesso a certos componentes, como elementos informacionais e gerenciais, que ficam entremeados em mensagens e *links*, e cuja legibilidade muitas vezes é prejudicada. **Pré-Seleção**: ocorre quando há, por exemplo, *cookies* ativados por padrão no segundo nível dos *banners*. **Manipulação Estética**: se dá quando o aviso de rastreadores apresenta diferenças de tamanho, cor ou disposição dos elementos afirmativos, negativos, gerenciais e informacionais, como nos casos em que o elemento afirmativo está mais visível e os demais elementos ficam bem menos perceptíveis. **Brincar com a Emoção**: este padrão tem vez quando são empregadas mensagens de sentido negativo quanto à escolha que for feita pelo indivíduo, na tentativa de influenciá-lo. **Falsa Hierarquia**: é quando um elemento da interface é ressaltado em relação aos demais, ou outros são apresentados apenas no segundo nível do aviso de *cookies*. **Ação Forçada**: tem lugar sempre que a interface obrigar o usuário a tomar uma decisão sobre autorizar instalação de *cookies*, como nas situações de *cookie wall*.

Como apresentado, os diversos *dark patterns* – ou *deceptive patterns*, padrões obscuros ou padrões enganosos – são largamente usados nos *website*s brasileiros. O *dark pattern* Manipulação Estética estava presente em 86,25% dos 640 *website*s estudados em 2022 que possuíam avisos de *cookies* e que conferiam destaque ao elemento afirmativo, em detrimento dos elementos negativos, gerenciais e informacionais. O *dark pattern* Pré-Seleção foi encontrado em 24,27% dos 206 *website*s cujo aviso de *cookies* possuía segundo nível, pois naqueles casos os *cookies* estavam ativados por padrão no referido segundo nível. O *dark pattern* Dissimulação, por sua vez, foi identificado em 46,25% dos

640 *website*s de 2022 que possuíam mensagens informativas nos avisos de *cookies* indicando consentimento tácito.

Assim, com base nos argumentos já apresentados, os *website*s brasileiros empregam sobremaneira os *dark patterns* com o fito de legitimar o consentimento do usuário, dando uma roupagem de legalidade à respectiva prática, porém aproveitando-se das diversas vulnerabilidades já mencionadas e que são inerentes às condições dos titulares de dados e consumidores de toda ordem. Ademais, e também conforme já discutido, o emprego desses padrões vai de encontro aos preceitos da legislação brasileira de proteção de dados, do Marco Civil da *Internet* e do arcabouço legal de proteção do consumidor. Tal prática: invalida o consentimento do titular de dados pessoais – que deve ser livre, informado, inequívoco e expresso; fere a liberdade de escolha do consumidor; descumpre o dever anexo de informar o consumidor de forma clara, expressa, diminuindo o grau de transparência.

5.3 Considerações gerais sobre o objetivo da pesquisa

No intuito de responder à pergunta de pesquisa, pode-se afirmar que com o advento da Lei Geral de Proteção de Dados, e sob a ótica do princípio da transparência aplicada aos *website*s brasileiros, houve aumento significativo do emprego de componentes que informam sobre a prática de rastreamento dos usuários na *Internet* durante os anos de 2020 e 2022, antes e depois da vigência da referida lei, considerando os 1.188 e 1.160 *website*s visitados durante a primeira e a segunda captura de dados dos anos respectivos. Nos *website*s visitados, o emprego de avisos de *cookies* cresceu de 6,90% para 55,17% entre 2020 e 2022. Deste modo, observando superficialmente, houve aumento considerável do nível transparência dos *website*s brasileiros quanto às práticas de rastreamento por meio do emprego de *cookies* e outras tecnologias.

Das 5 categorias de *website*s mais frequentes no *corpus* da pesquisa – Notícias, Educação, Governo, Comércio Eletrônico e Negócios – os *website*s de Governo foram os que tiveram menor preocupação em implementar os avisos de *cookies* após a vigência da LGPD: o percentual de *website*s governamentais em que foram identificados os avisos de *cookies* foi de 1,31% para 39,84% nos anos de 2020 e 2022. A categoria de *website*s com maior aderência à transparência sobre rastreamento de usuários e consumidores foi a dos *sites* de Comércio Eletrônico, que subiu de 4,69% em 2020, antes da vigência da LGPD, para 62,33% em 2022, dois anos depois que esta lei entrou em vigor. E no geral, todas as

demais categorias de *website*s apresentaram aumentos significativos no emprego de avisos de *cookies*.

Este número geral de 55,17% de *website*s com avisos de *cookies* identificado para o estrato de 2022 capturado nesta pesquisa acadêmica guarda aproximação com algumas outras pesquisas internacionais, que trouxeram percentuais tais como: 48% (Reino Unido) e 44% (Grécia) no trabalho de Kampanos e Shahandashti (2021); 62,1% (União Europeia) na pesquisa de Degeling *et. al.* (2018); 35,36% (União Europeia e outros) no trabalho de Klein *et. al.* (2022); 53% (Reino Unido) e 25% (Estados Unidos) conforme a pesquisa de Khandelwal *et. al.* (2022); e 65,6% (Alemanha) no estudo feito por Krisam *et. al.* (2021).

Aprofundando a visão sobre os dados capturados, os resultados da pesquisa para o ano de 2022, após a vigência da LGPD, indicaram a prevalência de elementos afirmativos, que comunicam escolha positiva quanto à aceitação de uso de *cookies*, em todos os avisos de *cookies* que foram encontrados. Os elementos informacionais, que fornecem mais informações sobre a prática de rastreamento de usuários pelos *website*s, estavam presentes em 86,41% dos casos. Elementos gerenciais, que permitem a configuração de detalhes da autorização de tratamento de dados pessoais, foram identificados em apenas 32,19% dos *banners*. E os elementos negativos, que servem para que o indivíduo não permita o emprego de *cookies* não necessários, foram encontrados em somente 21,25% dos *website*s que tinham os avisos de *cookies* (do total de 640 *website*s que mostravam tais *banners*, num universo de 1.160 endereços visitados).

O percentual do elemento afirmativo encontrado no Brasil (100%) se aproxima dos valores da Grécia (95%) e Reino Unido (88%) obtidos na pesquisa de Kampanos e Shahandashti (2021). No mesmo estudo, os percentuais de elementos negativos são os menores dentre os demais elementos: 20% na Grécia e 6% no Reino Unido; os resultados sobre elementos negativos nesta pesquisa brasileira também foram os menores dentre os 4 elementos procurados: 21,25% em 2022, após a vigência da LGPD. Os elementos informacionais estão muito mais presentes no Brasil (86,41%) do que na Grécia e Reino Unido (40% e 20% respectivamente). E a quantidade de elementos gerenciais no Brasil, de forma contrária, é menor (32,19%) do que na Grécia e no Reino Unido (50% e 69% respectivamente).

Então, é possível afirmar que os percentuais de elementos afirmativos e gerenciais são predominantes no cenário brasileiro, e que os resultados da pesquisa encontram correspondência quanto aos elementos afirmativos e negativos, mas se distanciam dos informacionais e gerenciais quando comparados aos resultados de pesquisa estrangeira.

Tal afirmação sobre componentes afirmativos e informacionais também é corroborada pela identificação do perfil de aviso de *cookies* mais recorrente no corpo de pesquisa: em 2020, o percentual do perfil A-x-x-I era de 63,41%; e em 2022, este mesmo perfil A-x-x-I foi identificado em 58,12% de todos os *website*s que possuíam *banner* de rastreamento (640 *sites* com *banners* no total em 2022). Este perfil indica que o *banner* tem elemento afirmativo e informacional, mas não apresenta componente negativo nem gerencial. O perfil A-N-G-I, por sua vez, apresenta todos os elementos buscados como critério de pesquisa, e sua presença subiu de 0,00% em 2020 para 13,44% em 2022, após a vigência da LGPD.

Comparando com os critérios de pesquisa do trabalho de Degeling *et. al.* (2018) – *No Option*, ou avisos de *cookies* **sem** elementos afirmativos e negativos; *Confirmation Only*, *ou* avisos **com** elemento afirmativo **e sem** elemento negativo; e *Binary*, ou avisos **com** elementos afirmativos e negativos – tem-se que os resultados da presente pesquisa se aproximam mais dos valores encontrados por Kampanos e Shahandashti (2021). Por exemplo, para estes pesquisadores o padrão *Confirmation Only* está presente em 75% e 82% dos casos (Grécia e Reino Unido respectivamente), e em 78,75% na segunda medição realizada após a vigência da LGPD, no caso da pesquisa brasileira. Ainda colacionando as duas pesquisas, são prevalentes os avisos de *cookies* que apresentam duas opções (2 dos 4 elementos), com 57% e 58% para Grécia e Reino Unido, e 64,21% para o Brasil.

O nível de transparência dos *websites* brasileiros quanto à presença de elementos afirmativos, negativos, informacionais e gerenciais nos avisos de *cookies* aumentou de 2020 para 2022, e o perfil de *banner* prevalente nos dois anos é aquele que apresenta uma mensagem simples, um elemento informativo, como um *link* para mais informações sobre o uso de *cookies*, e um botão afirmativo, como “Ok”, “Entendi”, “Aceito” e outros.

Quanto ao emprego de *cookie wall* medido nesta pesquisa, tal prática diminuiu de 2,44% em 2020 para 1,88% em 2022. A quantidade de ocorrências desta prática é muito baixa, e com a vigência da Lei Geral de Proteção de Dados foi identificada uma tendência de desuso de *cookie walls* nos *sites* brasileiros.

Em relação à prática de consentimento tácito nos avisos de *cookies*, identificou-se a diminuição de 59,76% para 46,25% da incidência deste comportamento durante os anos de 2020 e 2022. Assim, apesar da diminuição após a vigência da LGPD, a prevalência de tal prática ainda é alta.

O destaque do elemento afirmativo nos avisos de *cookies* em detrimento dos demais elementos também sofreu leve queda após a vigência da LGPD, indo de 93,90% em 2020 para 86,25% em 2022. Da mesma forma que o consentimento tácito, também o destaque de elemento afirmativo é prática predominante nos *banners* de *cookies* dos *website*s brasileiros estudados.

Nas situações em que havia segundo nível para os dados de 2022, o elemento afirmativo estava presente no referido segundo nível em 31,55% dos casos, e o elemento negativo em 50% dos casos (correspondendo a 103 *banners*). Assim, como foi apresentado que apenas 21,25% dos *banners* tinham elemento negativo no primeiro nível (de um total de 640), correspondentes a 136 casos, então 239 avisos de *cookies* (103 + 136) possuíam elemento negativo no primeiro ou segundo nível, correspondendo a 37,34% de 640 no total. Assim, a presença de elementos negativos nos *banners* de *cookies* era baixa no ano de 2022.

Os *cookies* estavam ativados por padrão no segundo nível em 24,27% dos casos em 2022, indicando que o uso de *dark patterns* era feito por uma parte dos *website*s brasileiros naquele momento da medição. A língua estrangeira é pouco empregada nos avisos de *cookies*, e diminuiu de 7,32% em 2020 para 3,75% em 2022. E os CMPs foram usados como solução tecnológica para os avisos de *cookies* em 12,34% dos casos em 2022.

Alguns dos *dark patterns* mais usados referem-se a Manipulação Estética, Falsa Hierarquia e Interferência de Interface, com diferenças entre os elementos afirmativos e negativos dos avisos de *cookies*. O padrão *Roach Motel* também é empregado, pois muitos *website*s não permitem retirar o consentimento anteriormente fornecido. A Pré-Seleção é outro padrão obscuro muito usado quando os *cookies* não necessários estão ativados por padrão. E o padrão Informações Ocultas também é utilizado, pois em diversos casos os elementos informacionais e gerenciais foram identificados no meio das mensagens dos avisos de *cookies* dos *website*s analisados.

Assim, pode-se afirmar que o grau de transparência dos *website*s brasileiros aumentou com o advento da vigência da LGPD, pois houve significativo crescimento do número de avisos de *cookies*, informando sobre o rastreamento dos usuários. Apesar disso, junto com este aumento, o índice de práticas que manipulam o comportamento do

usuário permaneceu alto, denotando um grande interesse dos controladores em obter os dados pessoais dos visitantes dos *website*s, em linha com outros estudos comparados.

6 CONSIDERAÇÕES FINAIS

Este trabalho teve o intuito de investigar quais foram os efeitos da vigência da Lei Geral de Proteção de Dados nos avisos de *cookies* dos *websites* brasileiros em relação aos aspectos de transparência. É importante que o dever de informar seja observado pelos controladores dos *sites* para que os usuários tenham ciência sobre as práticas de rastreamento *online*, que são exercidas sobre eles também com a instalação de *cookies* em seus dispositivos.

Foram apresentados alguns conceitos de economia comportamental, e tais conceitos foram então relacionados à autodeterminação informativa e à liberdade de escolha. Também foram apresentados os conceitos de *nudges* e de *dark patterns*, sendo que estes também foram detalhados em alguns de seus tipos mais conhecidos e a relação entre eles foi explicitada.

Alguns aspectos tecnológicos sobre o funcionamento dos *cookies* também foram explicados, bem como o protocolo HTTP que serve de base para sua existência. Juntamente com classificações dos *cookies*, também foi mencionada a solução tecnológica implementada por meio de *consent management platform*, ou sistema de gestão de consentimento, mencionando decisão administrativa europeia sobre este assunto.

Conceitos sobe privacidade e proteção de dados também foram visitados, assim como princípios que os fundamentam. O trabalho apresentou elementos gerais de transparência, e outros elementos específicos. Também foram abordados aspectos sobre o caso brasileiro envolvendo políticas de privacidade do Whatsapp, assim como o guia orientativo sobre *cookies* e o Ofício da ANPD ao Governo Federal sobre os avisos de *cookies*, e ainda sobre a *E-Privacy Directive*.

No contexto brasileiro, foram trazidos pontos importantes sobre o Marco Civil da Internet, assim como do Direito do Consumidor, que também foi abordado quanto aos direitos básicos do consumidor, quanto ao consumidor *standard* e por equiparação, quanto ao fornecedor de serviços *online*. Algumas classificações sobre a vulnerabilidade do consumidor foram apresentadas, bem como sobre a autodeterminação informativa e a Lei de Defesa dos Usuários de Serviços Públicos.

Em seguida, a metodologia do trabalho foi explicada, detalhando a construção do robô de *software*, e ainda a forma como foram capturados os dados da pesquisa. O método de classificação dos dados também foi exposto, assim como as decisões de projeto tomadas no início e respectivas razões.

Os resultados da pesquisa empírica feita sobre 1.282 *websites* com TLD ".br" durante os anos de 2020 e 2022, antes e depois da vigência da LGPD, permitiram a coleta de dados de 1.188 e 1.160 *websites* que estavam acessíveis em 2020 e 2022 respectivamente. Das 21 categorias de *sites* do *corpus*, as 5 mais frequentes foram as de notícias, educação, governo, negócios e comércio eletrônico.

Os resultados mostraram que, com a vigência da Lei Geral de Proteção de Dados, o percentual de avisos de *cookies* subiu de 6,90% para 55,17% nos anos pesquisados, em consonância com outros dados coletados internacionalmente. Das categorias mais frequentes, os *sites* de governo foram os que tiveram menor adoção de tais avisos, indo de 1,31% para 39,84%.

Na anatomia dos avisos de *cookies* de 2022, o elemento afirmativo estava presente em 100% dos casos, o elemento informacional em 86,41% deles, o gerencial em 32,19% e o elemento negativo em 21,25%. Assim, os avisos cujo perfil tem apenas o elemento afirmativo e o informacional predominam no Brasil: eram 63,41% em 2020 e passaram a 58,12% em 2022. O intuito dos avisos dos *websites* para os usuários é basicamente o de informar e confirmar a única opção disponível – a de aceitar o uso de rastreadores, o que é confirmado pelo percentual de 78,75% dos *banners* que possuem componente afirmativo e não possuem elemento negativo – perfil *Confirmation Only* mostrado na Tabela 9 do trabalho.

Entre 2020 e 2022, a quantidade média de elementos nos avisos de *cookies* subiu de 2,1 para 2,4, indicando tendência de aumento da transparência e da legalidade da obtenção de autorização para tratamento de dados pessoais. O emprego de *cookie wall* no Brasil tem tendência de queda, de 2,44% para 1,88% dos casos. A presunção de consentimento tácito também diminuiu, porém continua alta, indo de 59,76% para 46,25% nos dois anos observados. Também o destaque para o elemento afirmativo caiu de 93,90% para 86,25%, apesar de ainda ser muito alto. No segundo nível dos *banners*, o perfil predominante é aquele que tem elemento negativo, e no qual os rastreadores estão desativados por padrão. O uso de textos em língua estrangeira também caiu nos anos

pesquisados, de 7,32% para 3,75%. O emprego de PETs, exemplificado pela adoção de sistemas de gestão de consentimento – CMPs – aumentou, como era de se esperar pela vigência da LGPD e urgência na adoção de medidas de transparência e legalidade, chegando a 12,34% dos casos em que os *websites* apresentavam algum dos tipos de *banner* de rastreamento.

Ao final, contabilizando os casos em que os critérios de primeiro e segundo nível são atendidos – A-N-G-I e A-N-C no primeiro e segundo nível respectivamente conforme a Tabela 22, chegou-se ao número absoluto de 8 *sites* (0,69% do total de 1.160 endereços acessíveis em 2022). E filtrando por atendimento de critérios adicionais sobre consentimento tácito, destaque para elemento afirmativo, uso de *cookie wall* e de língua estrangeira, apenas 4 *websites* (0,35% do total de 1.160 endereços acessíveis em 2022) atenderam no final aos requisitos definidos por este trabalho.

Quanto ao emprego de *dark patterns*, ou *deceptive patterns*, padrões obscuros ou padrões enganosos, muitos deles estavam presentes nos *banners*. A Ilusão de Controle, a Manipulação Estética e a Falsa Hierarquia são alguns dos exemplos mais recorrentes, dentre outros.

Algumas das saídas óbvias para questões discutidas neste trabalho são o aumento da transparência mediante informações claras, acessíveis e adequadas, diminuindo a assimetria da informação; adoção de padrões de interação que privilegiem a igualdade de condições entre fornecedores de *website*s e usuários, privilegiando a liberdade de escolha, evitando o emprego de *dark patterns*, e aplicando *nudges* para situações que beneficiem os titulares de dados e consumidores; ampliação da implementação de sistemas que fazem tratamento de dados com o uso de padrões calcados em *Privacy by Design*, garantindo assim a segurança dos serviços *online* em busca do atendimento à confiança que legitimamente se espera; implantação desses sistemas em configurações aderentes ao princípio *Privacy by Default*, contribuindo assim para o aumento da privacidade e diminuição do esforço do usuário dos serviços.

Outra possível medida para mitigar o problema da transparência é a melhoria da educação das pessoas quanto ao uso de seus dados na *Internet*, rastreamento e assuntos similares, assim como conscientização ética para os desenvolvedores de sistemas e *designers* de interação. Medida adicional é o incremento de transparência pela criação de formas melhores de comunicar sobre o uso de rastreadores e compartilhamento de dados

pessoais com terceiros. É interessante também a adoção de recurso baseado em *Visual Law*, tal como concebido por Lorrie Cranor sobre a solução análoga à tabela nutricional (CRANOR *et. al.*, 2010), ou ainda como a solução informativa sobre uso energético por eletrodomésticos adotada no Brasil.

Em especial, a implementação do *Privacy by Design*, tirando a responsabilidade da camada de apresentação do *website*, e movendo-a para o nível de configuração do navegador – para além da simples instalação de bloqueadores de *cookies* – é outra medida que contribui para o aumento da privacidade: o próprio navegador pode ter a configuração padrão prevenindo o compartilhamento de dados pessoais por *cookies* e outras tecnologias de rastreamento, diminuindo assim o atrito entre usuário e *website* fornecedor de serviços. Obviamente, como o desenvolvedor do navegador mais usado no mundo obtém sua receita majoritariamente a partir de anúncios publicitários, esta situação causa conflito de interesse no enfrentamento dessa questão, e uma saída para este ponto específico é a adoção de medidas que diminuam a concentração de mercado das *big techs*, impedindo que atuem em áreas conflitantes.

Assim, medida adicional é a cobrança, pelos órgãos reguladores de proteção de dados e de defesa do consumidor, de implementação de medidas que contribuam para o aumento da privacidade e da proteção de dados, com ações a serem executadas pelas próprias plataformas de navegação, os navegadores, então responsabilizando conjuntamente tanto os fornecedores de navegadores – desenvolvidos inclusive por empresas que lucram na outra ponta com o mercado de publicidade digital – quanto os próprios fornecedores de serviços *online* responsáveis pelos *website*s; tal implementação de *Privacy by Design*, como sugerida no parágrafo anterior, poderá mitigar riscos associados à confiança, à segurança, à proteção dos dados no compartilhamento com terceiros, à privacidade no rastreamento digital, riscos esses na maioria das vezes introduzidos pelos próprios *website*s, cujo funcionamento e transmissão de dados a terceiros atualmente foge do controle dos navegadores, que são a plataforma de suporte. Tal imposição de ônus poderia também recair nos órgãos que desenvolvem especificações técnicas e que são adotadas pelos agentes de mercado e se tornam padrões de fato, tais como a IETF e organismos correlacionados.

E quanto à pesquisa como um todo, ressalta-se que todos os projetos são capazes de ensinar algo: são as lições aprendidas dos projetos. Os desafios enfrentados nesta pesquisa foram muitos. Primeiro, o robô foi desenvolvido com tecnologia que foi

mudando ao longo do tempo, fruto de um trabalho que iniciou no primeiro semestre de 2020. O aprendizado de novas tecnologias, a pesquisa de soluções existentes e a falta de conhecimento inicial sobre que tipo de solução poderia dar as respostas buscadas foram alguns dos obstáculos superados. Inicialmente, o *software* capturou todos os dados dos rastreadores, as políticas de privacidade e as telas dos *websites*. A identificação automatizada de avisos de *cookies*, tal como feita por outros trabalhos comentados e com os quais esta pesquisa foi comparada, revelou-se uma tarefa dificílima, razão pela qual optou-se pela classificação manual, com tripla verificação dos resultados pelo mesmo pesquisador. Uma parte do trabalho classificou os *cookies* utilizando *machine learning*, porém os resultados não foram apresentados neste momento por necessidade de recorte metodológico.

Como mencionado, o escopo do trabalho teve que ser diminuído ao longo do tempo. O primeiro corte extirpou a análise das políticas de privacidade. Posteriormente, a tabulação de todos os dados, tanto sobre os rastreadores de *cookies* quanto sobre os avisos também foi complexa, pois demandou a criação de um microssistema de análise de dados, com mais de 40 planilhas interligadas, alimentadas por mais de 15 consultas complexas que foram feitas a 3 planilhas básicas: uma planilha geral, uma com dados sobre *cookies* e outra com dados sobe os *banners* de *cookies*. Estas 3 planilhas básicas, por sua vez, foram fruto de trabalho de processamento de dados automatizado e também manual, sendo que as fontes de dados brutos superaram os 50 Gigabytes.

Como os resultados da pesquisa estavam tomando proporções maiores do que o necessário para uma pesquisa de mestrado, então houve outra decisão: interromper a análise dos *cookies*, e focar apenas nos avisos de *cookies*. Os resultados sobre a análise dos *cookies*, junto com a dos respectivos *banners* dos *sites*, estava mostrando o que acontecia por dentro dos sistemas eletrônicos: apesar de os avisos de *cookies* indicarem uma determinada informação, na prática as decisões dos usuários não eram respeitadas. Porém, esta análise mais detalhada, que envolve os princípios de segurança e de confiança, será fruto de trabalhos posteriores a este, pois os dados já existem – sobre *cookies* e sobre políticas de privacidade – e podem ser comparados com outros ainda mais novos que vierem a ser produzidos em nível de Doutorado ou em outros caminhos acadêmicos.

As possibilidades de trabalhos futuros são imensas: a análise das mensagens de *banners* de primeiro nível, a análise de *sites* quanto a crianças e adolescentes, a análise

de políticas de privacidade e assemelhados, o uso de tecnologias de inteligência artificial para análise de textos usando a tecnologia BERT-LEGAL em português, a análise automatizada de *dark patterns* em mensagens de avisos, como o trabalho de Mathur *et. al.* (2019), e ainda o desenvolvimento de ferramentas de apoio ao *enforcement* a ser realizado pelas autoridades de proteção de dados, utilizando a tecnologia e o conhecimento produzidos nesta pesquisa científica.

Ao final, considera-se que ocorreu produção de algum conhecimento novo sobre a área de proteção de dados em relação à transparência dos *websites* em abordagem interdisciplinar. Todavia, há muito o que se fazer sobre este assunto. Uma das lições aprendidas sobre a situação atual dos sistemas eletrônicos empregados nos *websites* do Brasil é que, com a entrada da LGPD em vigor, aumentou – ao menos na aparência, e de forma bastante ampla – a preocupação dos controladores dos *websites* em cumprir as leis vigentes, ainda que o cumprimento possa se mostrar com baixa efetividade ou com muitos problemas de implementação. Todavia, é necessário avançar mais e sempre, ampliar o debate sobre o que a sociedade legitimamente espera e o que precisa para garantir seus direitos fundamentais – tanto do consumidor, quanto da proteção dos dados pessoais e da privacidade.

REFERÊNCIAS

ACQUISITI, Alessandro. ***The Economics of Personal Data and the Economics of Privacy.*** Disponível em: <https://www.oecd.org/sti/ieconomy/ 46968784.pdf>. Acesso em: 15 dez 2022

ADAMS, Paul C. ***Agreeing to Surveillance: Digital News Privacy Policies.*** Journalism & Mass Communication Quarterly, vol. 97, no. 4, Dec. 2020, pp. 868–889. Disponível em: <https://journals.sagepub.com/doi/10.1177/1077699020934197>. Acesso em: 18 mai 2022

BARTH, A., ***RFC 6265 – HTTP State Management Mechanism***. Disponível em: <https://www.rfc-editor.org/info/rfc6265>. Acesso em: 20 mai 2022.

BIELOVA Nataliia; MATTE, Célestin; SANTOS, Cristiana***. Are cookie banners indeed compliant with the law?*** Technology and Regulation, 2020, 91–135 • https://doi.org/10.26116/techreg.2020.009 • ISSN: 2666-139X. Disponível em: <https://arxiv.org/pdf/1912.07144.pdf>. Acesso em: 15 jan 2023

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** 2ª Reimpr. Rio de Janeiro: Forense, 2019.

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

BLUM, Renato Ópice; MALDONADO, Viviane Nóbrega (orgs.). **Lei geral de proteção de dados comentada.** 2. ed. rev. atual. ampl. São Paulo: Thomson Reuters Brasil, 2019.

BLUM, Rita Peixoto Ferreira. **O direito à privacidade e à proteção dos dados do consumidor**. São Paulo: Almedina, 2018.

BOERMAN, Sophie C.; BORGESIUS, Frederik J. Zuiderveen; KRUIKEMEIER, Sanne. ***Online Behavioral Advertising: A Literature Review and Research Agenda***. Journal of Advertising, 46:3, 363-376, 2017. Disponível em: <https://pure.uva.nl/ws/files/16200980/Online_Behavioral_Advertising.pdf>. Acesso em: 22 mai 2022

BOLLINGER, Dino. ***Analyzing Cookies Compliance with the GDPR.*** Zurich: 2021. Disponível em: <https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/477333/Bollinger_Dino.pdf?isAllowed=y&sequence=1>. Acesso em: 18 out 2022

BORGESIUS, Frederik J. Zuiderveen *et. al*. ***Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation.*** European Data Protection Law Review, Vol. 3, no. 3, pp. 353 – 368, 2017. Disponível em: <https://pure.uva.nl/ws/files/19576493/EDPL_Tracking_Walls.pdf>. Acesso em: 25 mar 2022

BÖSCH, Christoph *et. al.* ***Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark patterns***. Proceedings on Privacy Enhancing Technologies; 2016 (4):237–254. De Gruyer Open. Disponível em: <http://rolandhubscher.org/courses/hf765/readings/Boesch_2016.pdf>. Acesso em: 25 mar 2022

BRASIL. **Constituição da República Federativa do Brasil**. Disponível em: < https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 18 abr 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências.** Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 28 set 2022.

BRASIL. **Lei 10.098 de 2000. Estabelece normas gerais e critérios básicos para a promoção da acessibilidade das pessoas portadoras de deficiência ou com mobilidade reduzida, e dá outras providências.** Disponível em: <http://www.planalto. gov.br/ccivil_03/LEIS/L10098.htm>. Acesso em: 08 set 2022.

BRASIL. **Decreto 5.903, de 20 de setembro de 2006. Regulamenta a Lei no. 10.962, de 11 de outubro de 2004, e a Lei no 8.078, de 11 de setembro de 1990**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/decreto/d5903.htm>. Acesso em: 03 jan 2023.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011. Lei do Cadastro Positivo. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 10 mar 2023

BRASIL. **Decreto nº 7.962, de 15 de março de 2013. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm>. Acesso em: 18 mar 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 17 set 2022.

BRASIL. **Lei nº 13.146, de 6 de julho de 2015. Institui a Lei Brasileira de Inclusão da Pessoa com Deficiência (Estatuto da Pessoa com Deficiência).** Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13146.htm>. Acesso em: 10 set 2022.

BRASIL. **Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na *Internet* e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na**

requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 16 set 2022.

BRASIL. **Lei 13.460, de 26 de junho de 2017. Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13460.htm>. Acesso em: 26 set 2022.

BRASIL. **Lei no 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <http://www.planalto.gov.br/ ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 15 mai 2022.

BRASIL. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.** Brasília, 2022. Disponível em: < https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper >. Acesso em: 15 set 2022.

BRASIL. **Nota Técnica no 46/2022/CGF/ANPD.** Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000730_2022_53-nt-46.pdf>. Acesso em: 15 set 2022.

BRASIL. **Nota Técnica nº 49/2022/CGF/ANPD**. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt_49_2022_cfg_anpd_versao_publica.pdf>. Acesso em: 15 set 2022.

BRASIL. **Guia orientativo sobre *cookies* e proteção de dados pessoais.** Brasília, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-*cookies*-e-protecao-de-dados-pessoais.pdf>. Acesso em: 08 jan 2023.

BRIGNULL, Harry. 2011. ***Dark patterns: Deception vs. Honesty in UI Design***. Disponível em: <https://alistapart.com/article/dark-*patterns*-deception-vs.-honesty-in-ui-design>. Acesso em: 31 jan 2023.

BRIGNULL, Harry *et. al*. 2023. ***Dark patterns - User Interfaces Designed to Trick You***. Disponível em: <https://www.deceptive.design>. Acesso em: 31 jan 2023.

BUCKLER, David *et. al.* ***Prevalence of Third-Party Tracking on COVID-19– Related Web Pages.*** Disponível em: <https://www.timlibert.me/pdf/ McCoy_et_al-2020-Covid_Web_Tracking.pdf>. Acesso em: 07 mai 2022.

BUDA, Richard.; ZHANG, Yong. ***Consumer Product Evaluation: the interactive effect of message framing, presentation order and source credibility***. Journal of Product & Brand Management. v. 9, n. 4, p. 229-242, 2000. Disponível em: <http://www.sabilfeb.lecture.ub.ac.id/files/2014/04/857732.pdf>. Acesso em: 22 mai 2022

CARISSIMI, Alexandre da Silva; GRANVILLE, Lisandro Zambenedetti; ROCHOL, Juergen. **Redes de computadores.** Série Livros didáticos; n. 20. Porto Alegre: Bookman, 2009. E-book.

CAVOUKIAN, Ann. ***Privacy by Design. The 7 Foundational Principles*.** Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Acesso em: 15 mai 2022.

CIELO. **Cielo – Máquina de cartão de crédito e débito.** Disponível em: <https://www.cielo.com.br>. Acesso em: 01 set 2022.

COMPUTER WEEKLY. ***Political parties harvest personal data to create profiles on voters, most of it wrong***. Disponível em: < https://www.computerweekly.com/news/252485111/Political-parties-harvest-personal-data-to-create-profiles-on-voters-most-of-it-wrong >. Acesso em: 12 dez 2022.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados: comentada**. 3. ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, Thomson Reuters Brasil, 2020. 263 p.

CRANOR, Lorrie Faith; MCDONALD, Aleecia M. ***The Cost of Reading Privacy Policies*.** In: I/S: A Journal of Law and Policy for the Information Society. 2008 Privacy Year in Review issue. http://www.is-journal.org/ Disponível em: <https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>. Acesso em: 02 out 2022

CRANOR, Lorrie Faith *et. al.* ***Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach***. Disponível em: <https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab09014.pdf>. Acesso em: 10 dez 2022

CRANOR, Lorrie Faith. ***Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice***. Journal on Telecommunications and High Technology Law 10, no. 2 (2012): 36. Disponível em: <http://www.law.nyu.edu/sites/default/files/upload_documents/Cranor%20-%20Necessary%20but%20Not%20Sufficient.pdf>. Acesso em: 10 dez 2022

CULNAN, Mary J.; MILNE, George R. ***Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices***. In: Journal of Interactive Marketing. vol. 18. no. 3. Ano: 2004. Disponível em: <https://journals.sagepub.com/doi/10.1002/dir.20009>. Acesso em: 22 mai 2022

DEGELING, Martin *et. al.* ***We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy***. Disponível em: <https://arxiv.org/pdf/1808.05096.pdf>. Acesso em: 08 jun 2022

DE LIMA, Cíntia Rosa Pereira. **Validade e obrigatoriedade dos contratos de adesão eletrônicos (*Shrink-wrap* e *click-wrap*) e dos termos e condições de uso (*browse-wrap*)**: um estudo comparado entre Brasil e Canadá. 2009. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2009. Disponível em:

http://www.teses.usp.br/teses/disponiveis/2/2131/tde-03062011-090910/?&lang=pt-br. Acesso em: 17 set. 2022.

DE LIMA, Cíntia Rosa Pereira. **O ônus de ler o contrato no contexto da "ditadura" dos contratos de adesão eletrônicos.** 2014, Anais. Florianópolis, SC: CONPEDI, 2014. Disponível em: <https://edisciplinas.usp.br/pluginfile.php/5727704/mod_resource/content/1/O%20O%CC%82uns%20de%20Ler%20o%20Conteu%CC%81do%20do%20Contrato...%20%28Profa%20Ci%CC%81ntia%20Rosa%29.pdf>. Acesso em: 17 set. 2022.

DE LIMA, Cíntia Rosa Pereira *et. al*. **Comentários à lei geral de proteção de dados: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019.** São Paulo: Almedina, 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados.** 2ª ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo *et. al.* **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021. E-book.

ERMAKOVA, Tatiana; FABIAN, Benjamin; LENTZ, Tino. ***Large-scale readability analysis of privacy policies*.** Proceedings of the International Conference on Web Intelligence (WI '17). pp 18–25. New York: 2017. Disponível em: <https://dl.acm.org/doi/10.1145/3106426.3106427>. Acesso em: 01 fev 2022

ETTELDORF, Christina. ***A New Wind in the Sails of the EU ePrivacy-Regulation or Hot Air Only? On an Updated Input from the Council of the EU under German Presidency*.** European Data Protection Law Review (EDPL) 6. no. 4. pp. 567-573. 2020. Disponível em: <https://edpl.lexxion.eu/article/EDPL/2020/4/13>. Acesso em: 01 ago 2022

FIELDING, Roy *et. al.* ***RFC 2616 – Hypertext Transfer Protocol – HTTP/1.1.*** Disponível em: <https://www.rfc-editor.org/info/rfc2616>. Acesso em: 10 mai 2022.

FORBRUKERRÅDET. ***Deceived by Design. How tech companies use dark patterns to discourage us from exercising our rights to privacy.*** 27.06.2018. Disponível em: <https://fil.forbrukerradet.no/wp-content/uploads/2018/ 06/2018-06-27-deceived-by-design-final.pdf>. Acesso em: 12 dez 2022

FOWLER, Geoffrey A. ***I tried to read all my app privacy policies. It was 1 million words.*** Disponível em: <https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/>. Acesso em: 11 mai 2022.

FRANCO, Cezar Augusto de Oliveira *et. al.* **A proteção do consumidor contra as mensagens subliminares dolosas.** Revista de Direito do Consumidor. vol. 116. ano 27. São Paulo: Ed. RT, mar-abr. 2018. Disponível em: <https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/665/591>. Acesso em: 13 jan 2023

FROTA, Pablo Malheiros da Cunha; RAMOS, André Luiz Arnt. **Produtos de conteúdo virtual: linguagem comercial abusiva, juridiquês e a disciplina jurídica do comércio eletrônico no Brasil**. Revista de Direito do Consumidor. vol. 116. ano 27. São Paulo: Ed. RT, mar-abr. 2018. Disponível em: <https://bdjur.stj.jus.br/jspui/bitstream/2011/121306/digital_content_products_ramos.pdf>. Acesso em: 13 jan 2023

GALITZ, Wilbert O. ***The essential guide to user interface design: an introduction to GUI design principles and techniques.*** 3. ed. Indianapolis: Wiley Publishing, Inc, 2007. E-book. Acesso em: 22 mai 2022

GRAEPEL, Thore; KOSINSKI, Michal; STILLWELL, David. ***Private traits and attributes are predictable from digital records of human behavior***. Proceedings of the National Academy of Sciences. April 9, 2013. vol. 110. no. 15. 5802-5805. Disponível em: <https://www.pnas.org/doi/epdf/10.1073/pnas.1218772110>. Acesso em: 12 dez 2022.

GRAßL *et. al.* ***Dark and bright patterns in cookie consent requests***. (2021). Disponível em: <https://pdfs.semanticscholar.org/4f08/7abeb923dbaf5cd730a3dd55940628a4c817.pdf?_gl=1*17iew*_ga*MTQ1MjQ4NjU2Ny4xNjU0OTAzMjAy*_ga_H7P4ZT52H5*MTY4NDc4MTkzOC40MS4xLjE2ODQ3ODI3NDguNTYuMC4w>. Acesso em: 01 ago 2022

GRAY *et. al.* ***The dark (patterns) side of UX design***. In R. Mandryk, M. Hancock, M. Perry, & A. Cox (Eds.), Proceedings of the 2018 CHI Conference on Human Factors in Comput- ing Systems - CHI ’18 (pp. 1–14). New York, New York, USA: ACM Press. https://doi.org/10.1145/3173574.3174108. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108>. Acesso em: 01 ago 2022

GRINOVER, Ada Pellegrini *et. al.* **Código Brasileiro de Defesa do Consumidor: comentado pelos autores do anteprojeto: direito material e processo coletivo**. vol. ún. 12. ed. Rio de Janeiro: Forense, 2019.

GUERRA *et. al.* (2017). **Análise das relações entre traços de personalidade, compra impulsiva e compra compulsiva**. Consumer Behavior Review, 1(1) 24-37. Disponível em: <https://periodicos.ufpe.br/revistas/cbr/article/view/15183/18721>. Acesso em: 12 dez 2022

HANSEN, Pelle Guldborg. ***The Definition of Nudge and Libertarian Paternalism: Does the Hand Fit the Glove?*** European Journal of Risk Regulation, 7(1), 155-174. doi:10.1017/S1867299X00005468 (2016). Disponível em: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/16D7A1CBCE9928E3E9ED713BF48C315C/S1867299X00005468a.pdf/div-class-title-the-definition-of-nudge-and-libertarian-paternalism-does-the-hand-fit-the-glove-div.pd>. Acesso em:

IAPP. ***CJEU to consider questions from IAB Europe TCF decision***. Disponível em: <https://iapp.org/news/a/cjeu-to-consider-questions-from-iab-europe-tcf-decision/>. Acesso em: 12 dez 2022

INTERNATIONAL CHAMBER OF COMMERCE UK. ICC UK. ***Cookie guide.*** **November 2012.** Disponível em: <https://www.*cookie*law.org/wp-content/uploads/2019/12/icc_uk_*cookies* guide _revnov.pdf>. Acesso em:17 set 2022.

JABLONOWSKA, Agnieszka; MICHALOWICZ, Adrianna. ***Planet49: Pre-Ticked Checkboxes Are Not Sufficient to Convey User's Consent to the Storage of Cookies (C-673/17 Planet49)***. European Data Protection Law Review. Volume 6, Issue 1 (2020). pp. 137 – 142. Disponível em: <https://edpl.lexxion.eu/article/EDPL/2020/1/19>. Acesso em:12 dez 2022

JOLLS, Christine; SUSTEIN, Cass R; THALER, Richard H. ***A Behavioral Approach to Law and Economics***. 50 Stanford Law Review 1471 (1998). Disponível em: <https://dash.harvard.edu/bitstream/handle/1/12921734/A%20Behavioral%20Approach%20to%20Law%20and%20Economics.pdf?sequence=1>. Acesso em:12 dez 2022

JONES, Tim, ***Facebook's "evil interfaces"***. Disponível em: <https://www.eff.org/de/deep*links*/2010/04/facebooks-evil-interfaces>. Acesso em: 01 ago 2022

JURUENA, Cynthia Gruendling; VALLE, Vivian Cristina Lima López. **O usuário do serviço público e a aplicação da Lei 13.460/2017 sob o enfoque dos Poderes Executivo e Judiciário**. Seqüência: Estudos Jurídicos e Políticos, [S. l.], v. 42, n. 87, p. 1–29, 2021. DOI: 10.5007/2177-7055.2021.e76786. Disponível em: <https://periodicos.ufsc.br/index.php/sequencia/article/view/76786>. Acesso em: 2 out. 2022.

KAMANTAUSKAS, Povila. ***Formation of Click-Wrap and Browse-Wrap Contracts*.** Teises Apzvalga Law Review. no. 12. pp 51-88. 2015. Disponível em: <https://www.vdu.lt/cris/bitstreams/1ca95f67-7c8f-44ef-b6cf-4aa95c31798e/download>. Acesso em: 01 ago 2022

KAMPANOS, Georgios; SHAHANDASHTI, Siamak F. ***Accept All: The Landscape of Cookie Banners in Greece and the UK*.** Disponível em: <https://arxiv.org/abs/2104.05750>.Acesso em 05 jun 2022.

KHANDELWAL, Rishabh *et. al.* ***CookieEnforcer: Automated Cookie Notice Analysis and Enforcement***. ArXiv abs/2204.04221 (2022): n. pag. Disponível em: <https://arxiv.org/pdf/2204.04221.pdf>. Acesso em: 05 jun 2022

KLEIN, David *et. al.* ***Accept All Exploits: Exploring the Security Impact of Cookie Banners***. Proceedings of the 38th Annual Computer Security Applications Conference (2022): n. pag. Disponível em: <https://dl.acm.org/doi/10.1145/3564625.3564647>. Acesso em: 05 jun 2022

KOSINSKI *et. al*. ***Personality and Website Choice***. ACM Web Sciences 2012 | January 2012. Published by ACM Conference on Web Sciences. Disponível em: <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/person_WebSci_final.pdf>. Acesso em: 12 dez 2022.

KOSTA, Sokol; SØRENSEN, Jannick Kirk. ***Before and After GDPR: The Changes in Third Party Presence at Public and Private European Websites***. The World Wide Web Conference. 2019. Disponível em: <https://dl.acm.org/doi/10.1145/3308558.3313524>. Acesso em: 05 jun 2022

KRISAM, Chiara *et. al.* ***Dark patterns in the Wild: Review of Cookie Disclaimer Designs on Top 500 German Websites***. Proceedings of the 2021 European Symposium on Usable Security (2021): n. pag. Disponível em: <https://pure.itu.dk/ws/files/86390699/Cookies_Dark_Patterns_EuroUSEC_6.pdf>. Acesso em: 02 out 2022

KULYK *et. al.* ***"This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer***. (2018). Disponível em: <https://www.ndss-symposium.org/wp-content/uploads/2018/06/eurousec2018_12_Kulyk_paper.pdf>. Acesso em: 02 out 2022

LE POCHAT, Victor, *et. al.* ***Tranco: A Research-Oriented Top sites Ranking Hardened Against Manipulation*.** Proceedings 2019 Network and Distributed System Security Symposium. 2019. Disponível em: <https://arxiv.org/pdf/1806.01156.pdf>. Acesso em: 15 mar 2022

LUNA, Florencia. ***Elucidating the Concept of Vulnerability: Layers Not Labels***. International Journal of Feminist Approaches to Bioethics 2, no. 1 (2009): 121–39, https://doi.org/10.3138/ijfab.2.1.121. Disponível em: <https://utpjournals.press/doi/10.3138/ijfab.2.1.121>. Acesso em: 02 out 2022

MALGIERIA, Gianclaudio; NIKLAS, Je Ꭰrzej. ***Vulnerable data subjects***. computer law & security review 37 (2020) 105415. Disponível em: <https://orca.cardiff.ac.uk/id/eprint/133307/1/1-s2.0-S0267364920300200-main(1).pdf>. Acesso em: 13 dez 2022.

MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais**. 9. ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2019.

MENDES, Laura Schertel. **A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais**. Revista de Direito do Consumidor. vol. 102. ano 24. p. 19-43. São Paulo: Ed. RT, nov.-dez. 2015. Disponível em: <https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/download/441/385/>. Acesso em: 13 jan 2023

MENDES, Laura Schertel Ferreira **Autodeterminação informativa: a história de um conceito.** PENSAR, FORTALEZA, v. 25, n. 4, p. 1-18, out./dez. 2020. Disponível em <https://periodicos.unifor.br/rpen/article/view/10828/pdf>. Acesso em 11 set 2022.

MIRAGEM, Bruno. **Princípio da vulnerabilidade: perspectiva atual e funções no direito do consumidor contemporâneo**. In (MIRAGEM *et. al.*, 2021): Direito do consumidor: 30 anos do CDC: da consolidação como direito fundamental aos atuais desafios da sociedade / Amanda Flávio de Oliveira... [*et. al.*]; organização Bruno Miragem, Claudia Lima Marques, Lucia Ancona Lopez de Magalhães Dias. Rio de Janeiro: Forense, 2021.

MORAIS, Ezequiel. **A boa-fé objetiva pré-contratual: deveres anexos de conduta.** 2. ed. São Paulo: Thomson Reuters Brasil, 2021. 2. ed. em e-book baseada na 2. ed. impressa. E-book.

MOZILLA.ORG. **O que é Javascript?** Disponível em: <https://developer.mozilla.org/pt-BR/docs/Learn/JavaScript/First_steps/What_is_JavaScript>. Acesso em: 05 mai 2022.

NEVES, Daniel Amorim Assumpção; TARTUCE, Flávio. **Manual de direito do consumidor: direito material e processual.** vol. ún. 11. ed. Rio de Janeiro: Forense, 2022.

NODEJS.ORG. **Sobre Node.js.** Disponível em: <https://nodejs.org/pt-br/about/>. Acesso em 05 mai 2022.

NOGUEIRA MATIAS, J. L.; VASCONCELOS CAMURÇA, L. C. **Direito à privacidade e à proteção de dados pessoais: análise das práticas obscuras de direcionamento de publicidade consoante a lei n° 13.709, de 14 de agosto de 2018**. Revista de Direitos Fundamentais & Democracia, [s. l.], v. 26, n. 2, p. 6–23, 2021. DOI 10.25192/issn.1982-0496.rdfd.v26i21590. Disponível em: <https://search.ebscohost.com/login.aspx?direct=true&db=foh&AN=152964828&lang=pt-br&site=eds-live>. Acesso em: 5 fev. 2023.

NOUWENS *et. al.* ***Dark patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence.*** Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (2020): n. pag. Disponível em: <https://dspace.mit.edu/bitstream/handle/1721.1/129999.2/3313831.3376321.pdf;jsessionid=12CA3ADA8FF9594C6DC271E060AD0795?sequence=6>. Acesso em: 02 out 2022

OPENWPM. ***A web privacy measurement framework*.** Disponível em: <https://github.com/openwpm/OpenWPM>. Acesso em: 05 mai 2022.

ORACLE. **O que é Big Data?** Disponível em: <https://www.oracle.com/br/big-data/what-is-big-data/>. Acesso em: 13 set 2022.

PAIM, Rafael *et. al.* **Gestão de processos: pensar, agir e aprender.** Porto Alegre: Bookman, 2009. E-book.

PALHARES, Felipe *et. al.* **Temas Atuais de Proteção de Dados.** 1. ed. São Paulo: Thomson Reuters Brasil, 2020. 1. ed. em e-book baseada na 1. ed. impressa. E-book.

PEREIRA, Caio Mário da Silva. **Instituições de direito civil: contratos.** 25. ed. Rio de Janeiro: Forense, 2022.

POULLET, Yves. ***About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?*** In: Data Protection in a Profiled World. Springer Science+Business Media B.V., 2010. Disponível em:

<https://link.springer.com/chapter/10.1007/978-90-481-8865-9_1>. Acesso em: 02 ago 2022

POZEN, David (2005). ***The Mosaic Theory, National Security, and the Freedom of Information Act***. The Yale Law Journal. v. 115. pp. 628–679. Disponível em: < https://www.yalelawjournal.org/pdf/358_fto38tb4.pdf >. Acesso em: 12 dez 2022.

PPTR. **Puppeteer.** Disponível em: <https://pptr.dev>. Acesso em: 05 mai 2022.

SAMSON, Alain (2015). **Introdução à economia comportamental e experimental.** Parte I. In Avila, F. e Bianchi, A. (Orgs.)(2015). Guia de Economia Comportamental e Experimental. São Paulo. EconomiaComportamental.org. Disponível em: <https://www.economiacomportamental.org>. Licença: Creative Commons Attribution CC-BY-NC – ND 4.0. Acesso em: 12 dez 2022

SEGIJN, Claire M. ***A new mobile data driven message strategy called synced advertising: Conceptualization, implications, and future directions***. Annals of the International Communication Association, 43:1. pp. 58-77. 2019. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/23808985.2019.1576020?journalCode=rica20>. Acesso em: 15 mai 2022

SELENIUM. **O Projeto Selenium de Automação de Navegadores.** Disponível em: <https://www.selenium.dev/pt-br/documentation/>. Acesso em: 05 mai 2022.

SOLOVE, Daniel J. ***Introduction: Privacy Self-Management and the Consent Dilemma*.** Harvard Law Review 126. pp. 1880-1903. 2013. Disponível em: <https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2093&context=faculty_publications>. Acesso em: 05 mai 2022

SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais: pluralismo jurídico e transparência em perspectiva.** São Paulo: Thomson Reuters Brasil, 2019.

STATCOUNTER. ***Desktop Browser Market Share South America***. Disponível em: <https://gs.statcounter.com/browser-market-share/desktop/south-america/#monthly-202003-202003-bar>. Acesso em: 01 abr 2022.

SUSTEIN, Cass R. ***Why Nudge? The Politics of Libertarian Paternalism.*** New Haven: Yale University Press, 2014. Disponível em: <https://www.jstor.org/stable/j.ctt5vm0nr>. Acesso em: 12 dez 2022

SUSTEIN, Cass R; THALER, Richard H. ***Nudge*: como tomar melhores decisões sobre saúde, dinheiro e felicidade**. / Richard H. Thaler, Cass R. Sunstein; tradução Ângelo Lessa. — 1ª ed. — Rio de Janeiro: Objetiva, 2019.

TECHNOLOGY REVIEW. ***Differential privacy***. Disponível em: <https://www.technologyreview.com/10-breakthrough-technologies/2020/#differential-privacy>. Acesso em: 15 mai 2022.

TEPEDINO, Gustavo *et. al.* **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** 1.ed. São Paulo: Revista dos Tribunais, 2019.

THALER, Richard H. ***Behavioral Economics: Past, Present, and Future***. Disponível em: <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2790606_code74929.pdf?abstractid=2790606&mirid=1>. Acesso em: 12 dez 2022

THALER, Richard H. ***Nudge, not sludge***. Science, 361 (6401), 431–431. https://doi.org/10.1126/science.aau9241 (2018). Disponível em: <https://pubmed.ncbi.nlm.nih.gov/30072515/>. Acesso em: 12 dez 2022

TRADEZONE. **Tradezone – Bem vindo ao futuro!** Disponível em: <https://www.tradezone.com.br>. Acesso em: 02 set 2022.

TURING, Dermot. **História da Computação: do Ábaco à Inteligência Artificial**. São Paulo: Editora M.Books, 2019.

UNIÃO EUROPEIA. ***Opinion 4/2007 on the concept of personal data***. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>. Acesso em: 12 set 2022.

UNIÃO EUROPEIA. **DIRECTIVA 2009/136/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 25 de Novembro de 2009 que altera a Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas, a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas e o Regulamento (CE) no. 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor.** Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX: 32009L0136&from= EN>. Acesso em: 14 set 2022.

UNIÃO EUROPEIA. ***Guidelines on transparency under Regulation 2016/679*.** Bruxelas, 2017. Disponível em: < https://ec.europa.eu/newsroom/article29/redirection/document/51025>. Acesso em: 14 set 2022.

UNIÃO EUROPEIA. **REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/? uri=CELEX: 32016R0679 &from=EN. Acesso em: 12 set 2022.

UNIÃO EUROPEIA. ***Storing cookies requires Internet users' active consent*.** Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190125en.pdf. Acesso em: 13 jan 2023

UNIÃO EUROPEIA. ***Article 29 Working Party*.** Disponível em <https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en>. Acesso em: 14 set 2022

URBAN, Tobias *et. al.* ***Beyond the Front Page:Measuring Third Party Dynamics in the Field*.** Proceedings of The Web Conference 2020. 2020. Disponível em: <https://arxiv.org/pdf/2001.10248>. Acesso em: 02 ago 2022