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

RODRIGO TOLER

USO DO *LEGAL DESIGN* NOS AVISOS DE PRIVACIDADE PARA EFETIVAÇÃO DA PROTEÇÃO DE DADOS

SÃO PAULO
2023

RODRIGO TOLER

USO DO *LEGAL DESIGN* NOS AVISOS DE PRIVACIDADE PARA EFETIVAÇÃO DA PROTEÇÃO DE DADOS

Dissertação de Mestrado desenvolvida sob a orientação da professora Dra. Tainá Aguiar Junquilho e Danilo Cesar Maganhoto Doneda (*in memorian*), apresentada para obtenção do título de Mestre em Direito, Justiça e Desenvolvimento.

SÃO PAULO
2023

RODRIGO TOLER

USO DO *LEGAL DESIGN* NOS AVISOS DE PRIVACIDADE PARA EFETIVAÇÃO DA PROTEÇÃO DE DADOS

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.

BANCA EXAMINADORA

_____

Prof. Dra. Tainá Aguiar Junquilho IDP

_____

Prof. Dr. João Paulo Lordelo

IDP

_____

Prof. Dr. Vinicius José Poli USP

AGRADECIMENTOS

Quando decidi embarcar nesta jornada acadêmica, jamais poderia imaginar que ela se tornaria uma das mais significativas da minha carreira. A partir de uma mudança de perspectiva e, experimentando ousar, foi possível me confrontar comigo mesmo, com minhas vulnerabilidades, minhas virtudes, minha vaidade e humildade e, assim, me colocar em um lugar diferente. O caminho não foi fácil, e cada passo dado representou um desafio a ser superado. Mas, graças ao apoio das pessoas aqui mencionadas, e tão importantes na minha vida, hoje posso finalmente celebrar esta conquista.

Gostaria de começar agradecendo à minha amada esposa, Maria Elisa, que sempre esteve ao meu lado, me incentivando, me levantando do chão, me apoiando, me motivando e, sempre, confiando em mim. Sem o seu amor, dedicação e renúncias, eu jamais teria chegado até aqui. Obrigado por ter se mantido ao meu lado, junto com nosso filho Miguel, mesmo quando as coisas pareciam impossíveis. Obrigado por ser minha companheira de vida, minha melhor amiga e maior incentivadora.

Gostaria de agradecer também ao meu grande amigo Vinicius Poli. Desde a faculdade, ele se mostrou um grande parceiro, me ajudando a superar as mais diversas dificuldades e a compreender melhor os conceitos e teorias estudadas ao longo da jornada. Obrigado por ter me apresentado um mundo novo, ter me ajudado a expandir minha visão de mundo e, sempre, me desafiar intelectualmente. Sua amizade é um dos maiores tesouros que eu poderia ter em minha vida.

Agradeço também à minha orientadora, Tainá Junquilho. Sua orientação foi fundamental para possibilitar a conclusão do trabalho. Obrigado por ter me direcionado com paciência, tranquilidade e sabedoria, por ter me encorajado a ser mais ousado em minhas reflexões. Seu comprometimento e profissionalismo são exemplos que espero seguir por toda a minha vida.

Ao professor, João Lordelo que, prontamente, atendendo a pedido emergencial, aceitou o convite de participar da banca de qualificação e contribuiu de forma muito enriquecedora com seus comentários que foram acatados e incorporados ao trabalho.

Não posso deixar aqui de render minha homenagem e gratidão ao colega de IDP Fabio Lopes Toledo, pelos incansáveis esclarecimentos, apoio institucional e parceria nos momentos de mais desesperos. Fábio, obrigado por iluminar os caminhos até aqui.

Por fim, quero fazer um agradecimento póstumo ao estimado professor Danilo Doneda. Sua precoce ausência é sentida por toda a comunidade que trabalha, direta ou indiretamente,

com privacidade e proteção de dados. Embora tenha partido antes de eu finalizar este trabalho, sua contribuição no começo desta orientação e em todas as aulas e seminários, com todo apoio intelectual, entusiasmo e generosidade, jamais serão esquecidos. Para área de proteção de dados isso é inegável. Seu legado se faz presente em cada linha desta dissertação, e espero que meu trabalho possa ser uma pequena homenagem a sua memória.

Aos meus familiares, amigos e colegas de trabalho, também gostaria de agradecer. Sua torcida e apoio foram essenciais para que eu pudesse chegar até aqui. Obrigado por acreditarem em mim e por me ajudarem a realizar este sonho.

Este é um momento de muita emoção e alegria para mim, e espero que todos que me acompanharam nesta jornada possam compartilhar dessa felicidade. Que esta conquista seja mais um recomeço, de muitos outros, e que possamos seguir em frente juntos, aprendendo, crescendo e contribuindo para um mundo melhor. Obrigado a todos.

Cito, aqui, uma frase exposta no rótulo dos vinhos produzidos por Alejandro Vigil, da bodega El Enemigo: “No final do caminho você só se lembra de uma batalha, aquela que travou consigo mesmo, o verdadeiro inimigo, a batalha que te tornou único”.

O que é a lei – e o que é nosso sistema legal – não é o que está escrito nos livros. É o que é experimentado pelas pessoas que usam o sistema – como litigantes, como réus criminais, como leigos que estão tentando obter ajuda legal.

(Margaret Hagan)

Não é a tecnologia que determina se uma sociedade é livre ou não, mas sim as instituições políticas e econômicas que as usam.

(José Saramago)

RESUMO

O trabalho se propõe a analisar a aplicabilidade do *Legal Design* nos documentos de privacidade vocacionado aos titulares dos dados pessoais. A proposta é analisar a forma de evolução de comunicação e o seu impacto no mundo contemporâneo, as funções que a tecnologia deve assumir dentro da sociedade, sem que exerça controle sobre ela, e a efetividade dos princípios da informação, da transparência e da finalidade, importantes instrumentos legais que garantem a proteção de dados pessoais. O presente trabalho conseguiu concluir que, quando se fala a respeito de uma linguagem própria da juridicidade, deve-se entender que uma parcela bem pequena da população compreende o que o documento está querendo dizer. O *Legal Design*, nesse sentido, possui diversas práticas que estão relacionadas a outras áreas do conhecimento, como a Linguagem Simples e Arquitetura das Plataformas, que, em conjunto com as demais estruturas que compõem os documentos jurídicos, possuem a capacidade de transformar este conceito. Para se obter uma resposta ao problema desenvolvido, foram utilizadas: pesquisa bibliográfica, pesquisas em revistas eletrônicas especializadas e análise dos documentos sobre proteção de dados nacionais e internacionais produzidos pelas autoridades competentes. Foram analisados os avisos de privacidade da Skol; L'Oreal; Sanofi e PlayStation, com aplicação das técnicas de *Legal Design*. Conclui-se que a aplicação do *Legal Design* nos avisos de privacidade torna as informações mais acessíveis e compreensíveis aos titulares de dados pessoais, possibilitando mais compreensão da forma de tratamento e exercício dos seus direitos.

Palavras-chave: Transparência. Compreensão. Avisos de Privacidade. *Legal Design*.

ABSTRACT

This paper proposes to analyze the applicability of Legal Design in privacy documents aimed at the holders of personal data. The proposal is to analyze the formo f communication Evolution and its impact on the contemporary world, the functions that technology must assume within society, without exercising control over it, and the effectiveness of the principles of information, transparency and purpose, importante legal instruments that guarantee the protection of personal data. The presente work was able to conclude that, When ono talks about the language of legality, it must be understood that a very small portion of the population understands what the document is trying to say. Legal Design, in this sense, has several practices that are related to other áreas of knowledge, such as Simple Language and Platform Architecture, which, together with the Other structures that make up legal documents, have the ability to transform this concept. To obtain an answer to te problem developed, the following were used: bibliographic research, research in specialized electronic journals, and analysis of national and international data protection documents produced by the competente authorities. The privacy notices from Skol; L'Oreal; Sanofi and PlayStation were analyzed, with the application of Legal Design techniques. The conclusion is that the application of Legal Design in privacy notices makes the information more acessible and understandable to the holders of personal data, enabling a better understanding of the form of treatment and exercise of their rights.

Keywords: Transparency. Understanding. Privacy Notices. Legal Design.

SUMÁRIO

1 INTRODUÇÃO

O uso da tecnologia tem proporcionado à sociedade uma multiplicidade de produtos e serviços que antes eram restritos apenas a grandes centros urbanos e que, para serem comercializados, necessitavam da interação física e direta entre os interlocutores. A gama de serviços oferecidos pelas plataformas digitais tem aumentado à medida que novas soluções surgem para facilitar o dia a dia. Desde o transporte, em que se pode utilizar aplicativo para encontrar um profissional com nossa rota preestabelecida, passando pela nossa alimentação, com um amplo cardápio disponível que registra nossas preferências, até nosso entretenimento, para o qual as plataformas de *streaming* fornecem filmes, séries, desenhos e documentários dos mais variados.

Os dados se tornam cada vez mais importantes para a sociedade e são comuns a toda a população, e, ainda que os dados pessoais pertençam ao titular, as organizações os utilizavam livremente, de acordo com sua comodidade[1]. A Lei Geral de Proteção de Dados Pessoais (LGPD) foi instituída com o objetivo de organizar essa dinâmica, buscando devolver ao titular o controle do fluxo de seus dados. Dessa forma, é necessário que todos os titulares saibam quais são seus direitos, entendam a repercussão do compartilhamento de seus dados e passem a compreender os documentos de privacidade que as organizações utilizam para legitimar o tratamento desses dados.

A frase: "Os dados são o novo petróleo", cunhada pelo matemático e especialista em Ciência de Dados Clive Humby, ilustra o cenário atual da sociedade, em função da alavancada das empresas que têm nos dados a base de seu modelo de negócios, tornando-se as mais valiosas do mundo, ultrapassando grandes companhias sedimentadas nesse ranking. Além do mais, a frase faz o comparativo com o petróleo considerando seu necessário processo de refinamento para sua comercialização, assim como os dados que precisam ser tratados (refinados), usando inteligência humana ou artificial para transformá-los em produto ou serviço altamente rentável[2]. Os dados pessoais são comercializados como *commodities* pelas companhias, sendo fornecidos pelos próprios titulares, através de permissões de uso e compartilhamento obtidas

[1] A Lei Geral de Proteção de Dados Pessoais (LGPD) define "dado pessoal" como uma informação relacionada a pessoa natural identificada ou identificável. Contudo, sob o ponto de vista de tecnologia da informação, "dado" não se confunde com "informação". O "dado" é algo que pode ser físico, abstrato ou lógico, portanto, "dado", não tem contexto. Apenas a interpretação de um "dado" segundo uma metodologia específica revela uma determinada "informação", que depende, diretamente, da metodologia de análise e interpretação.

[2] Também são considerados como "o novo urânio", tendo em vista o enorme potencial de energia e valor, contudo, podem ser perigosos e prejudiciais se não forem manuseados com cuidado.

por meio de termos de uso e políticas de privacidade complexos, com linguagem técnica de difícil compreensão e muito extensos. Ou seja, não é garantida ao titular a informação de forma transparente, e, por essa dificuldade de leitura e compreensão, muitas empresas acabam se valendo de termos de difícil entendimento para coletar mais dados do que o necessário para a finalidade principal do usuário.

A inserção definitiva do homem na sociedade da informação evidenciou a necessidade de se estabelecer confiança nas relações, principalmente envolvendo dados pessoais. Os titulares de dados, como clientes e consumidores, em geral, quando mais experimentados nas novas tecnologias, não costumam confiar nas informações de privacidade apenas de textos jurídicos destinados a proteger a organização. Se antes não havia nenhuma – ou muito pouca – troca de dados para aquisição de produtos e serviços, como, por exemplo, assistir televisão, jogar *videogame* e até mesmo encontros amorosos, hoje todas essas atividades são monitoradas por algoritmos que processam nossos dados e nos geram preferência através da nossa própria conduta. Contudo, na maioria das vezes não se trata de um serviço de fidelização do usuário, porque esses mesmos dados são compartilhados, monetizados e utilizados para outras finalidades não informadas de maneira clara.

O *Legal Design* é uma metodologia voltada à democratização do direito, com foco no destinatário final, visando a uma maior compreensão e inclusão social. A aplicação do *Legal Design* nos avisos de privacidade, que é o instrumento pelo qual as organizações que utilizam dados pessoais informam os titulares sobre como será a forma de tratamento, utilização, compartilhamento, retenção, bem como os orienta sobre o canal adequado para que possam exercer seus direitos, pretende tornar os documentos de privacidade mais compreensíveis para todo usuário.

O *Legal Design* foi desenvolvido na Universidade de Stanford, na Califórnia, tendo como precursora a professora Margaret Hagan (2013), com o objetivo de colocar o destinatário das normas jurídicas no centro da resolução do problema. Esse método é desenvolvido através da intersecção do *Design*, da Tecnologia e do Direito. É necessária, para tal, uma mudança de conceito na forma de olhar os documentos de privacidade destinados aos titulares. A formalização de termos de uso e políticas de privacidade apenas para cumprir os requisitos da lei é insuficiente para fornecer a informação adequada.

Pesquisas indicam a relevância do tema considerando-se que, a cada nova tecnologia lançada no mercado, a adesão dos usuários é cada vez mais rápida. É possível que uma plataforma digital alcance mais de 50 milhões de usuários em menos de um mês, como foi o

caso do aplicativo *Pokémon Go*[3]. O imediatismo típico da geração dos nativos digitais impulsiona a adesão a essas plataformas quase que de forma automática. E isso pode gerar consequências financeiras, perda de autonomia, bem como desencadear crises emocionais de ansiedade, depressão e estresse. Nesse sentido, é necessário desonerar o titular de dados para uma escolha com maior autonomia sem, contudo, atribuir um grande ônus de conhecimento técnico.

Diante disso, surge o problema que esta pesquisa busca compreender: como o uso do *Legal Design* pode ser aplicado nos avisos de privacidade das plataformas digitais, para torná- los mais acessíveis, claros e eficazes na conscientização dos titulares, considerando as leis de proteção de dados pessoais? Os avisos de privacidade são os documentos que informam os usuários sobre como a organização tratará seus dados pessoais. Eles devem conter a forma de tratamento, a finalidade da coleta, a existência de compartilhamento, o prazo de retenção desses dados, além de imprimir o dever de estar aderente aos princípios da LGPD. Geralmente, esses documentos são de difícil compreensão, tendo em vista o uso de linguagem complexa, técnica e lacunosa, e não cumprem o papel de informar o titular de maneira transparente sobre o tratamento dos seus dados. Nesse sentido, é importante investigar o *Legal Design*, que é vocacionado a tornar o direito mais acessível, através de uma linguagem simples e de recursos visuais, aplicados nos avisos de privacidade, com o objetivo de aumentar sua efetividade de proteção dos dados dos titulares.

A justificativa desta dissertação está respaldada em três situações que ilustram bem a necessidade de se promover de forma efetiva a proteção de dados nos ambientes digitais. A primeira delas é a falsa ilusão de que a grande maioria dos serviços disponibilizados na internet é gratuita. Na verdade, ao acessar plataformas digitais, é coletada uma quantidade massiva de dados e não se tem a exata compreensão de como estes serão utilizados, com quem serão compartilhados e a delimitação da finalidade. Estamos diante do novo ditado: “Se você não paga pelo produto, o produto é você”. Assim, é necessário colocar luz na maneira como as companhias tratam os dados pessoais dos titulares.

A segunda justificativa apoia-se na análise dos documentos de privacidade disponibilizados aos usuários. Esses documentos exigem do titular alto grau de escolaridade e, mesmo assim, são construídos com termos técnicos ou em inglês que apenas especialistas no assunto são capazes de compreender. Não é incomum algumas plataformas inserirem bônus para o titular que ler e solicitar a recompensa, mas que sempre passa despercebido,

[3] DESJARDINS, 2018. Disponível em: https://www.visualcapitalist.com/how-long-does-it-take-to-hit-50-million-users/. Acesso em: 24 set. 2022.

considerando que a maioria das pessoas não leem esses documentos pela sua dificuldade de compreensão.

A terceira justificativa se respalda no aumento da aplicação de uma técnica chamada de *dark patterns*[4] ("padrões escuros", em tradução livre), que são ferramentas de *design* para enganar ou manipular os consumidores a fornecerem seus dados renunciando à proteção à privacidade. Mesmo diante de um cenário em que a coleta dos dados é massiva, modelos de negócio pautados em dados querem, cada vez mais, ter acesso aos dados pessoais. O surgimento dos padrões escuros é uma tentativa de driblar as leis da privacidade, persuadindo o titular a aderir a políticas de privacidade que autorizam a coleta e o compartilhamento em dissonância com a finalidade principal.

A lógica da aplicação do *Legal Design* nos avisos de privacidade visa, além da proteção dos direitos centrada no controle do titular, também ao uso responsável desses dados com inovação. Não se pretende obstar as organizações do uso dos dados pessoais, e sim permitir que o titular tenha clareza sobre como, onde e por quem seus dados são tratados, com a possibilidade de ingerência nesse tratamento e máxima transparência. A ideia é empoderar o usuário para equilibrar a relação com a organização.

O mundo globalizado tem proporcionado inúmeros avanços em todos os setores da humanidade, mas, também, existem desafios que devem ser enfrentados para que o avanço da tecnologia respeite o Estado Democrático de Direito. Além disso, a coleta e o armazenamento de dados pessoais cada vez mais acentuados podem ferir princípios e direitos fundamentais, sendo necessária a ampliação da tutela de tais direitos, para trazer maior proteção aos titulares de dados pessoais.

A partir desse cenário e buscando apresentar uma solução para o problema apresentado, tem-se como objetivos: (i) investigar se as políticas de privacidade estão aderentes à proteção de dados no ambiente digital, considerando as leis de privacidade existentes; (ii) analisar se o *Legal Design* poderá ser utilizado como um instrumento eficaz para efetivar os direitos dos titulares dentro dessas plataformas. Esse problema, contudo, não é fruto da LGPD e não é exclusivo da noção de privacidade, de forma que exige esforços multissetoriais, envolvendo outras áreas do Direito, como Direito Civil, Direito do Consumidor e Marco Civil da Internet (MCI) – em que pese a proposta desta dissertação, que é um recorte da LGPD (Lei nº 13.709/2018), considerando a proteção como direito fundamental e sua efetivação através do *Legal Design*.

[4] De acordo com pesquisa realizada pela Agência de Defesa do Consumidor da Noruega (*ForbrukerRadet*) e dos Estados Unidos (*Federal Trade Commission*).

Não basta que as leis de privacidade estabeleçam a promoção da transparência a respeito do tratamento de dados pessoais. Elas precisam garantir mecanismos eficazes para minimamente proporcionar autonomia ao titular a respeito da entrega dos seus dados pessoais. A utilização do *Legal Design* não significa a elaboração de documentos esteticamente bonitos. É necessário atribuir valor e funcionalidade, colocando o usuário no centro da solução. O Direito precisa repensar suas práticas, abrindo-se às novas contribuições de outras áreas do conhecimento, sob pena de não reconhecer seus institutos, crises e paradoxos, tendo em vista o incessante e imprevisível avanço da tecnologia.

Para compreensão do *Legal Design*, serão analisados seu conceito, método e aplicabilidade. Será abordado também o conceito de Linguagem Simples, criado pelo autor Rudolf Flesch[5], que é uma técnica de comunicação destinada à democratização da linguagem e compreende práticas para elaboração de textos fáceis de ler. Além disso, será analisado o procedimento da privacidade como padrão (*privacy by design)* como forma de instrumentalizar a estruturação de documentos de privacidade centrados no usuário.

Este estudo busca compreender o impacto da arquitetura de design dos documentos de privacidade no direito à proteção de dados. Será utilizada pesquisa bibliográfica e documental, partindo da premissa geral da efetivação da funcionalidade dos avisos de privacidade e questionando se o design pode contribuir para a concretização da proteção dos dados do titular. Segundo Rodrigues (2007), a pesquisa bibliográfica possibilita a recuperação de conhecimentos já sistematizados em determinada área. Além disso, Vergara (2016) aponta que materiais publicados em livros e trabalhos acadêmicos são capazes de sustentar pesquisas tendo como premissa o modo de acesso às fontes secundárias. A pesquisa bibliográfica possibilita um estudo mais amplo sobre o tema, pois se utiliza de uma grande quantidade de fenômenos, diferentemente da pesquisa realizada de maneira direta (GIL, 2008).

Nesse sentido, buscou-se efetuar pesquisas em portais de periódicos, bem como investigações relacionadas a leis, decretos e documentos que pudessem sustentar a discussão aqui proposta, além de exemplos práticos da aplicação do *Legal Design* em documentos de privacidade. Foram analisados os avisos de privacidade da Skol; L'Oreal; Sanofi e PlayStation, com aplicação das técnicas de *Legal Design* para destacar a forma de comunicação mais empática e assertiva centrado no usuário.

[5] O livro *The art of plain talk* (A arte de falar com clareza), de 1946, divulgava os conceitos de inteligibilidade que o autor havia desenvolvido na pós-graduação em Biblioteconomia na Universidade de Columbia (FISCHER, 2018, p. 21).

2 A SOCIEDADE DA INFORMAÇÃO E A PROTEÇÃO DE DADOS

A sociedade tem experimentado um crescimento exponencial de acesso às inovações em tecnologia. Fenômenos como a globalização, a revolução tecnológica e a invenção da internet fizeram o planeta dar um salto quântico rumo à modernidade. Isso gerou um processo global de transformação digital para oferta de produtos e serviços e, consequentemente, a substituição do atendimento pessoalizado por canais on-line (FISCHER, 2018).

A privacidade pode ser identificada em diferentes épocas da sociedade, contudo, sua noção, conforme é conhecida hoje, começou a ser melhor estruturada a partir do século XIX e apenas recentemente assume a esfera de direito fundamental, conforme exposto pelo professor Doneda (2021, p. 30):

> Praticamente não havia lugar para a tutela jurídica da privacidade em sociedades nas quais as condutas humanas estavam condicionadas a outra ordem de mecanismos – fosse uma rígida hierarquia social ou então uma determinada arquitetura dos espaços públicos e privados; fosse porque eventuais pretensões a esse respeito fossem neutralizadas por um ordenamento jurídico de caráter corporativo e patrimonialista; fosse, então, em determinadas sociedades nas quais a privacidade representasse não mais que um sentimento subjetivo que não poderia nem deveria ser tutelado. O despertar do direito para a privacidade ocorreu justamente num período em que muda a percepção da pessoa humana pelo ordenamento e ao qual se seguiu a juridificação de vários aspectos de sua vida cotidiana. A moderna doutrina do direito à privacidade, cujo início podemos considerar como sendo o célebre artigo de Brandeis e Warren, The right to privacy, apresenta uma clara linha evolutiva. Em seus primórdios, marcada por um individualismo exacerbado e até mesmo egoísta, portava a feição do direito a ser deixado só. A esse período remonta o paradigma da privacidade como uma zero-relationship, pelo qual representaria, no limite, a ausência de comunicação entre uma pessoa e as demais. Essa concepção foi o marco inicial posteriormente temperado por uma crescente consciência de que a privacidade seria um aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade.

Inobstante tenham advindo marcos legais regulamentadores da proteção de dados, no Direito do Consumidor essa é uma vertente que tem início mais cedo, com o surgimento dos bancos de dados de cadastro de consumo. No Brasil, não muito tempo atrás, não havia qualquer disciplina jurídica que tratasse dos arquivos de consumo. Como resultado, muitos abusos graves, frequentes e indevidos eram cometidos na busca de informações para assegurar que o consumidor era idôneo e adimplia suas obrigações (BENJAMIN, 2019, p. 556).

O consumo a crédito, na primeira metade da década de 1950, era demorado, caro e complicado. As empresas necessitavam de infraestrutura própria para parcelamento, cadastramento e investigação. Quem necessitava de crédito “precisava preencher minucioso cadastro, não só com seus dados pessoais, mas indicando ainda os locais onde habitualmente

adquiria produtos e serviços, como o armazém, a alfaiataria e, em especial, outros estabelecimentos onde já comprara a prazo" (BENJAMIN, 2019, p. 558).

As empresas investigavam os clientes e mantinham arquivados seus cadastros para repassar informações umas às outras, especialmente os grandes magazines, que, mais estruturados, eram procurados para informar dados dos consumidores. Foi isso que deu ensejo aos Serviços de Proteção ao Crédito (SPCs) e, desdobrando-se deles, aos demais bancos de gerenciamento de dados de consumidores.

Entretanto, o advento da internet e das novas tecnologias da informação amplificou essa realidade. Da manutenção de dados manuais pelos grandes magazines, que os vendiam às lojas menores, desencadeou-se uma circunstância em que nossos dados são captados diuturnamente por empresas que se situam em relações de consumo. É o exemplo dos *marketplaces* e das financeiras e empresas gerenciadoras de banco de dados de clientes.

Aliada a esse avanço e à dinamicidade da mudança na forma de comunicação, com a chegada da quarta revolução industrial (SCHWAB, 2016), surge uma série de leis envolvendo proteção de dados, exigindo políticas de privacidade claras e transparentes quanto aos dados pessoais tratados (EUROPEAN COMISSION, 2018).

> Por que a privacidade é tão importante? Instintivamente, todos nós entendemos por que a privacidade é tão essencial para nossos "eus" individuais. Até mesmo para aqueles que afirmam que não dão tanto valor à privacidade nem têm nada a esconder, fazemos e dizemos muitas coisas que não queremos que ninguém mais saiba. Há um número abundante de pesquisas que mostram que quando alguém sabe que está sendo observado, seu comportamento torna-se mais conformista e complacente (SCHWAB, 2016).

O ponto de partida para a discussão envolvendo uma lei federal refere-se ao recenseamento da população alemã e se deu frente ao processamento eletrônico de dados, que viabilizaria tanto o processamento quanto o armazenamento e a transmissão ilimitada de dados. De acordo com o tribunal, o processamento automatizado dos dados ameaçaria o poder do indivíduo de decidir por si mesmo se e como ele desejaria fornecer a terceiros as suas informações pessoais, considerando que o processamento de dados possibilitaria a elaboração de um "perfil completo da personalidade" por meio de "sistemas automatizados integrados sem que o interessado pudesse controlar de forma suficiente sua correção e utilização" (DONEDA; SARLET; MENDES, 2021, p. 36).

A primeira legislação internacional reconhecida propriamente como proteção de dados foi a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares, que determina princípios com o objetivo de garantir a todas as pessoas o respeito pelos seus direitos

e liberdades fundamentais, especialmente o direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal.

Posteriormente, foi aprovada a Diretiva 95/46, que estabeleceu para as empresas obrigações relativas ao tratamento de dados pessoais, ou seja, dados que podem tornar o seu possuidor identificado ou identificável, além de exigir que todo país da União Europeia tenha um órgão de proteção de dados que supervisione a aplicação dos princípios e das leis de proteção à privacidade individual (MENDES, 2014). Mais recentemente, foi criada a *General Data Protection Regulation* (GDPR, em português, *Regulamento Geral sobre a Proteção de Dados*), que impõe obrigações a todas as empresas ou pessoas físicas que tratem dados pessoais com fins econômicos.

A GDPR estabelece que esses dados sejam tratados dentro da expectativa do titular, com o objetivo principal de oferecer ao usuário maior controle e transparência sobre as informações pessoais armazenadas em bancos de dados.

No âmbito nacional, houve um maior fomento ao debate acerca da proteção de dados nos últimos dez anos. Nossa regulamentação era feita de forma esparsa e carecia de uniformidade e segurança jurídica. O avanço da tutela de privacidade não é proporcional diante dos desafios dos novos tempos, que se mostram avassaladores. A construção desse direito foi feita pelo ordenamento jurídico associado a liberdades individuais. Nesse sentido,

> Entre esses diversos institutos e matérias entre os quais, por muito tempo, a proteção de dados no Brasil foi associada, a mais relevante é o direito à privacidade – como também pela forte ressonância entre os dois institutos. A bem da verdade, até hoje se observa, coloquialmente ou mesmo em literatura especializada, uma certa ambivalência na utilização dos conceitos de privacidade e proteção de dados. Para o que nos interessa, essa ambivalência faz inclusive as vezes de elemento de continuidade entre uma tradição jurídica que reconheceu, regulou e atualizou o direito à privacidade até chegar às portas de um marco regulatório específico para a proteção de dados pessoais. Dessa forma, uma parte dominante dos temas de proteção de dados no Brasil pode ser lida à luz dessa evolução do direito à privacidade e sua aplicação em situações específicas. A assimilação da proteção à privacidade pelo direito brasileiro é, de modo geral, linear com a sua progressiva consolidação como um dos direitos da personalidade pela doutrina e jurisprudência, até a sua previsão constitucional e sua menção específica no Código Civil de 2002, no art. 21. O efetivo desenvolvimento e aplicação desse direito, no entanto, não chegaram a formular um arcabouço capaz de fazer frente às novas situações e questões que surgiriam com a introdução de novas tecnologias (DONEDA; MENDES; CUEVA, 2020, p. 30).

O Marco Civil da Internet, que foi o primeiro instrumento que de fato teve como objetivo fiscalizar as questões relacionadas à manipulação de dados, e, mais recentemente, a Lei Geral de Proteção de Dados Pessoais (LGPD), que aborda de modo específico a forma como deve ser feito o tratamento de dados pessoais, não apenas por pessoa física mas também por pessoa jurídica, abrangendo inclusive os meios digitais, têm como objetivo a proteção de direitos

fundamentais como o direito à liberdade e o direito à privacidade de cada um dos indivíduos, buscando promover uma maior segurança em relação ao público.

A criação dessas leis está em consonância com vários países do mundo, que já contam com uma legislação específica há tempos, sendo que leis como a *General Data Protection Regulation* (GDPR), da Europa, está em vigor desde 2018, e a *Children's Online Privacy Protection Rule* (COPPA), nos Estados Unidos, desde 1998.

A criação de regramentos como a Lei do Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, além de equiparar o Brasil aos outros países no combate a delitos no ciberespaço, ainda viabiliza melhor diálogo e interação entre o Direito e as novas tecnologias, sobretudo as que envolvem o ciberespaço e a mídia digital.

> Em 2014, o Marco Civil da Internet entrou em vigor no Brasil, estabelecendo princípios, garantias, direitos e deveres para o uso da Internet no país. Foi uma forma de reconhecer e regulamentar as novas relações jurídico-virtuais, em razão da existência de inúmeros usuários e provedores, bem como de empresas que trabalham online, dado que grande parte não estava adaptada à nova realidade digital. O MCI trata dos delitos praticados online (crimes cibernéticos) e da neutralidade da rede, estabelecendo direitos e garantias para liberdade de expressão, e, apesar de cuidar da privacidade, acabou restando uma lacuna sobre o tratamento de dados pessoais, pois não foi dada a devida atenção ao seu uso, destino, comercialização, etc. (SOUZA, 2018).

A LGPD foi publicada em 14 de agosto de 2018 e entrou em vigor em 18 de setembro de 2020, e uma de suas principais missões é apropriar as pessoas naturais de seus dados pessoais. A lei tem como um de seus fundamentos a autodeterminação informativa, ou seja, o controle que o próprio titular deve ter quanto ao trânsito de seus dados pessoais. Dessa forma, portanto, o titular dos dados pessoais pode solicitar informações sobre seus dados à organização que os detém.

O art. 2º, II da LGPD estabelece como um dos seus fundamentos a autodeterminação informativa de origem alemã. Sua construção baseou-se na interpretação de um único artigo da Lei Fundamental da Alemanha, que garante que todos têm direito ao livre desenvolvimento de sua personalidade (SARLET, 2021, p. 13). O caráter abstrato do direito da personalidade geral possibilita sua aplicação a novas formas para garantir proteção suficiente para o indivíduo (SARLET, 2021, p. 34). O Tribunal Constitucional Alemão também faz uma abordagem quanto ao processamento não transparente dos dados pessoais dentro da autodeterminação informativa, em uma interpretação conjugada com a dignidade da pessoa humana.

O que se observa na década atual é uma clara demonstração de que em nenhum outro momento da história houve tantas inovações ou o mundo cresceu de forma tão rápida. Alguns fenômenos podem auxiliar na explicação a respeito desse desenvolvimento tão acelerado, como

a própria globalização, a revolução da tecnologia e a invenção do conceito de internet, que foram questões determinantes para que de fato entrássemos na Idade Moderna. Neste sentido, Klaus Schwab, criador do conceito da Quarta Revolução Industrial, alerta sobre os impactos da tecnologia sobre nosso modo de vida.

> A quarta revolução industrial não está mudando apenas o que fazemos, mas também quem somos. O impacto sobre nós como indivíduos é múltiplo, afetando nossa identidade e as muitas facetas relacionadas a ela – nosso senso de privacidade, nossas noções de propriedade, nossos padrões de consumo, o tempo que dedicamos ao trabalho e ao lazer, a forma de desenvolvermos nossas carreiras e cultivarmos nossas competências (SCHWAB, 2016, p. 127).

Assim, o mundo passa por uma constante ampliação de informações, que possibilita uma facilidade de acesso a dados que deveriam ser privados e que somente dizem respeito ao indivíduo. Consequentemente, começa a existir a necessidade de criação de mecanismos para não apenas coibir as questões de abuso relacionadas à manipulação desses dados, mas também regular o excesso de sua utilização, mesmo por empresas que tratem dados pessoais.

Pesquisa desenvolvida pelo site *Visual Capitalist* (DESJARDINS, 2018) mostrou o tempo que a sociedade levou para chegar a 50 milhões de usuários em cada tecnologia inovadora. O estudo revelou que, para companhias aéreas, automóveis e telefone, foram mais de 50 anos. No caso de cartões de crédito e televisão, levou-se entre 20 e 30 anos. Computadores, celulares e internet, entre sete e 14 anos. Já para as tecnologias mais recentes, o tempo é vertiginosamente menor. O Facebook demorou quatro anos para atingir 50 milhões de usuários, ao passo que o WeChat levou um ano e o aplicativo Pokémon Go, apenas 19 dias, ou seja, mais de dois milhões e seiscentos mil usuários por dia.

Se, por um lado, a economia moderna apresenta cada vez mais ferramentas para propiciar uma nova experiência imersiva, por outro, cresce uma demanda de consumidores mais exigentes e preocupados com os impactos dessas ferramentas e sua segurança (SERAFINO; CARDOSO, 2022).

A proteção dada pela lei surge dentro de um contexto de garantia em relação a todas as informações que possam ser coletadas, mesmo que com autorização do usuário, visto que ele deve ter consciência dessa coleta e acesso à sua finalidade. A importância da LGPD foi reconhecida pela Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que incluiu o direito à proteção de dados pessoais no rol dos direitos e garantias individuais, assegurado no artigo 5º, LXXIX, da Constituição Federal do Brasil (MORAES, 2022).

Portanto, a privacidade se apresenta como uma liberdade negativa, ou seja, ela é estática no sentido de não sofrer interferência alheia. Já a proteção de dados é uma liberdade positiva, sendo dinâmica no sentido de atingir a privacidade.

O direito à proteção de dados pessoais se estabelece como um direito fundamental, não apenas nos ordenamentos nacionais, mas também em textos internacionais, como a antiga Diretiva 95/46/CE sobre proteção de dados pessoais na União Europeia, que coloca como um de seus objetivos principais o tratamento de dados pessoais, e, posteriormente, a própria Carta de Direitos Fundamentais da União Europeia, de 2000, que traz uma seção exclusiva para a proteção de dados pessoais (SOUZA, 2018).

> Além dos aspectos relacionados à segurança e à legislação supracitados, é importante ressaltar que as possíveis soluções para as implicações bioéticas emergentes com uso da internet perpassam pela conscientização de todos os envolvidos, sejam usuários ou administradores dos servidores de internet, da importância da privacidade, bem como do consentimento das pessoas para coleta e uso de dados (SILVA BARBOSA *et al*., 2014, p. 112).

Nessa vertente, consideram-se a proteção dos direitos da personalidade que decorre da constitucionalização dos direitos civis e a consequente previsão desses direitos, que têm íntima relação com os direitos fundamentais. Assim, o Código Civil resguarda o direito à integridade psicofísica (arts. 13 a 15), o direito ao nome e ao pseudônimo (arts. 16 a 19), o direito à imagem (art. 20) e o direito à privacidade (art. 21).

Nota-se que, como decorrente dos direitos fundamentais constitucionalmente assentados, o direito protege a personalidade humana e o potencial violador, por meio da manutenção de cadastros e bancos de dados, especialmente no que se refere aos eixos do direito ao nome, à imagem e à privacidade, o que se impõe que sejam respeitados no plano concreto. Portanto, está alinhado com outras previsões do ordenamento, como o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais e a própria Constituição Federal. No que se refere à proteção da personalidade, portanto:

> Questionando a natureza do direito da personalidade, surgem as teorias monistas e as tipificadoras. Enquanto aquelas defendem a unidade da personalidade humana, estas irradiam várias facetas como o direito ao nome, o direito à imagem, o direito do consumidor etc. Deve-se salientar, antes de tudo, que é necessária uma unidade de propósito, o que levou a maioria da doutrina e jurisprudência brasileira a recorrer ao princípio da dignidade da pessoa humana como principal fundamento de um direito geral da personalidade no ordenamento jurídico. É interessante pontuar que, relacionado a esse direito geral de personalidade, tanto aqui quanto em diversos países, também está o chamado direito fundamental à privacidade (NASCIMENTO, 2017, p. 265).

Outro importante tema diz respeito à proteção da personalidade humana, que ganha, assim, novo impulso após a Segunda Grande Guerra, momento em que passa a ter como lastro fundamentador a garantia à dignidade humana. Essa proteção abarca a da personalidade, especialmente nas atuais sociedades, uma vez que a pluralidade humana torna o enquadramento de subjetividades um movimento de difícil equalização.

Os direitos da personalidade são a face civilística da proteção à dignidade subjetiva. São, portanto, direitos individuais que, se violados, fazem nascer um direito à indenização. Nesse sentido, o Código Civil positiva uma série de conceitos tidos como direito da personalidade, que não se encerram no texto legal, mas abarcam ainda situações que o completam.

Esses direitos da personalidade são, portanto, direitos subjetivos privados, inatos e vitalícios, que têm como objeto de tutela as manifestações interiores da pessoa, não podendo ser disponibilizados de forma absoluta ou relativa. Dentre eles encontramos o direito à privacidade.

Privacidade refere-se a algo íntimo e pessoal, cujo conhecimento público e privado mantém-se na esfera de controle do próprio destinatário do direito. Não é, no entanto, um conceito de fácil apreensão, existindo controvérsias quanto a seus exatos termos e alcance.

> Assim, resultaram consideráveis divergências de concepção sobre o que seria privacidade. Para evidenciar o problema, lembrem-se os termos inseridos no conceito de direito à privacidade: garantir a ilicitude da publicação de imagens sem consentimento, o direito de abortar ou a inviolabilidade de domicílio. É possível observar que tais exemplos insinuam certa manipulação pelo próprio ordenamento (NASCIMENTO, 2017, p. 272).

Nota-se que a construção do conceito de privacidade remonta à dicotomia público-privado, partindo de concepções do que poderia ser relegado à esfera pública e o que mereceria ser protegido pelo Estado, e da possibilidade de o indivíduo manter informações no âmbito privado, ou seja, em sigilo, mediante seu próprio controle. É uma garantia da não invasão de aspectos privativos do indivíduo (COSTA; OLIVEIRA, 2019).

> Nesse cenário, a privacidade caminhou da sequência “pessoa-informação-sigilo” para “pessoa-informação-circulação-controle” (RODOTÀ, 2008, p. 93). A ideia tradicional de privacidade deve relacionar-se com as novas dimensões contemporâneas que perpassam a esfera privada e as informações pessoais. Isso não significa, contudo, que a proteção de dados pessoais é uma simples extensão do processo evolutivo do conceito de privacidade. Ao contrário, indica que ela se estabelece como um direito autônomo, que necessita de clareza e especificidade normativa, pois, mesmo que a proteção de dados esteja relacionada, em alguns aspectos, à tutela da privacidade dos indivíduos, ela não está restrita à dicotomia do público e do privado (COSTA; OLIVEIRA, 2019, p. 29).

Constitui-se, assim, em uma liberdade negativa do titular que, com o passar dos anos, adquiriu forma de guarda-chuva, abrigando inúmeras ações. Nas sociedades hipercomplexas e elevadamente globalizadas, a concepção de ter controle sobre o uso de dados pessoais está abarcada entre as condutas que são cobertas pelo manto da privacidade.

Dessa forma, portanto, os dados pessoais, à medida que identificam ou tornam identificável o indivíduo, devem ser considerados como extensão da sua personalidade (DONEDA, 2021), sobretudo na sociedade cada vez mais digital em que estamos inseridos, na qual essas informações se tornaram insumo de grande valor (SANTOS, 2021).

A lei trata, como dados pessoais, a definição constante do art. 5º e seus incisos, que estabelece o que podem ser considerados dados pessoais e traz uma série de hipóteses, inclusive sobre os dados sensíveis e os chamados dados anonimizados. O legislador dividiu a definição de dados pessoais em: dados pessoais e dados pessoais sensíveis. Essa divisão permite que os dados pessoais recebam tratamento diferenciado, conforme suas características particulares e as características dos dados pessoais a serem tratados, de forma a promover de fato a proteção à privacidade do indivíduo. Nesse sentido foi o parecer do Senador Ricardo Ferraço, responsável pela condução dos projetos de lei que formam hoje a LGPD:

> A proteção de dados pessoais diz respeito, na verdade, à forma como empresas e governos podem nos oferecer bens e serviços com base no processamento de nossos dados pessoais que lhes informem, por exemplo, não somente nossa identidade, mas ainda nossos hábitos pessoais, nosso consumo sobre produtos e serviços, nosso comportamento, opinião política ou filosófica, orientação sexual, preferências gastronômicas, artísticas ou culturais etc (BRASIL, 2018).

Dado pessoal, portanto, segundo a definição da Lei nº 13.709/2018, é toda informação pessoal, podendo ser ainda sensível – quando seu conteúdo tratar de convicções pessoais, como as de política e religião, orientação sexual, raça e etnia –, e por isso receber um tratamento especial dessa legislação. *Dado anonimizado*, por sua vez, é aquele dado do qual não é possível conhecer seu titular, pois não contém quaisquer elementos de identificação, ou tais elementos encontram-se encriptados.

Embora de fácil assimilação, o conceito de dado pessoal não é tão simples, posto que, na prática, as novas tecnologias apresentam cenários cada vez mais complexos e delicados a respeito do assunto.

> Definitivamente, vive-se num tempo em que a simultaneidade proporcionada pela internet oportuniza a vivência de uma experiência revolucionária da comunicação, do relacionamento social e do consumo. Diante disso, é inegável que as relações estabelecidas no ambiente virtual carecem de análise da ciência jurídica sob os prismas sociológico, hermenêutico, jurisdicional e do *modus operandi* que a tecnologia instiga a investigar (BOFF; FORTES, 2014, p. 111).

Tem-se ainda que os dados privados podem ser tornados públicos, tanto por iniciativa de seu titular como por obrigação legal. Diante disso, torna-se indiferente a iniciativa ou o consentimento do titular, pois é de interesse público o acesso às informações, e o interesse público, como é sabido, sempre prevalecerá sobre o interesse privado – nesse caso, o direito à privacidade.

Esses são os casos de criação, por parte da administração pública, de políticas públicas em que o interesse coletivo se torna mais relevante que os interesses individuais, como o de privacidade.

No contexto da sociedade da informação, a tecnologia e as ferramentas de marketing progridem de forma muito acelerada, comprometendo o desenvolvimento dos benefícios e aumentando o desafio da tutela dos direitos fundamentais.

Assegurar diretrizes básicas para o uso da internet e dos dados pessoais no mundo digital para o uso da rede em território nacional tornou-se imprescindível. Com as duas leis anteriormente referidas e a chancela constitucional da proteção de dados, a tutela do Estado se fez integralmente presente, e o marco zero da internet e da proteção e tratamento de dados é atualmente uma realidade no Brasil.

2.1 **A proteção de dados para consumidores, idosos, crianças e adolescentes**

O Direito do Consumidor também desenvolve importante papel na sociedade da informação, principalmente na economia de dados, em que a atuação da Secretaria Nacional dos Consumidores (Senacon), em conjunto com a Autoridade Nacional de Proteção de Dados (ANPD), tende a trazer resultados positivos para garantir que fornecedores atuem com mais transparência. Não só as leis de privacidade devem atuar para que a sociedade seja mais consciente quanto ao uso e compartilhamento de dados pessoais.

No caso do direito do consumidor, os princípios regentes da área são todos aplicáveis à circunstância da proteção de dados, porém, dá-se especial relevo ao princípio da proteção da transparência e confiança. Este decorre da boa-fé objetiva e está previsto no Código de Defesa do Consumidor (CDC), em seu art. 4°, inciso III, sendo um dos princípios basilares. Afirma que o direito do consumidor se preocupa com o plano dos fatos, de forma objetiva, analisando as regras de conduta para concluir se os sujeitos da relação jurídica de consumo atuaram ou não com boa-fé (NUNES, 2018).

Não somente os fornecedores devem atuar com boa-fé, como os próprios consumidores, ou seja, o princípio previsto no Diploma Consumerista vale para ambos os lados da relação. A boa-fé objetiva tem três funções: função integrativa, pois garante direitos e deveres que integram o contrato, mesmo que não estejam dispostos em suas cláusulas, como os deveres de lealdade, de cuidado, de informação; função interpretativa, pois proíbe a interpretação dos contratos de forma maliciosa e prejudicial a uma das partes; e função de controle (CAVALIERI FILHO, 2019).

> Além disso, há princípios do Código de Defesa do Consumidor que também são similares e aplicáveis aos avisos de privacidade no momento de coleta do consentimento, como a transparência (art. 4°, caput), liberdade de escolha (art. 6°, II), informação adequada e clara (art. 6°, III) e proibição de cláusulas abusivas ou impostas (art. 6°, IV). Aplicam-se, ainda, a obrigação de assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa (art. 31, caput), a exigência de termos claros e com caracteres ostensivos e legíveis (art. 54, § 3°) e o requisito de redação com destaque, permitindo a imediata e fácil compreensão do consumidor quando houver a limitação de seus direitos (art. 54, § 4°) (FERREIRA; CABELLA, 2020).

As partes devem agir com lealdade e confiança recíprocas. Essa expectativa de um comportamento adequado por parte do outro é um componente indispensável não só nas relações de consumo, mas na sociedade da informação. A boa-fé, em sua função de controle, estabelece um limite a ser respeitado no exercício de todo e qualquer direito subjetivo (VIEIRA, 2020).

O respeito à confiança tornou-se, assim, um princípio geral, prevalecendo em todas as áreas do Direito. Exatamente por isso, o sistema de proteção ao consumidor foi desenhado com a previsão de leis cogentes, que servirão para a proteção da confiança depositada no fornecedor, na segurança do produto e do serviço disponibilizado a ele.

O princípio da confiança é decorrente da boa-fé, com sua face subjetiva, e com estreita ligação com o princípio da transparência. É a expectativa que vem da boa-fé que resulta em confiar. “Confiança é a credibilidade que o consumidor deposita no produto ou no vínculo contratual como instrumento adequado para alcançar os fins que razoavelmente deles se espera. Prestigia as legítimas expectativas do consumidor no contrato” (CAVALIERI FILHO, 2019, p. 67).

Ao lado da proteção da confiança, cabe destacar o princípio da vulnerabilidade, que se encontra consubstanciado no art. 4º, I, do Código de Defesa do Consumidor, e reconhece o consumidor como a parte mais vulnerável no mercado de consumo. A importância do referido princípio reside na constatação de que a relação de consumo é extremamente desigual, sendo

indispensável a busca de instrumentos jurídicos capazes de tentar reequilibrar a relação entre consumidor e fornecedor de forma a torná-la mais justa.

Além disso, apesar de o direito ser o mesmo para todos, nem sempre é possível exercê- lo de forma semelhante e em condições de igualdade ao próximo. É necessário, para isso, que sejam criadas tais condições de igualdade, de forma a atender àqueles que se encontram em situação de inferioridade, carência e menor proteção. Nesse sentido, a professora Laura Schertel Mendes, antes da vigência da LGPD, já pensava em formas de proteção dos dados dos consumidores através do CDC:

> Sob as condições de uma economia da informação, em que os dados pessoais dos consumidores são processados pelos mais diversos setores econômicos a partir de tecnologias cada vez mais avançadas, ampliando os riscos à personalidade do consumidor, é de se questionar como se efetiva esse dever de proteção estatal na atualidade. Isto é, como devemos interpretar o Código de Defesa do Consumidor de modo a manter vivos e atuais os seus preceitos normativos e concretizar o mandamento constitucional de proteção da parte mais fraca das relações de consumo? (MENDES, 2014).

A vulnerabilidade do consumidor, quando se trata de pessoa física, é absoluta, ou seja, fica presumida a sua posição inferior em relação ao fornecedor, não sendo necessária qualquer demonstração ou comprovação de desequilíbrio nas relações estabelecidas entre uma parte e outra. Entretanto, quando se tratar de consumidor que é pessoa jurídica ou profissional, é necessário que tal desequilíbrio na relação seja comprovado para que as regras presentes no CDC possam atingir tais pessoas nas suas relações de consumo (BENJAMIN; MARQUES; BESSA, 2016).

Uma diferença importante para se abordar é aquela entre os conceitos de vulnerabilidade e hipossuficiência, que podem se confundir. Apesar de ambos estarem intimamente ligados à fraqueza do consumidor, eles não são sinônimos. A vulnerabilidade é um fenômeno de direito material e possui presunção absoluta, enquanto a hipossuficiência é um fenômeno de direito processual e possui presunção relativa.

A vulnerabilidade do consumidor se apresenta de várias formas na relação de consumo. De acordo com a doutrina, ela se divide em: técnica, jurídica/científica, fática/socioeconômica e informacional. Quando consiste na fragilidade do consumidor no que diz respeito à falta de conhecimentos técnicos sobre determinado produto ou serviço adquirido ou contratado no mercado de consumo, é denominada vulnerabilidade técnica. Nesse caso, o fornecedor, como detentor do monopólio dos meios de produção, é o único conhecedor da matéria-prima ou do produto utilizado na confecção de determinado bem (MIRAGEM, 2016).

Quando a vulnerabilidade for jurídica ou científica, dizer-se-á que falta ao consumidor conhecimento sobre a matéria jurídica ou a respeito de outros campos científicos, como economia ou contabilidade. A vulnerabilidade jurídica ou científica tem presunção relativa, pois, quando o consumidor é pessoa jurídica ou profissional, presume-se que tenha entendimento científico sobre determinado produto, departamento jurídico, para tratar de certos assuntos ou profissional da área contratado para auxiliá-lo (TARTUCE; NEVES, 2021).

Em se tratando de vulnerabilidade fática ou socioeconômica, a fragilidade do consumidor se dá no quesito econômico. Trata-se de uma espécie ampla, genérica, de uma modalidade aberta, capaz de albergar várias situações nas quais o consumidor mais humilde se deixa influenciar pelo vendedor, o qual o manipula por meio de conversa enganosa. Isso ocorre, por exemplo, no caso de vendedor que induz o cliente a comprar uma joia mais cara, por significar que seria a melhor da loja.

Nesse sentido:

> O direito do consumidor, e a premissa da qual esta parte, de desigualdade fática entre consumidor e fornecedor, impõe então que em matéria de responsabilidade civil decorrente das relações de consumo, adote-se o critério da responsabilidade objetiva, independente da demonstração de culpa. A finalidade é contemplar situações nas quais, em face da vulnerabilidade do consumidor e da ausência de conhecimento sobre a atividade de fornecimento de produtos e serviços, o fornecedor, expert em sua atividade profissional habitual, e que dá causa ao risco em razão da atividade econômica que desenvolve, responda pelos danos que dela sejam decorrentes (MIRAGEM, 2016).

Há ainda a vulnerabilidade informacional. Parte da doutrina defende esse tipo de vulnerabilidade como sendo um subtipo da vulnerabilidade fática (ou socioeconômica), pois ela se dá devido à grande quantidade de informações que circulam nos dias de hoje, tanto em razão dos meios de comunicação quanto da publicidade, e que acabam confundindo o consumidor.

O art. 6º, inciso III, do CDC, estabelece que a informação adequada e clara é um direito básico do consumidor. Esse direito está intimamente relacionado ao previsto no inciso II do mesmo artigo: “a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações”. O direito à informação e à educação não é limitado apenas a alertar os consumidores, mas também a possibilitar ao consumidor liberdade de escolha e contratação.

No momento em que acessa as plataformas digitais, o consumidor acaba por adotar uma posição mais passiva, na qual recebe a informação, mas é incapaz de atestá-la como verdadeira ou falsa, não conseguindo determinar as qualidades ou os defeitos de determinado produto ou

serviço. Diante disso, a liberdade do consumidor fica suprimida, isto é, ele deixa de ter uma opinião própria, sendo manipulado pelo fornecedor, detentor exclusivo das informações, o que torna necessária uma maior proteção pelo direito do consumidor, evidentemente fragilizado. Neste sentido, Bruno Bioni analisa a vulnerabilidade sob a ótica da proteção de dados:

> É certo que há uma assimetria e (hiper)vulnerabilidade no âmbito da proteção dos dados pessoais, pois o cidadão, em meio ao mercado informacional, deve ser identificado como um sujeito vulnerável que não tem condições de discernir com absoluta clareza todos os efeitos colaterais relativos ao tratamento de suas informações pessoais (BIONI, 2020, p. 155).

Ou seja, avisos de privacidade que buscam orientar o consumidor a tomar uma decisão consciente e informada sobre a disposição dos seus dados. Assim, quando sua ação não necessariamente condiz com sua vontade, haverá também violação ao CDC, o que, além da dissonância com os princípios citados, também poderá ser categorizado como publicidade enganosa. Os avisos de privacidade informam aos titulares (consumidores) como suas informações serão processadas pela organização, de forma que devem ser claros e de fácil compreensão.

No artigo intitulado “Escrevendo e implantando os avisos de privacidade (privacy notices) na coleta do consentimento válido”, Raissa Ferreira e Daniela Cabella defendem: “Somente com o fácil acesso, total transparência e liberdade é que o titular de dados terá, de fato, pleno controle sobre o uso de seus dados pessoais, conforme determina o item nº 7 do preâmbulo do GDPR: As pessoas [físicas] deverão poder controlar a utilização que é feita dos seus dados pessoais” (FERREIRA, CABELLA, 2020, p. 138).

Complementando, o princípio da harmonia nas relações de consumo está previsto no artigo 4º, inciso III, do CDC, e tem como principal objetivo a compatibilização entre os interesses dos participantes das relações de consumo e também entre a proteção do consumidor e a necessidade de desenvolvimento econômico e tecnológico. Em relação a esse objetivo, o desenvolvimento tecnológico deverá ser feito de maneira harmoniosa, satisfazendo tanto o consumidor quanto o fornecedor (TARTUCE; NEVES, 2021). A tecnologia não deve prejudicar aquele que é mais frágil, porém, ao mesmo tempo, a proteção não pode atrapalhar o desenvolvimento tecnológico.

Por fim, o princípio da proteção ao consumidor, segundo Bessa (2006), está relacionado com a responsabilidade objetiva, em conjunto com a inversão do ônus da prova. Isso se dá porque todos os princípios que compõem a base do CDC têm como objetivo em comum a proteção do consumidor, que é a parte hipossuficiente, dentro das relações de consumo.

A LGPD buscou centralizar toda a matéria referente a proteção de dados no mesmo dispositivo legal, contudo, este tema é permeável por muitas outras leis, como visto, o CDC, bem como o Estatuto do Idoso e Estatuto das Crianças e Adolescentes. Cada uma dessas leis regula, de maneira específica, as peculiaridades de cada tipo de indivíduo e visa assegurar, sobretudo, todos os seus direitos de forma digna.

Em relação as crianças e adolescentes, a LGPD estabelece algumas regras específicas para equilibrar a relação desses titulares, que ainda estão em fase de desenvolvimento, com os agentes de tratamento. O art. 14 da LGPD estabelece que todo o tratamento de dados de crianças e adolescente deverá ser realizado, sempre, no seu melhor interesse. A definição de criança é estabelecida no art. 2º do ECA, sendo a pessoa de até doze anos de idade incompletos e, quanto aos adolescentes, entre doze e dezoito anos de idade incompletos.

Nos termos do art. 14, §1º da LGPD, a princípio, apenas o consentimento dos pais ou responsável autorizaria o tratamento de dados das crianças. Contudo, este tema poderá ser regulamentado pela Autoridade Nacional de Proteção de Dados, considerando que outras bases legais poderão ser utilizadas para satisfazer o melhor interesse da criança. Já em relação a adolescentes, não existe a obrigatoriedade do uso do consentimento, contando que o tratamento de dados seja realizado para o seu melhor interesse.

A intenção é equilibrar essa relação, considerando a ausência de conhecimento sobre as consequências do uso de seus dados. Dessa forma, o §6º do art. 14, que para este grupo de titulares, existe um reforço para que as informações sejam fornecidas de maneira simples, clara e acessível, considerando as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou responsável legal e adequado ao entendimento da criança.

Nesse sentido:

> Neste parágrafo há preocupação com a eventual dificuldade da criança de ter plena compreensão sobre os limites do tratamento dos seus dados pessoais, quer em decorrência da natural falta de maturidade ou nível de conhecimento, ou de eventuais limitações físicas, auditivas, visuais ou mentais do titular dos dados. Com isso, há reforço à clareza com a informação prévia ao tratamento dos dados, bem como a necessidade de implementar soluções de acessibilidade, cabendo observar quanto a esse tocante a Lei 13.146/2015 (Lei Brasileira de Inclusão da Pessoa com Deficiência – Estatuto da Pessoa com Deficiência), em especial, o disposto no artigo 63, que trata da obrigatoriedade de portais em geral implementarem soluções de acessibilidade. (MALDONADO, BLUM, 2019).

Já em relação ao Estatuto do Idoso, embora a LGPD não trate de forma específica sobre estes titulares, compete a ANPD garantir que o tratamento de dados seja efetuado de maneira

simples, clara, acessível e adequada ao seu entendimento art. 55-J, XIX, LGPD). Além do mais, o regulamento de Dosimetria e Aplicação de Sanções, aprovado através da Resolução CD/ANPD n.º 4 de 24 de fevereiro de 2023, estabelece que a infração será considerada grave quando envolver tratamento de dados de crianças, adolescentes ou idosos (art. 8, §3º, I, "d"), repercutindo em uma sanção mais gravosa ao agente de tratamento.

Assim, não houve uma preocupação do legislador apenas em determinar quais são de fato os direitos dos consumidores, mas em instituir um microssistema de proteção aos direitos fundamentais, contribuindo para garantia da dignidade, da privacidade, e da segurança dessas pessoas, que tem como objetivo principal permitir que essa proteção também se estenda aos órgãos públicos e privados. Estes, por sua vez, devem batalhar pela tutela e pela defesa dos consumidores, com a finalidade de alcançar a eficácia da legislação consumerista.

Esta preocupação já mostra alguns efeitos práticos, como observado no *Relatório anual de Jurimetria* (OPICE BLUM, 2022): a privacidade de dados do consumidor encontra-se entre as maiores motivações para judicialização de demandas com base na proteção de dados.

2.2 Marco Civil da Internet: Lei nº 12.965/2014

A Lei nº 12.965/14, denominada de Marco Civil da Internet, foi aprovada, após cerca de nove anos em que se apresentavam projetos de lei para normatizar o ambiente virtual brasileiro, período no qual o número de usuários da internet só cresceu (CALDAS, 2019). Embora muitos dos direitos passíveis de violação na rede mundial de computadores já estivessem tutelados pela normativa brasileira, especialmente desde a promulgação da Constituição Federal de 1988, apenas uma legislação específica poderia diminuir as inseguranças das decisões judiciais sobre o tema (CALDAS, 2019).

A necessidade de se estabelecer o Marco Civil da Internet veio ao encontro do aumento de ilícitos civis e penais praticados na internet, sob a falsa premissa do anonimato, tornando-se necessário apresentar resposta contra esses infratores para garantir a segurança do uso da rede. O chamado "efeito Snowden", em referência a Edward Snowden, ex-funcionário da Agência de Segurança Nacional dos Estados Unidos que relatou publicamente o desenvolvimento de programas governamentais de espionagem contra pessoas físicas de todo o mundo, inclusive de agentes do governo brasileiro, ajudou a fomentar o debate (SOUZA; LEMOS, 2016).

O ex-agente revelou detalhes precisos e altamente sigilosos, que versavam sobre como funcionava o programa de vigilância americano, que abrangia o mundo todo. O programa de espionagem agia por meio do tráfego de informações de vários países. Esses acontecimentos

causaram uma comoção mundial, de cunho político, alertando países como o Brasil, os integrantes da União Europeia e outras nações a discutirem mudanças estruturais significativas na proteção de dados pessoais, o que incluía leis mais rígidas.

Dessa preocupação surgiu a previsão de institutos como: regras de consumo; inviolabilidade da intimidade da vida privada, bem como do sigilo no fluxo de comunicações pela internet; guarda e disponibilização dos registros de acesso a aplicações de internet, devendo atender à preservação da intimidade, da honra e da imagem das partes envolvidas.

Considerado um avanço, ao menos parcial, por muitos setores da sociedade, o Marco Civil da Internet ainda era insuficiente, de acordo com estudiosos, para uma proteção mais específica de certos aspectos do direito à privacidade – especialmente porque os direitos relacionados à coleta e à venda de dados dos usuários, se anonimizados, ainda não estavam tão detalhadamente regulados – ao contrário do que ocorria na legislação europeia, por exemplo –

, principalmente para a proteção em termos de ações individuais.

Machado (2015, p. 43), entre outros, entendia que o Marco Civil da Internet era insuficiente para tanto:

> De fato, essa legislação não poderia ficar alheia à proteção de dados pessoais, muito embora não seja seu objetivo principal, no entanto, na ausência de legislação específica acerca desta matéria, o Marco Civil teve que antecipar algumas regras referentes ao tratamento de dados pessoais, até porque uma grande parte da utilização da web envolve a questão do uso de dados pessoais dos internautas. Nesse sentido, observa-se que os sites brasileiros utilizam os dados dos usuários de forma totalmente indiscriminada, não esclarecem nem informam de forma transparente o que acontecerá com as informações que lhes são solicitadas. Muitos sites de redes de lojas sequer informam que utilizam na sua política de segurança os chamados Cookies, ou quando informam não o fazem de forma clara e transparente.

Assim, uma nova lei tratando de questões semelhantes foi discutida e promulgada no país para abarcar os temas que não eram contemplados no Marco Civil da Internet ou que foram tratados de forma insuficiente. Nesse sentido, o texto legal *General Data Protection Regulation* (GDPR), emanado no âmbito da União Europeia, trouxe inovações que não constavam no Marco Civil brasileiro.

A lei descreve, dentre seus princípios, a proteção à privacidade, proteção dos dados pessoais, segurança da rede e adoção de medidas técnicas compatíveis e uso de boas práticas. Conforme observam Camilla Jimene e Guilherme Sicuto:

> O mesmo dispositivo legal prossegue nos incisos subsequentes assegurando o direito do usuário ao 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 (inc. VII) e informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados

> pessoais (inc. VIII). No art. 11, referido Diploma Legal preconiza que em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (JIMENE; SICUTO, 2021).

O Marco Civil da Internet passa a ter novos contornos, um pouco diferentes da tendência legislativa da época de criminalizar condutas, assumindo o papel de consolidador de direitos constitucionais vocacionados à proteção da privacidade e dos dados pessoais dos titulares (usuários da internet). A Lei nº 12.965/2014 assegurou o tratamento de dados pessoais, prevendo que não fossem transferidos sem o consentimento expresso do titular ou determinação legal (SOUZA; LEMOS, 2016). Com a LGPD, por sua vez, amplia-se o escopo da proteção de dados e passa-se a prever não apenas o consentimento como base legal, mas dez bases legais para legitimar o tratamento de dados pessoais. Nesse sentido, Bioni *et al*. (2020, p. 177) afirmam:

> Com isso, cria-se uma dinâmica obrigacional pela qual não só o cidadão titulariza o direito em circular a sua informação pessoal, mas, também, outros o fazem, sem que devam necessariamente consultá-lo para tanto. Dito de outra forma, terceiros, que não o próprio titular da informação, detêm a liberdade jurídica para destravar o fluxo informacional desde que lastreiem a sua atividade em uma das outras nove bases legais.

Cumpre registrar importante artigo do Marco Civil da Internet que impõe ao poder público a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico. Dentre essas iniciativas, deve promover reduzir as desigualdades em relação ao uso da tecnologia (arts. 26 e 27 da Lei nº 12.965/14).

Crescem os anseios da sociedade pela proteção da privacidade ante o aumento do uso de plataformas digitais, considerando que os dados pessoais passaram a representar um ativo econômico e político para as *big techs* que os detêm, manipulam e monetizam. Assim, em 2018 é sancionada a Lei nº 13.709/2018, Lei Geral de Proteção de Dados, que trouxe uma série de direitos aos titulares de dados pessoais, com o objetivo de reduzir o tratamento excessivo e, muitas vezes, abusivo, dos titulares de dados. Em reforço à necessidade de proteção dos dados pessoais, a Emenda Constitucional nº 115, de 10 de fevereiro de 2022, incluiu o direito à proteção de dados pessoais no rol dos direitos e garantias individuais no artigo 5º, LXXIX, CF.

Diga-se, contudo, que tanto o Marco Civil da Internet quanto a Lei Geral de Proteção de Dados Pessoais são leis vocacionadas a regular a privacidade e o tratamento de dados, seja

nos meios físicos, seja nos digitais. A LGPD e o MCI trouxeram vários direitos aos titulares de dados pessoais e aos usuários de internet, alguns já existentes em outras legislações, como o Código de Defesa do Consumidor (CDC). Contudo, esses direitos demandam uma interpretação harmônica com o recorte interpretativo e seus eventuais pontos de atrito.

2.3 O direito à proteção de dados nas plataformas digitais

Com a velocidade de transformação da atual sociedade, especialmente no que se refere ao elevado uso do suporte digital para as mais variadas facetas das relações humanas, a regulamentação existente tornou-se insuficiente:

> O documentário Terms and Conditions my apply ("Sujeito a termos e condições"), do diretor americano Cullen Hoback, lançado em 2013, discute a expansão progressiva do mercado de dados alimentado pelos Estados e grandes corporações como Facebook, Google e Amazon e nos alerta sobre as dimensões cada vez mais problemáticas para a tratativa jurídica desse mercado. Nossos dados já são vistos como "o novo petróleo", sendo imprescindíveis para as articulações mercadológicas na contemporaneidade. Como destaca Nick Srnicek (2018), o capitalismo do século XXI é estruturado pela data-driven economy (economia movida a dados), ou seja, os dados pessoais ocupam a centralidade em grande parte das atividades econômicas no contexto do capitalismo globalizado (COSTA; OLIVEIRA, 2019).

Em setembro de 2020, completaram-se dois anos de vigência da LGPD. A lei nº 13.709 foi sancionada em 14 de agosto de 2018. Contudo, teve seu primeiro marco de vigência em 28 de dezembro de 2018 (art. 55), com a criação da Autoridade Nacional de Proteção de Dados (ANPD). Em setembro de 2020, todos os artigos, com exceção dos art. 52, 53 e 54 (referentes às penalidades), entraram em vigor. O último marco temporal (vigência plena) ocorreu em 1º de agosto de 2021. Nesse cenário, a LGPD surgiu para atender a uma necessidade de lei específica sobre o tema, e também para contribuir com o manejo seguro dos dados pessoais, mitigando os riscos desse processo e evitando que tais dados fossem utilizados para fraudes, divulgados sem autorização do titular ou usados para discriminação ou perseguição política.

Destaca-se, no entanto, que, já em fevereiro de 2022, a Constituição Federal contemplou a proteção de dados entre os direitos fundamentais, por meio da Emenda Constitucional nº 115/2022. Desse modo, foi incluído ao art. 5º, CF, o inciso LXXIX: "É assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". Além disso, acrescentaram-se os art. 21, XXVI: "Organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei"; e 22, XXX: "Proteção e tratamento de dados pessoais", que estabelecem a competência privativa da União em legislar sobre a matéria.

Esse reconhecimento confere relevância à matéria referente à proteção de dados, principalmente em tempos em que a troca de informações dentro do meio digital está cada vez mais alta e rápida. Os dados pessoais ganharam status de direitos fundamentais, o que trouxe significativas mudanças na ordem de tratamento, recepção e gestão destes, representando maior segurança aos usuários – que terão garantia de observância de seus direitos, especialmente quanto à utilização legítima dos dados para as finalidades para as quais foram colhidos.

> Na sociedade digital, as redes sociais constituem um cenário de novos desafios para a tutela da personalidade humana. A partir das atividades de controle e armazenamento de dados pessoais efetivadas pela economia de dados, as personalidades são mapeadas no espaço digital por "signos identificadores" das pessoas. É uma nova identidade que os controladores de dados precisam classificar, de acordo com a personalidade do titular das informações (COSTA; OLIVEIRA, 2019).

Dessa forma, todos os agentes envolvidos no tratamento desses dados passam a ter de observar as regras de utilização das informações a que têm acesso, de modo que seja possível garantir os direitos do seu titular. As mudanças trazidas pela LGPD representam verdadeira quebra de paradigma e desafio à cultura nacional quanto à forma de tratamento dos dados pessoais no país, demandando a conscientização de toda a sociedade acerca da importância desses dados e seus reflexos em direitos fundamentais como a liberdade, a privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Embora, com a promulgação da EC nº 115/2022, tenha restado sedimentada a proteção de dados como direito fundamental, não se pode deixar de mencionar precedente histórico do Supremo Tribunal Federal, em que o plenário referendou a Medida Cautelar das Ações Diretas de Inconstitucionalidade (ADIs) nºs 6.387, 6.388, 6.389, 6.390 e 6.393. Desse modo, determinou a suspensão da Medida Provisória 954/2020, que permitia às empresas de telecomunicação prestadoras do Serviço Telefônico Fixo Comutado (STFC) e do Serviço Móvel Pessoal (SMP) disponibilizar ao Instituto Brasileiro de Geografia e Estatística (IBGE), em meio eletrônico, a relação de nomes, números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas.

Segundo Doneda *et al*. (2021), essa decisão trouxe algo mais importante para o Direito brasileiro: "o reconhecimento de um direito fundamental à proteção de dados como direito autônomo, extraído a partir de leitura sistemática do texto constitucional brasileiro". Continua a autora que essa proteção não está isenta de limitação, no caso concreto, em que se exige

> (i) uma base jurídica segura, (ii) com a clareza necessária sobre a finalidade do tratamento de dados, para que se avalie o nível de intervenção no direito fundamental,
> (iii) e que seja também proporcional, adequada e necessária à finalidade pretendida, adotando, ainda, (iv) as providências preventivas mínimas de cunho procedimental e

> organizacional, orientadas à segurança dos cidadãos envolvidos e à diminuição dos riscos de danos a seus direitos da personalidade (DONEDA *et al*., 2021, p. 87).

Os dados são fontes valiosas para as empresas que conseguem monetizar negócios com base nas informações pessoais. Por isso, cada vez mais, tem crescido a demanda por dados pessoais para alimentar cadastros e sistemas, não só para oferta de produtos e serviços, mas para criação de perfil de usuário à sua própria revelia. Dessa forma, a LGPD traz como um de seus fundamentos o art. 2º, II, que possibilita ao titular o controle sobre o fluxo de dados (MALDONADO; OPICE BLUM, 2019).

A sociedade da informação é marcada pela crescente interação com os meios digitais, e trouxe a necessidade de multiplicidade de ramos do Direito para formar o arcabouço de Direito Digital. Dentre suas singularidades está a característica de que os princípios prevalecem em relação às regras, já que o ritmo da evolução tecnológica é sempre mais acelerado que o da atividade legislativa (ROSA; NUNES; ASSUNÇÃO, 2021).

Percebe-se que o Direito Digital pode ser entendido como um dos alcances do Direito tradicional e costumeiro – eis que é a própria matéria do Direito, com seus princípios e normas reguladoras, aplicadas entre pessoas físicas e jurídicas quando elas se relacionam no ciberespaço, devido à intensa utilização da tecnologia, protegendo, dessa forma, direitos afetados de cada um desses atores nesse novo ambiente.

A LGPD tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Com forte influência da legislação europeia, o Brasil buscou tutelar os dados pessoais com alcance extraterritorial, aplicável a qualquer pessoa ou organização, pública ou privada, envolvida em atividades que coletem dados pessoais no Brasil ou com a finalidade de oferecer e/ou fornecer bens e serviços do país. Essa Lei busca proporcionar alternativas para que o titular possa ter controle dos seus dados, além de contemplar medidas que abrangem desde a concepção de um novo produto ou serviço, voltadas à privacidade e à proteção de dados.

A legislação brasileira incorpora uma série de princípios e bases legais para o tratamento adequado dos dados pessoais. A Lei Geral de Proteção de Dados prevê dez bases legais para o tratamento de dados pessoais e oito para a realização do tratamento de dados pessoais sensíveis. Estabelece também direitos aos titulares de dados pessoais. O tratamento dos dados pessoais necessita de fundamento legal, com características próprias que devem ser analisadas de acordo com o procedimento realizado e a relação com o titular dos dados.

Além do mais, a LGPD impõe aos responsáveis que os dados sejam tratados de forma ética, assegurando também sua compatibilidade com os seus princípios. Assim, é necessário

que toda atividade que trate dados pessoais contenha mecanismos para resguardar os interesses de todos os titulares de dados com quem se relacione. A LGPD buscou organizar formalmente toda a matéria referente à proteção de dados pulverizada no ordenamento jurídico. Dessa forma, além de formatar um sistema amplo e detalhado sobre proteção, será necessário que os princípios encontrem concretude na própria lei (OLIVEIRA; LOPES, 2019).

A referida Lei exige que o controlador dos dados pessoais estabeleça uma das bases legais para o tratamento desses dados e, necessariamente, cumpra com todos os princípios da lei. Os princípios de transparência, finalidade, necessidade, proporcionalidade, qualidade, livre acesso e segurança formam a espinha dorsal de inúmeras normas existentes atualmente, sendo importante ressaltar que eles devem ser cumpridos independentemente das bases legais para o tratamento de dados pessoais (VAINZOF, 2019).

As atividades de tratamento de dados pessoais deverão observar, além da boa-fé, outros dez princípios. Os princípios de finalidade e adequação impõem que o tratamento dos dados pessoais deve respeitar propósitos legítimos, específicos, explícitos e informados ao titular. A limitação da finalidade impõe a obrigação de informar ao titular todos os usos, diretos e indiretos, de um dado coletado, ou seja, tanto para o cumprimento do propósito principal como para utilização em marketing, por exemplo, para envio de propagandas direcionadas. O princípio da necessidade determina que sejam coletados apenas os dados necessários para o atingimento da finalidade e seu armazenamento cumpra prazos mínimos.

Para o objeto deste estudo, um dos princípios mais relevantes é o da transparência, que impõe aos agentes de tratamento o fornecimento de informações claras, precisas e de fácil acesso. O princípio da transparência, além do art. 6º, está previsto nos arts. 9º; 10º§2º; 18º, I, II, VII e VIII; e no art. 20º. Isso porque a transparência não deve ser apenas assegurada na coleta de informações, mas em todo o processo de tratamento de dados (OLIVEIRA; LOPES, 2019). Além disso, a informação deverá ser feita de forma clara e concisa, evitando-se textos longos e repletos de linguagem técnica, que apenas especialistas conseguem compreender.

O reconhecimento da proteção de dados é importante, sobretudo, para reforçar a autodeterminação informativa e a diferenciação entre proteção de dados e intimidade. O uso de dados é uma realidade social que muitas vezes tem reforçado marginalizações e exclusões, contribuindo para a persistência de violações aos direitos dos seres humanos, em contraposição à luta pela aquisição de direitos, que teve um longo caminho de construção.

> O direito fundamental à privacidade na internet encontra fundamentos na obra de Paul Bernal (2014), que apresenta quatro direitos básicos: o direito de navegar com privacidade na internet, o de monitorar quem monitora, o de excluir dados pessoais e o de proteger a identidade on-line. Percebe-se que os dois últimos estão diretamente

> relacionados ao direito à “extimidade” e ao direito ao esquecimento, já que este justamente se baseia na possibilidade de apagar ou não definitivamente os dados pessoais, e aquele se relaciona ao âmbito da proteção pública, privada ou não (“extima”) dos dados on-line. De qualquer modo, objetiva-se demonstrar a necessidade de uma tutela transversal da privacidade, em nível nacional e internacional, e de dimensões verticais e complementares (NASCIMENTO, 2017).

É necessário, ainda, objetividade e clareza nesses dados, requisitos da transparência e da confiança, como decorrentes da necessidade de compreensão e acesso facilitado a todos, reequilibrando a vulnerabilidade que determina a necessidade de informações objetivas, compreensíveis e acessíveis. O ministro Antônio Herman de Vasconcellos e Benjamin afirma que, na sociedade de informação, os agentes econômicos e, decorrente disso, os cidadãos, depositam expressiva confiança nos bancos de dados. Acrescenta ainda que:

> Três desses traços da sociedade de consumo estão diretamente ligados aos arquivos de consumo. Tais entidades, a um só tempo, superam o anonimato do consumidor (o fornecedor não o conhece, mas alguém está a par de sua vida e história), auxiliam na concessão do crédito (por receber informações confiáveis de terceiros, o fornecedor, mesmo sem conhecer o consumidor, oferece-lhe o crédito), e, por derradeiro, permitem que os negócios de consumo sejam feitos sem delongas (se o crédito é rápido, o consumidor pode aproveitar essa economia de tempo para adquirir outros produtos ou serviços de fornecedores diversos) (BENJAMIN *et al.*, 2019).

Essa confiança abarca ainda o uso e o tratamento dos dados, sendo vedado o tratamento para envio de propagandas, spams, serviços não solicitados, telefonemas para ofertas de telemarketing e outras atuações que infrinjam a expectativa do titular. Dentro dessa sistemática, tem especial relevo o manejo de dados obtidos na internet. Assim,

> As redes como Google e Facebook, entretanto, expressam que não recolhem dados relacionados ao nome de seus usuários, ou seja, trata dados anonimizados, que não necessariamente identificam os indivíduos em particular. De fato, a forma como a Internet funciona não implica uma necessidade de identificação direta dos usuários para lhes direcionar conteúdo ou classificar seu perfil em um processo de decisão automatizada. Esse processo pode ser feito pela identificação do protocolo de endereço (IP) dos computadores e aparelhos, que podem ter múltiplos usuários. A partir desse “identificador eletrônico”, os dispositivos são reconhecidos e torna-se possível uma leitura do perfil comportamental da navegação on-line realizada (COSTA; OLIVEIRA, 2019).

Aos titulares dos dados pessoais também deverá ser garantido o livre acesso aos seus dados, assegurando-se a qualidade das informações armazenadas e sua possibilidade de correção. A segurança e a confidencialidade devem ser garantidas por meio de medidas técnicas e organizacionais, a fim de prevenir a ocorrência de incidentes de segurança envolvendo os dados pessoais.

Finalmente, temos os princípios de responsabilização, prestação de contas e não discriminação. Os controladores têm a obrigação de responsabilidade quando da coleta, da guarda e do processamento de dados pessoais. Deverão ser armazenados registros de todas as atividades de tratamento dos dados e das respectivas medidas tomadas para adequar tais atividades às normas relativas à privacidade e à proteção de dados pessoais, comprovando, inclusive, a eficácia e a eficiência dessas medidas, e assegurando que nenhum tratamento seja realizado para fins discriminatórios, ilícitos ou abusivos.

Recentemente, o Supremo Tribunal Federal (STF) decidiu, no julgamento conjunto da Ação Direta de Inconstitucionalidade (ADI) nº 6.649 e da Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 695, que o compartilhamento de dados entre órgãos da administração pública federal deve respeitar a Lei Geral de Proteção de Dados Pessoais. O STF afirmou que, para se justificar, o compartilhamento de dados deverá ser realizado de acordo com os postulados da proporcionalidade, da razoabilidade e dos princípios gerais de proteção da LGPD. Destacou ainda a necessidade de instituir medidas de segurança compatíveis com os princípios de proteção da Lei, em especial a criação de sistema eletrônico de registro de acesso, para efeito de responsabilização em caso de abuso (SUPREMO TRIBUNAL FEDERAL, ADI nº 6.649/DF. Relator: Gilmar Mendes).

No contexto europeu, para que os avisos de privacidade das plataformas digitais estejam em conformidade com o *General Data Protection Regulation* (GDPR), devem assegurar a observância ao princípio da licitude, ou seja, não deve ser utilizado nenhum modelo de design com a finalidade de induzir o titular. Além do mais, será necessário o respeito aos princípios da transparência, minimização de dados e prestação de contas (EUROPEAN DATA PROTECTIN BOARD, 2022).

Além dos princípios e da adequação à base legal, o que é minimamente esperado no contexto das legislações de privacidade, o design de plataformas digitais deve levar em conta a proteção de dados como padrão, nos termos do art. 25 da GDPR:

> 1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.

> 2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

Cabe reforçar que a Organização das Nações Unidas (ONU) emitiu relatório sobre direito à privacidade, colocando em pauta os desafios e analisando três áreas principais: o abuso de ferramentas intrusivas de *hackers* ("*spyware*") por autoridades estatais; o papel fundamental de métodos robustos de criptografia na proteção dos direitos humanos on-line; e os impactos do monitoramento digital generalizado de espaços públicos, tanto off-line quanto on-line.

Segundo Mendes (2014), é significativo o avanço quanto à proteção de dados no país, considerada a inexistência de legislação específica. Se antes a tutela dos arquivos pessoais se limitava aos ambientes particulares, hoje arquivos privados estão armazenados eletronicamente na "nuvem".

O status constitucional confere maior relevância à proteção de dados e demonstra a preocupação da sociedade em relação a esse tema, ainda mais considerando o curto espaço de tempo em que esse direito foi reconhecido na Constituição Federal. Agora, o titular de dados conta com mais um mecanismo de proteção aos direitos, tanto frente ao Estado, como entre particulares, considerando sua eficácia vertical e horizontal. Ou seja, qualquer pessoa, natural ou jurídica, privada ou pública, tem o dever de zelar pelos dados pessoais dos titulares, assumindo os riscos e podendo sofrer sanções caso não aplique as proteções necessárias para evitar o uso inadequado ou fraudulento dos dados pessoais (RODRIGUES, 2022).

A LGPD estabelece bases legais para o adequado tratamento dos dados pessoais, exige a observância dos princípios mencionados e prevê que sejam fortalecidos o atendimento dos direitos dos titulares – principalmente os de acesso a seus dados, correção, anonimização, eliminação e portabilidade – e a gestão do consentimento. De toda forma, o GDPR e seus guias orientativos se constituem como importante fonte interpretativa para a proteção de dados do Brasil. A Autoridade Nacional de Proteção de Dados (ANPD), embora ainda não tenha nenhum documento específico sobre design de plataformas, sugere a utilização de técnicas de design conhecidas como *User Experience*, ou UX, para buscar efetividade com os princípios e as obrigações da LGPD para o tratamento de dados pessoais.

3 A IMPORTÂNCIA DA TRANSPARÊNCIA NOS AVISOS DE PRIVACIDADE

Embora a noção de privacidade não seja recente, somente começou a ser concretamente abordada pelo ordenamento jurídico no final do século XIX, e muito recentemente assumiu, enfim, suas feições atuais. A conotação contemporânea da proteção da privacidade é manifestada especialmente pela proteção de dados pessoais e passa a confluir com vários interesses ligados à personalidade e às liberdades fundamentais do titular de dados (DONEDA, 2021).

Não apenas as *Big Techs*, mas também empresas de vários segmentos têm utilizado a captura de dados, como idade, classe social, geolocalização e preferências pessoais, para segmentar clientes por meio do marketing direcionado. Vale dizer que o próprio titular se transforma no produto. O lucro imanente da sociedade de dados está diretamente ligado à publicidade, que se revela como o mais notável meio de comunicação de massas de nossa época (BAUDRILLARD, 2009).

Comumente, nas plataformas digitais, é possível observar alguns documentos que são destinados aos usuários, principalmente os termos de uso, que funcionam como uma espécie de contrato de adesão entre a plataforma e o consumidor que estipula as regras de uso de produtos e serviços das plataformas. Os termos de uso são obrigatórios para o comércio eletrônico e, essencialmente, são regidos pelas regras do Código de Defesa do Consumidor e/ou do Código Civil. Dessa forma, os termos e condições de uso não são vocacionados a estabelecer regras sobre privacidade e proteção de dados dos titulares; nesse sentido, o recorte desta pesquisa compreende apenas os avisos de privacidade.

Outros documentos são os famosos avisos de *cookies* ou política de *cookies*. Os *cookies* assumem uma função mais técnica sobre a própria forma de funcionamento da página da web porque viabilizam o seu funcionamento, a prestação de serviços, a medição de desempenho e os anúncios personalizados. A política de *cookies* tem a função de informar os usuários quanto ao funcionamento deles, suas funcionalidades e as opções de desativá-los ou controlá-los. Um *cookie* não necessariamente contém um dado pessoal, e, embora sua má utilização possa acarretar danos à privacidade do titular, esta pesquisa centrou-se nos avisos de privacidade que, essencialmente, são documentos que servem para informar o titular sobre o tratamento dos dados pessoais. Além do mais, os avisos de privacidade contêm um resumo sobre quais *cookies* são utilizados e a sua finalidade.

O aviso de privacidade é o documento que contém as informações sobre como as organizações tratam os dados pessoais dos seus usuários. Tecnicamente, é chamado de “aviso

externo de privacidade", porque é direcionado às pessoas externas com a finalidade de dar transparência sobre como os dados são tratados, principalmente, os tipos de dados que são coletados, a finalidade do tratamento, informações sobre a existência de compartilhamento dos dados e a sua justificativa e a forma como o titular pode exercer seus direitos. Cumpre esclarecer, também, que o aviso de privacidade não se confunde com a política de privacidade, a qual é um documento interno da organização que estabelece regras sobre o tratamento de dados no ambiente interno. Contudo, na prática, ainda existe bastante confusão entre esses termos (MALDONADO, 2019, p. 315).

De acordo com a autoridade do Reino Unido sobre proteção de dados, Information Commissioner's Office (ICO), em seu material de referência *Transparency (cookies and privacy notices)* (*Transparência (cookies e política de privacidade)*), os avisos de privacidade trazem as informações que o titular de dados deve saber a respeito do tratamento, ou seja, o modo como a plataforma planeja utilizar seus dados, por quanto tempo os dados serão armazenados e a existência de compartilhamento desses com terceiros. Essa explicação deve ser anterior ao tratamento dos dados, e precisa ser simples de ler e de fácil acesso. Esse documento também é um instrumento para gerar confiança para os titulares dos dados (INFORMATION COMMISSIONER'S OFFICE, 2022).

Ainda existe a ideia de que as plataformas digitais oferecem uma gama de serviços grátis, contudo, na atual era da sociedade da informação, não se pode mais acreditar que a navegação na internet seja gratuita. Mesmo que não exista um pagamento em dinheiro para determinado uso de sites e aplicativos, tal uso não acontece sem custo. Grande parte dos usuários da internet, porém, não se dão conta da quantidade de dados que estão compartilhando com as plataformas e de como essas informações são monetizadas. Ao navegar pela rede, somos monitorados em todos os passos, seja quanto aos cliques, seja em relação ao conteúdo que acessamos e o tempo que passamos on-line (PALHARES, 2020).

Um ditado que se tornou popular com o documentário *O dilema das redes* define ainda melhor o problema: "Se você não paga pelo produto, o produto é você". Assim, além da falta de transparência, uma grande questão sobre as práticas desse mercado de dados é a ausência de condições para que os titulares tenham acesso de modo adequado à funcionalidade das plataformas. Em sua maioria, as políticas de privacidade são escritas em linguagem rebuscada e extremamente técnica, e estão muito além da capacidade de leitura do seu público-alvo (PALHARES, 2020). Nesse sentido, complementa ainda Mendes (2014, p. 4341):

> Esse controle adquire ainda mais relevância diante das evidências de que as políticas de privacidade de algumas empresas estabelecem, na realidade, o contrário do que

> aparentam: são uma carta branca para o fornecedor processar os dados pessoais dos consumidores como bem entender. Ademais, a declaração de nulidade das cláusulas pelo Poder Judiciário poderia incentivar a melhoria das políticas de privacidade das empresas, prevenindo futuros danos aos consumidores.

Geralmente as pessoas não leem os avisos de privacidade disponíveis nas plataformas digitais que utilizam e acabam por passar um cheque em branco para que esses sites coletem, usem e compartilhem seus dados. Um dos fatores determinantes é a forma como esses avisos e outros documentos de privacidade direcionados aos titulares são escritos. As políticas de privacidade são estruturadas com uma linguagem complexa e técnica, em formato de contrato por adesão, que não estão adaptados para leitura no ambiente digital, seja computador, tablet ou smartphone, e não dialogam com o público-alvo.

Pesquisa realizada pelo site *VPN Overview* (BLUVSHTEIN, 2022), especializado em cibersegurança e privacidade, elencou as políticas de privacidade mais difíceis de ler e entender, estando incluídas nesse universo as das grandes empresas com milhões de usuários espalhados pelo mundo. O estudo demonstrou que 60% das políticas examinadas são praticamente ilegíveis ao público comum, concluindo que para compreensão seria necessário nível acadêmico de pós- graduação.

As consequências da falta de informação dos titulares e a coleta massiva de dados pelas organizações são desastrosas, tendo em vista que a maioria das políticas analisadas afirmam que não garantem a exclusão dos dados, permitem o compartilhamento para terceiros e contam com disposições vagas. Essa conduta pode implicar o comércio ilegal dos dados pessoais, desde agências de marketing até informações na *dark web* com finalidade de ilícitos.

Em outra pesquisa, realizada nos Estados Unidos (THE NEW YORK TIMES, 2019), em que foram analisados 150 avisos de privacidade, identificou-se alto grau de dificuldade de compreensão de termos, considerando os conhecimentos de pessoas com formação de Ensino Médio.

Os avisos de privacidade devem ser direcionados aos usuários com a finalidade de esclarecer como será realizado o tratamento dos dados pessoais durante todo o seu ciclo de vida. O titular dos dados deverá receber informações claras e precisas sobre a finalidade do tratamento, quais dados serão tratados, a existência de compartilhamento e o canal para exercício dos seus direitos (SOUZA; OLIVEIRA, 2021).

Recentemente, a Associação Brasileira de Normal Técnicas (ABNT) editou a NBR ISO/IEC 29.184, com o escopo de especificar o conteúdo e a estrutura dos avisos de privacidade on-line. O objetivo é permitir que os titulares de dados pessoais compreendam, através de uma

linguagem apropriada, os impactos que o tratamento de dados pode trazer para eles, além de facilitar o acesso para esclarecimento de dúvidas. É recomendada a utilização de frases curtas e objetivas, que possam resumir e apresentar, de forma clara, quais os propósitos para tratamento de dados pessoais.

> Nesse contexto, as organizações devem cogitar ir além dos requisitos mínimos de segurança; elas devem fundamentalmente proporcionar aos titulares informações claras, precisas e facilmente acessíveis sobre o tratamento de dados pessoais e o gerenciamento de processos que aumentem a satisfação e reforcem a confiança dos titulares (PALHARES, 2020). A comunicação com os titulares de dados é feita essencialmente através do aviso de privacidade externo, que contém todas as informações de privacidade a respeito da coleta das informações pessoais e da forma como elas estão sendo tratadas. Portanto, a linguagem deve ser de fácil compreensão, especialmente considerando indivíduos vulneráveis, como crianças, titulares não familiarizados com a tecnologia e estrangeiros, sem jargões ou juridiquês, alinhada com o estilo da organização e mantendo coerência com seu público (INFORMATION COMMISSIONER'S OFFICE, 2022).

Existe ainda a ideia de que o uso de palavras técnicas seja símbolo de poder e demonstração de conhecimento quando, na verdade, ignora a realidade da maioria da população e gera discriminação (ZONARI, 2022). No Brasil, embora não haja nenhum documento específico da Autoridade Nacional de Proteção de Dados, foi emitido o *Guia orientativo de cookies e proteção de dados pessoais* (BRASIL, 2022a), que sugere a utilização de técnicas de design conhecidas como *User Experience*, ou UX, para formas de apresentação relativas ao uso de *cookies*, que, em geral se alinham com os princípios e as obrigações da LGPD para o tratamento de dados pessoais.

Diante dos desafios da revolução digital, é necessário que a adaptação a essa nova realidade esteja atrelada à confiança nas plataformas digitais em relação à forma de tratamento dos dados pessoais, à finalidade, ao compartilhamento, à exclusão etc., considerando que esses dados representam um ativo econômico e político para as organizações que os detêm, manipulam e monetizam (TIROLE, 2020).

Os usuários têm a confiança de que os dados fornecidos não serão utilizados a seu desfavor; contudo, ainda não temos condições de conhecer os potenciais riscos que aceitamos. Ou seja, existe a dificuldade, tanto de tempo como de expertise, para compreender um aviso de privacidade, cujas ramificações são complexas (TIROLE, 2020).

Em artigo intitulado “Termos de uso e política de privacidade: design e visual law como promotores do princípio da transparência”, Haikal, Becker e Gueiros expõem a necessidade do Direito de se adequar às novas demandas do mercado:

> Esse movimento exige a constante reinvenção do modo como os profissionais atuam, ao passo que também desperta nas empresas o reconhecimento e a busca por advogados que entendam essa nova necessidade de mercado. Tal realidade impulsiona o surgimento de prestação de serviços que antes eram vistos como fora do escopo de atuação dos advogados. Hoje, não só o entendimento jurídico acerca dos temas importa, como também ganha cada vez mais relevância a forma como tais conteúdos são apresentados. A escrita rebuscada, com citações em latim e orgulhosa da sua complexidade e pouca clareza, não tem mais lugar no mercado e finalmente passa a ser vista como contraproducente (HAIKAL; BECKER; GUEIROS, 2021).

O General Data Protection Regulation (GDPR) dispõe expressamente que os controladores de dados, ou seja, as organizações que coletam dados de titulares para efetuar algum tratamento, devem ser transparentes em relação às informações relacionadas com o tratamento de dados, de forma que para o atendimento do princípio da transparência é necessário que as informações sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples (MALDONADO, 2020, p. 310). Neste sentido, Rony Vainzof:

> Os *controllers* devem considerar sempre os titulares vulneráveis quanto ao entendimento das infinitas possibilidades de tratamento, notadamente quando ocorrer por meios digitais, em uma “conduta silenciosa”, pois o déficit informacional ganha relevância no ambiente digital, diante da velocidade das mutações do tratamento de acordo com o avanço tecnológico, aumentando, portanto, a necessidade de informações claras, completas e ostensivas aos titulares, que aceitam determinadas transações ao confiar voluntariamente nas informações concedidas pelos responsáveis (VAINZOF, 2020).

Nesse mesmo sentido estabelece o art. 6º, VI, da LGPD: “transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”. Essa preocupação do legislador, tanto na União Europeia, quanto no Brasil, revela que os titulares não têm ampla visibilidade sobre o tratamento dos dados para que consigam enxergar, de maneira clara, a legalidade, a legitimidade e os propósitos do tratamento (VAINZOF, 2022). Nota-se a preocupação do legislador no que concerne ao uso de linguagem adequada para atingir-se a completa compreensão, sugerindo ele próprio a utilização de recurso visual sempre que seja adequado (MALDONADO, 2020, p. 312).

Reforçando a importância que o legislador dispensou a esse assunto, o art. 9º da LGDP dispõe sobre os dados a que o titular deve ter acesso, de forma clara, facilitada e gratuita:

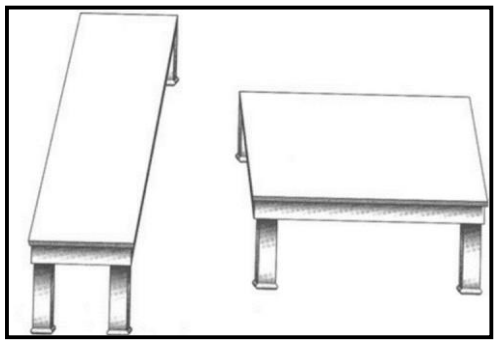
> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

O desafio é transformar informações de privacidade em conteúdo acessível. A proposta do *Legal Design* (design de produtos e serviços jurídicos) é melhorar a comunicação de informações legais complexas e a experiência do usuário do sistema. Por meio de sua aplicação, documentos como o aviso de privacidade podem ter estruturação visual, facilitando a compreensão de termos legais por meio da utilização de iconografia, informações em camadas de resumo e estruturação por tópico de assunto abordado, auxiliando a localização das informações (OPICE BLUM, 2022).

3.1 *Design* como ferramenta de influência psicológica

Roger Shepard, a partir dos seus estudos sobre representações visuais, demonstra como o nosso cérebro pode ser levado a erro a partir da compreensão do comportamento humano, e seus erros são cometidos de forma sistemática (THALER; SUNSTEIN, 2019). Na imagem a seguir, as duas mesas têm exatamente a mesma medida, contudo, em virtude da forma como foram desenhadas, é possível entender erroneamente que se trata de duas mesas de tamanhos diferentes:

Figura 1 – Duas mesas



Fonte: THALER; SUNSTEIN, 2019.

A neurociência classifica o sistema cognitivo em dois: sistema automático e sistema reflexivo. O sistema automático é responsável pelas decisões rápidas, de acordo com nossos reflexos e percepções. Esse sistema pode ser facilmente levado a erro considerando a velocidade da tomada de decisão de modo instintivo. Já o sistema reflexivo é responsável pelas tomadas de decisões de forma consistente e com base nos conhecimentos adquiridos. Este sistema é mais lento, considerando que é necessário empregar maiores esforços para a tomada de decisão consciente (THALER; SUNSTEIN, 2019).

A sociedade altamente conectada passa a impressão de que a quantidade de informação aumentou vertiginosamente, inversamente proporcional à disponibilidade de tempo (TOLER, 2020). A multiplicidade de tarefas que as pessoas executam impõe várias tomadas de decisão em um mesmo dia. Isso faz com que muitos usuários apenas aceitem os avisos de privacidade sem ler, ou apenas cliquem no botão de avançar para que determinado aviso deixe de cobrir o conteúdo do site.

O ser humano é responsável por apenas uma média de 5% a 15% das decisões que toma durante o dia. O restante provém do inconsciente, que se deixa levar por fatores externos e emoções (ASSAD, 2017). Essa informação torna-se extremamente relevante, tendo em vista que, de acordo com Brittany Kaiser, cofundadora do Own Your Data Foundation, a maioria das pessoas não percebe a quantidade de dados que produz e que é coletada, de forma gratuita, para ser comercializada posteriormente por todo o mundo, para organizações públicas e privadas.

O design pode proporcionar uma experiência que induza as pessoas a escolhas que não necessariamente representam sua vontade. Muitas plataformas digitais utilizam os *nudges* (em português, “cutucada”, “empurrão”), termo cunhado da economia comportamental e da psicologia, a partir dos quais se sugestionam escolhas por vieses psicológicos. Os usuários tomam decisões influenciados por vieses cognitivos, sem mesmo estarem cientes disso, ao invés de usar a racionalidade (WOODROW, 2018).

Essa arquitetura é desenvolvida a partir de comportamentos econômicos e psicológicos, combinados com a análise de dados qualitativos e quantitativos para o desenvolvimento do produto. Nesse sentido:

> A utilização de *nudges*, de um modo geral, é relacionada à estratégia de reenquadramento de atitudes, através da utilização de incentivos, isto é, a partir da influência à pessoa para que tome atitudes em uma determinada direção predefinida. Como se não bastasse, a estratégia também se relaciona à economia comportamental, tendo em vista que busca aprimorar o poder explicativo das teorias econômicas a partir da utilização de princípios psicológicos. Evidentemente, por meio de diversas

> variáveis, os *nudges* permitem ser a válvula motriz para influenciar decisivamente a forma de tomada de escolhas pelos indivíduos (BASAN; PROTO, 2021).

A imagem a seguir representa a interface do Snapchat. Observa-se que o design utilizando o ícone de contagem regressiva do relógio sugere que o compartilhamento será realizado apenas no tempo indicado.

Figura 2 - Snapchat

Fonte: WOODROW, 2018.

Contudo, não é exatamente assim que funciona, conforme bem apontado por Woodrow (2018, p. 21, tradução livre):

> Os Snaps simplesmente se tornam invisíveis para os destinatários. Cópias da foto ainda existem. A maioria dos telefones modernos são projetados para permitir que os usuários tirem capturas de tela — uma tática que é usada regularmente para "capturar" Snaps. Peritos forenses de dados são capazes de recuperar cópias de fotos ainda remanescentes no armazenamento. Há até mesmo um software de terceiros que permite que os usuários salvem snaps antes que eles desapareçam. Foi assim que a estudante Zeeshan Aqsar, de 19 anos, salvou uma foto nua enviada por uma estudante de 15 anos via Snapchat, que ele usou para chantageá-la por mais fotos e dinheiro. Como muitos usuários do Snapchat, a jovem pensou que a foto que ela enviou desapareceria. Como mencionado anteriormente, o Snapchat inicialmente falhou em garantir que apenas seu próprio cliente de software pudesse acessar sua interface de programação de aplicativos. O design poderia ter sido aproveitado para moldar melhor as expectativas dos usuários e tornar a economia de fotos mais difícil.

A estrutura usualmente utilizada pelas plataformas digitais não dá condições de conhecer o risco do compartilhamento de informações. Os usuários não têm tempo e expertise para entender os termos das políticas de privacidade, considerando suas ramificações complexas (TIROLE, 2020). Ou seja, os profissionais que elaboram esses avisos de privacidade e inserem-nos nas plataformas digitais não deveriam, apenas, se concentrar no cumprimento formal da lei. É necessário colocar o usuário no centro, como parte da sociedade, a fim de

proporcionar uma experiência positiva e de aculturamento. Sobre o papel do design:

> Em grande parte, o design é uma área projetual que atua na conformação da materialidade – em especial, dos artefatos móveis. Ele está associado, em suas origens, a outras áreas que projetam a configuração de artefatos, como artes plásticas, arquitetura e engenharia, tangenciando cada uma delas em várias frentes. Ao mesmo tempo, o design é uma área informacional que influi na valoração das experiências, todas as vezes que as pessoas fazem uso de objetos materiais para promoverem interações de ordem social ou conceitual (CARDOSO, 2016, p. 174).

Pesquisa realizada entre consumidores europeus (LOMAS, 2019) demonstrou como eles interagem com os diversos designs de *cookies* e, principalmente, de que maneira algumas formas de design podem direcionar suas escolhas. A conclusão do levantamento foi que, se os sites estivessem colhendo o consentimento de acordo com a GDPR (base legal utilizada na União Europeia para essa finalidade), apenas a minoria dos consumidores concordaria com a tecnologia de rastreamento dos *cookies*.

Nesse sentido, o julgamento da Corte de Justiça da União Europeia, em 01/10/2019 (UNIÃO EUROPEIA, 2019), quanto à análise do site de uma empresa de jogos on-line, determinou que os sites devem informar expressamente sobre a duração e a validade dos *cookies*, comunicando que a inatividade do usuário não pode ser considerada como forma de validade do consentimento e que caixas de seleção “pré-selecionadas” serão consideradas inválidas, ou seja, exige-se uma postura ativa do titular para expressar sua anuência.

A Agência Norueguesa de Proteção ao Consumidor (FORBRUKARRÅDET, 2018), numa análise de amostras de configurações do Facebook, do Google e do Windows 10, conseguiu demonstrar como o padrão de configuração desses aplicativos utiliza técnicas e recursos de design de interface destinados a manipular usuários para tomada de decisões intrusivas à sua própria privacidade.

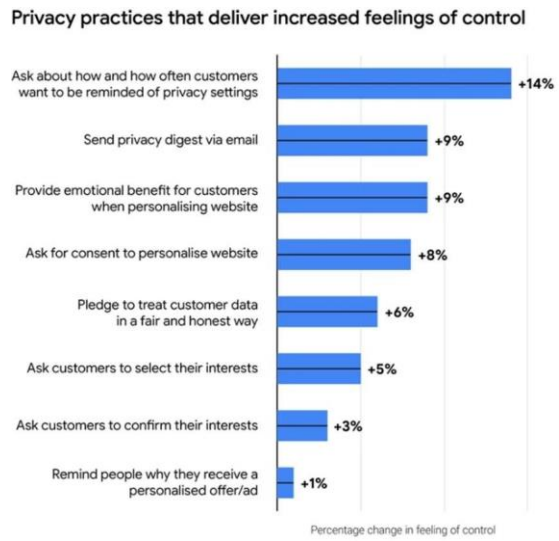
O estudo indicou também a existência do chamado paradoxo de controle, em que os usuários que recebem mais controle são também suscetíveis a correr mais riscos, ao divulgar informações confidenciais – o que sugere que os controles são realmente eficazes em garantir que a proteção dos dados seja apenas ilusória. Não basta que os avisos de privacidade apresentem ao usuário muitas informações complexas e de difícil compreensão, que certamente serão ignoradas, existindo uma falsa impressão de controle. É necessário, além da maximização da transparência, o empoderamento do titular quanto às suas opções de privacidade.

Pesquisa realizada pelo Google e pelo Instituto Ipsos demonstrou que 43% das pessoas mudariam de marca ao perceber que outra marca oferece boa experiência em privacidade. E, para tanto, não basta apenas oferecer controles sobre suas preferências. A pesquisa apontou:

> As marcas precisam ir além do básico para fornecer experiências de privacidade verdadeiramente positivas. Isso envolve informar às pessoas por que seus dados estão sendo coletados, para que serão usados e como a experiência do cliente será aprimorada. Todos esses fatores se combinam para criar transparência e construir a confiança com seus clientes (MINCKLER, 2022).

A pesquisa aponta importantes aspectos para tornar a experiência do usuário significativa, isto é, demonstrando para o titular a contrapartida em seu benefício em razão da coleta de dados, experiência memorável, lembrando aos titulares todos os dados que foram compartilhados, e a experiência gerenciável, fornecendo ferramentas simples e intuitivas para controlar suas permissões de privacidade.

Figura 3 - Práticas de privacidade



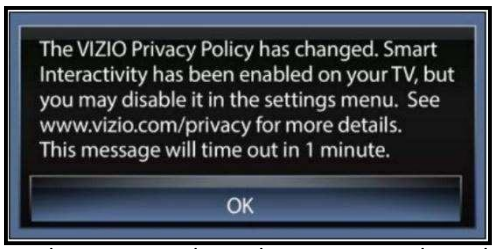
Fonte: https://www.thinkwithgoogle.com/intl/en-gb/future-of-marketing/ privacy-and-trust/research-customer- privacy-practices/

Nesse sentido, a Federal Trade Commission (FTC), nos Estados Unidos, tem adotado medidas para investigar empresas que não são totalmente transparentes nos avisos de privacidade. Um exemplo dessas ações foi o caso da Vizio, fabricante de Smart TV. No seu aviso de privacidade constava a mensagem (Figura 4): “O Aviso de Privacidade da Vizio mudou. A Interatividade Inteligente foi ativada na sua TV, mas você pode desativá-la no menu de configurações. Consulte www.vizio.com/privacy para obter mais detalhes. Esta mensagem irá expirar em 1 minuto.”

Percebe-se que a configuração “*Smart Interactivity*” não buscava apenas que os consumidores recebessem “ofertas e sugestões do programa”, na realidade permitia que a Vizio coletasse e compartilhasse o perfil de visualização de programas dos consumidores com

terceiros.

Figura 4 - Aviso de privacidade da Vizio



Fonte: https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark- patterns-designed-trick-trap-consumers.

A falta de um aviso de privacidade suficientemente claro e transparente acarreta violação à Lei Geral de Proteção de Dados Pessoais, podendo resultar em sanções pela Autoridade Nacional de Proteção de Dados. Além disso, pode acarretar danos reputacionais e perda da confiança dos usuários, bem como ações judiciais por parte dos consumidores.

Portanto, o design pode ser utilizado como ferramenta para sugerir tendências de comportamento. A utilização de tecnologia para coleta massiva de dados atualmente é observada como sendo um grande desafio para a garantia do direito à privacidade. Desse modo, a proteção de dados pessoais deve ser buscada a partir de um viés jurídico e econômico, considerando as funções que a tecnologia deve assumir dentro da sociedade, sem que exerça controle sobre ela.

3.2 *Dark pattern*: práticas manipuladoras no *design* de documentos

"Padrões escuros de design" é a tradução para o chamado *dark pattern*, que refere-se a armadilhas no design das plataformas para induzir o usuário a tomar decisões prejudiciais de forma imperceptível. O termo *dark pattern*, cunhado em 2010 pelo designer de Experiência do Usuário Harry Brignull, refere-se a práticas para tendenciar escolhas específicas com base na arquitetura de design em sites e aplicativos (BRIGNULL, 2021). Esses padrões envolvem opacidade dos dados, falta de clareza e técnicas que guiam a ação dos usuários para determinada resposta.

Ocorre, contudo, que não apenas as condutas reconhecidas como *dark pattern* devem ser combatidas. Muitas vezes, ainda que inexista uma conduta maliciosa ativa, é comum encontrar avisos de privacidade extensos, complexos, trazendo expressões técnicas específicas

e desconhecidas pelo público-alvo. São as condutas passivas – entendidas como um compilado de leis, regulamentos e orientações de difícil acesso e compreensão –, que também deverão ser combatidas.

A diretiva europeia recentemente aprovada prevê mecanismos e recomendações para combater o denominado *dark pattern* (padrões escuros), que leva os usuários a tomarem decisões potencialmente prejudiciais em relação ao tratamento de seus dados pessoais (EUROPEAN DATA PROTECTIN BOARD, 2022).

Segundo pesquisa da União Europeia (EUROPEAN COMISSION, 2022), existe uma tendência dos titulares, principalmente consumidores, de, mesmo percebendo práticas de *dark patterns*, acostumarem-se com essa postura que lhes é imposta, tendo em vista a dificuldade de se defender da plataforma.

A *Federal Trade Commission* (FTC), órgão responsável por proteger consumidores e realizar a defesa da concorrência nos Estados Unidos, emitiu relatório com base em recente pesquisa. O documento aponta significativo aumento do uso de *dark patterns* por empresas para enganar ou manipular os consumidores, forçando a aquisição de produtos e serviços ou o fornecimento de seus dados, renunciando à proteção à privacidade (FEDERAL TRADE COMMISSION, 2022).

O relatório, intitulado de *Bringing dark patterns to light* (*Trazendo padrões escuros para a luz*), concentrou-se em quatro formas comuns de padrões escuros: padrões que incluem anúncios disfarçados; padrões que dificultam o cancelamento de assinatura; padrões que não disponibilizam o custo real do produto ou serviço; e, por último, padrões que direcionam intencionalmente o compartilhamento de dados dos usuários. Utilizando um modelo desta última forma de indução de compartilhamento de dados, que é o recorte da presente dissertação, a Figura 5 demonstra a intenção do site de confundir o usuário, através de pergunta que subverte as preferências de privacidade.

Figura 5 - Aviso de privacidade da Fitness Trainer

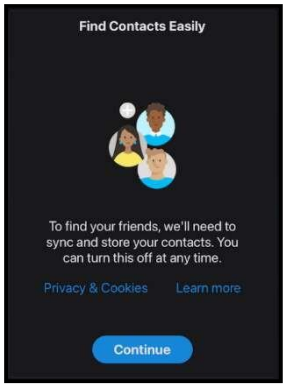
Fonte: https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark- patterns-designed-trick-trap-consumers.

O aviso de *cookies* do site Fitness Trainer utiliza uma pergunta de difícil compreensão para o compartilhamento de dados: “Você se opõe a não permitir que a Fitness Trainer compartilhe suas informações pessoais com terceiros?”. É evidente que a intenção é induzir o usuário a compartilhar informações. Este exemplo se enquadra perfeitamente na definição de *dark pattern*, criada pelo especialista em Experiência do Usuário Harry Brignull, em seu discurso na *Federal Trade Commission* (2021, tradução livre):

> Um *Dark Pattern* é um truque manipulador ou enganoso em software que faz com que os usuários concluam uma ação que de outra forma não teriam feito, se a tivessem entendido ou tivessem uma escolha no momento. Por exemplo, se você tem um botão que funciona como um “Sim” quando clicado, mas através do uso de posicionamento, cor e palavras de truque, parece dizer “Não”, muitos usuários serão pegos de surpresa (BRIGNULL, 2021).

Já no caso do Skype, ao abrir o aplicativo, apresentava-se a mensagem: “Para encontrar seus amigos, precisaremos sincronizar e armazenar seus contatos. Você pode desativar isso a qualquer momento.” A Figura 6 mostra apenas o botão azul para continuar prevalecendo o compartilhamento de dados sem dar ao usuário a opção de não aceitar com a mesma facilidade.

Figura 6 - Aviso de privacidade Skype



Fonte: https://www.deceptive.design/brands/skype

Reforçando a seriedade do tema e a preocupação das autoridades com relação a esses padrões escuros, a European Data Protection Board (EDPB) emitiu o *Guideline 3/2022: Dark patterns in social media platform interfaces: How to recognise and avoid them* (*Padrões escuros em interfaces de plataformas de mídia social: como reconhecê-los e evitá-los*) (EUROPEAN DATA PROTECTION BOARD, 2022). O EDPB, para formação do guia orientativo, considerou a jornada do usuário durante todo o ciclo de vida em uma plataforma de mídia social, examinado cinco hipóteses de uso: (i) cadastro; (ii) uso; (iii) segurança dos dados; (iv) granularidade de escolhas e (v) exclusão da conta.

A autoridade europeia considera padrões escuros como interfaces que levam os usuários a tomarem decisões não intencionais, relutantes e potencialmente prejudiciais sobre o processamento de seus dados pessoais nas plataformas de mídias sociais.

A autoridade europeia reforçou a importância da conformidade com a proteção de dados para que as plataformas não se utilizem desses padrões escuros, estabelecendo a necessidade de observância dos princípios de licitude, transparência, minimização dos dados e prestação de contas. Essas diretrizes identificam elementos para proteção de dados que se tornam ainda mais relevantes no que diz respeito a padrões escuros.

Nesse contexto, deve ser assegurada a autonomia do titular para determinar o uso dos seus dados, além da possibilidade de interagir com o controlador. O tratamento dos dados pela plataforma deve corresponder às expectativas razoáveis do titular, e as informações e as opções de processamento de dados devem ser fornecidas de forma objetiva e neutra, evitando qualquer linguagem ou design enganoso ou manipulador (EUROPEAN DATA PROTECTION BOARD, 2022).

Por outro lado, é possível observar ações para se evitar tais tipos de práticas maliciosas, considerando a emissão dos documentos citados pelas principais autoridades de proteção de

dados do mundo. O site *Privacy Patterns* (padrões de privacidade) (2022), da UC Berkeley School of Information, é uma iniciativa para sugerir e ajudar na construção de soluções de design para esses problemas de privacidade, por meio de conselhos práticos para engenharia de software.

De acordo com o site, ao tratar especificamente sobre assimetria da informação, para ajudar os titulares de dados a compreenderem o fluxo do tratamento de seus dados pessoais, recomenda-se que as organizações limitem a quantidade de coleta de dados por padrão, invertendo a ordem e dando a possibilidade ao titular de, caso queira, aumentar o fluxo de dados. Além do mais, é essencial que as políticas de privacidade sejam claras e concisas.

> Se a quantidade de dados necessária for minimizada, os usuários terão menos coisas para entender e menos para discordar. Isso também permite políticas mais simples. Tornar as políticas mais claras e concisas também é crucial, pois os usuários não vão querer vasculhar textos prolixos para entender o que aconteceria com seus dados. Dar destaque aos aspectos importantes para os próprios usuários, em vez de deixá-los confusos com jargões jurídicos, detalhes e complexidade (PRIVACY PATTERNS, 2022, tradução livre).

Já no Brasil, embora ainda não exista nenhum documento específico da Autoridade Nacional de Proteção de Dados, foi emitida a Nota Técnica nº 49/2022/CGF/ANPD (BRASIL, 2022b), em que se analisaram as alterações promovidas na política de privacidade e nos termos de serviço do WhatsApp. Concluiu-se pela necessidade, entre outras, de aumentar a transparência para o usuário, indicar de forma precisa as finalidades do tratamento e inserir de forma destacada as informações que são compartilhadas.

O *Guia orientativo cookies e proteção de dados pessoais*, publicado pela ANPD, embora não seja de caráter vinculante, é um importante balizador do referencial interpretativo da autoridade brasileira. O *Guia* indica a utilização de banners de *cookies*, como recurso visual, para leitura destacada com a finalidade de informar ao titular de dados, de forma resumida, simples e direta, o funcionamento de cookies necessários. O guia orienta que deve ser disponibilizado botão que permita rejeitar os *cookies* não necessários:

Figura 7 - Banner de primeiro nível

Fonte: Ofício Nº 6/2022/CGTP/ANPD/PR. Disponível em: https://www.gov.br/anpd/pt- br/assuntos/noticias/sei_pr-3368186-oficio.pdf.

Figura 8 - Banners de segundo nível

Fonte: Ofício Nº 6/2022/CGTP/ANPD/PR. Disponível em: https://www.gov.br/anpd/pt- br/assuntos/noticias/sei_pr-3368186-oficio.pdf.

Além disso, o banner deverá: fornecer acesso fácil para que o titular possa exercer seus direitos; descrever as categorias de cookies de acordo com seus usos e finalidades; apresentar descrição e informações simples, claras e precisas quanto a essas finalidades, bem como disponibilizar informações sobre como realizar o bloqueio de cookies.

3.3 Falta de transparência nos avisos de privacidade

O aviso de privacidade é o instrumento vocacionado a dar transparência aos titulares sobre como seus dados serão tratados pelas organizações. A LGPD tem como seus fundamentos o respeito pela privacidade e a autodeterminação informativa (art. 2º, I e II, LGPD). Isso garante ao titular o controle sobre seus dados pessoais e, caso haja obstáculo pelos agentes de tratamento, este poderá incorrer em violação direta à LGPD. Dessa forma, as organizações poderão sofrer requisições dos titulares, conforme estabelecido no art. 18 da LGPD, além de judicialização de demandas pelo titular, individuais ou coletivas, e, ainda, fiscalização das agências reguladoras, principalmente a Autoridade Nacional de Proteção de Dados e a Secretaria Nacional dos Consumidores.

A LGPD estabelece que, para todas as atividades de tratamento, o controlador estabeleça uma base legal adequada (arts. 7º e 11, LGPD), sendo disponibilizado ao titular canal para que possa exercer seus direitos previstos nos art. 17 a 22, bem como sejam observados os princípios da lei (art. 6º). As organizações devem garantir os meios necessários para que o titular dos dados pessoais seja suficientemente informado sobre como será o tratamento.

Especificamente em relação a crianças e adolescentes, o art. 14 da LGPD estabelece que as informações sobre o tratamento dos dados sejam fornecidas de maneira simples, clara e acessível, considerando as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com o uso de recursos audiovisuais quando adequado (§6º). Além disso, o art. 55-J estabelece que a ANPD deverá garantir que o tratamento de dados dos idosos seja realizado de maneira simples, clara, acessível e adequada ao seu entendimento.

Por sua vez, o art. 52 da LGPD estabelece as sanções administrativas que poderão ser aplicadas pela ANPD. Em razão da ausência de informações completas dispostas no aviso de privacidade, desde a coleta até o descarte final dos dados pessoais, é possível a aplicação de sanções não pecuniárias (advertência, publicização da infração, bloqueio dos dados pessoais a que se refere a infração, eliminação dos dados pessoais a que se refere a infração, suspensão parcial do funcionamento do banco de dados a que se refere a infração, suspensão do exercício da atividade de tratamento de dados pessoais a que se refere a infração e proibição parcial ou total de atividades relacionadas a tratamento de dados) e sanções pecuniárias (multa de até 2% do faturamento, podendo chegar a até R$ 50 milhões por infração, sendo a multa diária).

Nesse aspecto, é bom esclarecer que a ANPD ainda não aplicou nenhuma sanção administrativa a agentes de tratamento, tendo em vista que estavam pendentes de regulamentação a dosimetria e a aplicação das sanções, tendo sido, contudo, aprovadas no dia

24 de fevereiro de 2023, através da Resolução CD/ANPD nº 4. Portanto, agora, a Autoridade Nacional já estabeleceu os critérios para aplicar as sanções previstas no art. 52 da LGPD.

De toda forma, ainda que não tenha nenhum precedente, a ANPD instaurou processo administrativo para avaliação técnica do aviso de privacidade e dos termos de uso no WhatsApp, após sua atualização em 4 de janeiro de 2021. Nessa nota técnica, a Autoridade Nacional de Proteção de Dados apresentou recomendações para adequação do aviso de privacidade do WhatsApp à LGPD. O processo administrativo ainda está em curso e poderá estar sujeito às sanções disciplinares expostas acima. Os principais pontos de atenção da ANPD foram medidas de transparência das informações e garantia dos direitos dos titulares como, por exemplo, aprimorar a experiência do usuário por meio da personalização de recursos e conteúdos (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2022).

A ANPD também emitiu recomendação para adequação do portal Gov.br quanto à sua política de cookies em relação à LGPD (Ofício nº 6/2022/CGTP/ANPD/PR) e, com base nesta recomendação, elaborou guia orientativo de *cookies* e proteção de dados sugerindo, entre outras medidas, técnicas de design tendo em vista o alinhamento aos princípios e às obrigações da LGPD.

Outro importante indicativo sobre os riscos foi apontado em estudo de Jurimetria, em que foram analisadas todas as decisões que mencionam a Lei Geral de Proteção de Dados, num total de 438 decisões durante o ano de 2022. O relatório demonstrou que 82% geram algum tipo de condenação em razão do desvio de finalidade do tratamento dos dados, e, quando essas decisões também identificam a falta de transparência adequada, o percentual sobe para 91% (OPICE BLUM, 2022).

4 INFLUÊNCIA DO *LEGAL DESIGN* PARA PROTEÇÃO DE DADOS

O conceito de design está ligado a resolução de problemas, escolha de estratégias e funcionalidades para pensar, evitar ou solucionar uma situação de conflito de interesses (COELHO; HOLTZ, 2020). O propósito do *Legal Design* está alinhado com as novas tendências advindas da tecnologia e da comunicação e com a agilidade da informação, e passou a ser difundido após a fundação do The Legal Design Lab, da Universidade de Stanford, em 2013. O laboratório foi criado e é dirigido pela professora Margaret Hagan, uma das maiores expoentes em pesquisa e aplicação de técnicas de *Legal Design.* Assim, *Legal Design* é a aplicação do design, no mundo do Direito, para tornar sistemas e serviços jurídicos mais centrados no ser humano, utilizáveis e satisfatórios (HAGAN, [*s. d.*]).

No entanto, a tomada de decisão sobre privacidade não é tão simples, o que reforça a obrigação a respeito das finalidades da coleta de informações, bem como eventuais compartilhamentos com outras organizações. A LGPD elenca como fundamento a autodeterminação informativa para designar o direito dos indivíduos de decidirem, por si próprios, quando e dentro de quais limites seus dados pessoais podem ser utilizados (DONEDA, 2021). Na prática, são comuns a coleta, o uso e o armazenamento de dados pessoais, principalmente pelas plataformas digitais, sem que o titular entenda a dinâmica desse processo de tratamento de dados, que a cada dia fica mais complexo, com o uso de algoritmos avançados e de inteligência artificial.

Diga-se, por sua vez, que o favorecimento de autodeterminação informativa, a utilização de linguagem simples e a potencialização da transparência em relação ao tratamento de dados pessoais não buscam a compreensão técnica dos titulares de dados, assim como uma bula de remédio não é vocacionada a tornar médicos os pacientes. Contudo, continuando no exemplo proposto, um paciente passa por três camadas de informações: a do médico que prescreveu o medicamento; a do enfermeiro que vendeu a medicação; e, finalmente, a da bula. Já quanto ao tratamento de dados, ordinariamente, não existem outras camadas de informação e proteção ao titular. Ressalta-se também que não é a intenção comparar o direito à saúde com o direito à proteção de dados. De toda forma, é inegável que ambos são reconhecidos como direitos fundamentais, e o tratamento indevido de dados pode gerar prejuízos impensáveis ao titular e até vieses discriminatórios que podem prejudicá-lo, ainda que silenciosamente.

Torna-se necessário, assim, equalizar o denominado “paradoxo de privacidade”, descrito pelo professor norte-americano Daniel Solove, segundo o qual de um lado existe uma forte preocupação com a privacidade e as consequências gravosas com o uso desmedido e

inadvertido dos dados pessoais, e, de outro, uma crescente superexposição de dados. Esse fenômeno é observado quando os usuários abrem mão da proteção dos seus dados pessoais em troca de um acesso imediato ao conteúdo proposto pelas organizações. Contudo, isso ocorre sem que os titulares percebam as consequências da exposição inadvertida dos seus dados.

Embora a privacidade e a proteção de dados sejam direitos fundamentais previstos na Constituição Federal, os titulares dos dados não compreendem sua importância e valor até que se vejam prejudicados numa situação real. Isso decorre da dificuldade em entender a identidade na sociedade em que estamos inseridos, na qual tecnologias disruptivas surgem em uma velocidade incompreensível, agravada pela escassez de meios para controlá-las, dentro de uma perspectiva regulatória tradicional (DONEDA, 2021). O resultado é o descasamento entre as ações dos titulares de dados e as suas escolhas em relação à sua privacidade.

O *Legal Design* faz a junção do Design, da Tecnologia e do Direito. Design, na elaboração de avisos de privacidade e na arquitetura de plataforma que ajudem os titulares a compreenderem e terem empatia com a leitura, aprimorando sua experiência. Tecnologia, para aumentar a eficácia da ação das pessoas e integrar o usuário, por meio de ferramentas, no centro do processo. E o Direito, para promover a pacificação social (MEDEIROS NETO *et al*., 2021). Dessa forma, a utilização de técnicas de *Legal Design* pode auxiliar os titulares no entendimento dos pontos controvertidos, gerando economia de tempo em suas decisões. É importante que as organizações sejam transparentes em seus documentos de privacidade, informando os titulares de forma clara e precisa sobre como serão tratados seus dados pessoais, e conscientizem os usuários sobre os riscos e benefícios do uso dos dados pessoais.

A metodologia do *Legal Design* tem como premissa a utilização do design orientado para inovação jurídica, colocando o usuário final no centro do projeto e partindo de análises de problemas reais. A inovação, diga-se, não está necessariamente atrelada a novas tecnologias e pode ser experimentada apenas através de uma forma diferente de fazer algo que é reproduzido em um mesmo formato há muito tempo.

> Uma abordagem voltada para o design para a inovação pode centrar nosso trabalho em problemas humanos reais e vividos. E oferece um conjunto claro de processos, mentalidades, e mecanismos que podem estruturar nossas tentativas de inovar – dando-nos um caminho a seguir, que nos ajudará a pensar de forma mais ambiciosa e criativa sobre como poderíamos lidar com as muitas frustrações, confusões e atritos em lei (HAGAN, [*s. d.*], tradução livre).

Apesar de ainda não haver uma metodologia uníssona sobre o que deve compor a estrutura do *Legal Design*, nas palavras dos primeiros autores a escreverem uma obra dedicada ao tema, este é definido como a aplicação de princípios e elementos de design e da experiência

do usuário na concepção e na elaboração de documentos ou produtos jurídicos. Destacam os autores que, apesar da associação quase automática entre design e arte, não basta apenas a utilização de recursos gráficos para aplicar o *Legal Design*, uma vez que o propósito do design vai muito além disso (MAIA; NYBO; CUNHA, 2020). Nesse sentido:

> Por isso é que não podemos restringir esses conceitos a uma única técnica ou simples metodologia, embora possamos nos valer dessas práticas ao longo dos projetos. Mas limitar o Legal Design a um método, neste contexto, traria uma expectativa equivocada de fórmula estanque que serve para todo e qualquer tipo de situação. Legal Design, na prática, é a busca por novas formas para solucionar problemas e desafios jurídicos, e isso vai depender do tipo de problema que se quer resolver e das múltiplas formas para se fazer isso (COELHO, BATISTA, 2021).

A vigência da Lei Geral de Proteção de Dados, desde setembro de 2020, trouxe uma nova camada protetiva aos titulares a respeito dos seus dados pessoais. A lei traz entre seus princípios a segurança e a transparência para o tratamento de dados. Contudo, na maioria dos casos, o titular dos dados acaba por dar consentimento em termos de privacidade que não lê (e não lê porque não os compreende); ou apenas dá o aceite porque entende que não tem uma opção real de escolha com relação às condições colocadas nesses termos (SOUZA; OLIVEIRA, 2021).

Usa-se, aqui, a expressão *Legal Design* não apenas como a elaboração de documentos jurídicos com inserção de gráficos ou esteticamente bonitos. É necessário atribuir valor, funcionalidade e experiência do usuário. De acordo com Margaret Hagan, *Legal Design* é a forma como avaliamos e desenhamos negócios jurídicos de maneira simples, funcional, atrativa e com boa usabilidade (HAGAN, [*s. d.*]. Assim,

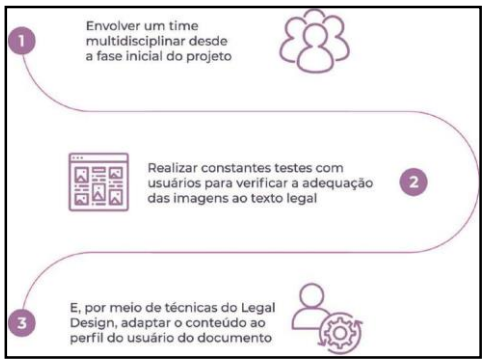
> O aviso de privacidade deve primar pela clareza, objetividade, concisão e facilidade de compreensão. O principal benefício dessa abordagem não é tão somente o estrito cumprimento da lei de proteção de dados, mas, sim, também a construção de vínculos e relacionamentos de confiança, baseados na boa-fé e transparência (SERAFINO, 2021).

A boa-fé, além de permear todas as relações do Direito moderno, em especial as que envolvem os consumidores, considerando sua posição de vulnerabilidade, também é determinada pela LGPD para o tratamento de dados pessoais, sendo elencada como o princípio da Lei. Em seu artigo 46, §2, a LGPD estabelece que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais. Estas deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. Retiramos dessa interpretação o conceito de *privacy by design*, criado pela canadense Ann Cavoukian, que representa uma mudança no modo de garantir a privacidade e a proteção de

direitos e liberdades dos indivíduos, já que é pensado e incorporado às práticas de negócio antecipadamente.

Para que os interesses dos usuários sejam visados de forma prioritária, é crucial que eles tenham real conhecimento e compreensão acerca da utilização de seus dados. Nesse sentido, o *Legal Design* auxilia na implementação do *privacy by design*, ao permitir que os usuários consigam ter acesso à informação de forma mais clara e didática. Pela utilização de recursos visuais, por exemplo, os usuários podem ter um melhor entendimento das políticas de privacidade e proteção de dados das empresas, o que garante a concessão consciente do consentimento, evitando futuros conflitos.

Figura 9 - Processo multidisciplinar



Fonte: SERAFINO, 2021, p. 39.

Além da utilização de ícones para proporcionar melhor compreensão do conteúdo, esta regra não é estanque e sua utilização deve ser analisada no contexto em que será disponibilizado ao titular; existem outras técnicas e princípios de design que auxiliam na elaboração de documentos jurídicos que se apresentam de forma mais empática ao usuário. Nesse sentido, a elaboração de avisos de privacidade, agrupando os itens mais relevantes de cada título, poderá melhorar significativamente a experiência do usuário (LOWDERMILK, 2019). O autor ainda traz o princípio da hierarquia do design, que também é perfeitamente aplicável aos avisos de privacidade, em especial para organizações que tratam dados para múltiplas finalidades.

> O princípio da hierarquia, ou hierarquia visual, estabelece que os aplicativos devem fornecer indicadores visuais para ajudar o usuário a perceber como o aplicativo está organizado. Com muita frequência, isso assume a forma de submenus e de outros elementos para navegação. Também pode ser aplicado por intermédio do uso do princípio de proximidade (LOWDERMILK, 2019).

De fato, existem várias técnicas de design que podem ajudar na elaboração do documento jurídico, contudo, não sendo uma ciência exata, sua aplicabilidade deve ser

analisada de acordo com cada perfil de usuário, produto e serviço. Conforme bem abordado pela advogada Danielle Serafino, o desafio está em criar e avaliar elementos com o objetivo de reduzir a margem de erro na interpretação dos avisos pelos usuários (SERAFINO, 2021). Essa abordagem é compatível com as novas exigências da sociedade atual que demandam por soluções mais customizadas.

> Nos anos 1960, o paradigma de fabricação industrial ainda era a produção em massa: tudo igual em grandes quantidades para todos. Hoje, a indústria caminha a olhos vistos em direção à produção flexível, com cada vez mais setores buscando segmentar e adaptar seus produtos para atender à demanda por diferenciação (CARDOSO, 2016).

Ou seja, com o desenvolvimento de novas tecnologias e a crescente legislação de proteção de dados e privacidade, não há mais espaço para que as empresas busquem apenas o cumprimento formal da lei, sem de fato demonstrar que realmente agem e respeitam os direitos dos titulares. O *privacy by design* é um importante instrumento para mudança de mentalidade e aculturamento a respeito da relevância da privacidade e da proteção de dados.

A contribuição do *Legal Design* é vocacionada a melhorar a eficiência desses produtos e serviços, bem como torná-los mais acessíveis (SERAFINO, 2022).

4.1 Importância da Linguagem Simples na elaboração de documentos

A linguagem simples é fundamental para a compreensão não só dos documentos técnicos, mas da própria comunicação atual. A pandemia de Covid-19 demonstrou o quanto é importante que informações básicas cheguem a todos os níveis da sociedade, como forma de atendimento público, para economizar tempo, agilizar processos e, principalmente, fortalecer a relação de confiança entre os interlocutores.

Linguagem simples é uma técnica de comunicação com o objetivo de tornar textos e documentos mais fáceis de ler e mais rápidos de entender (FISCHER, 2018).

É difícil a compreensão de documentos e termos jurídicos, considerando se tratar, ainda, de um segmento tradicionalmente conservador. Contudo, a tecnologia e as novas formas de comunicação têm influenciado todas as áreas do conhecimento e as classes sociais. E não é diferente em políticas e avisos de privacidade, principalmente em documentos que são direcionados a informar sobre o tratamento de dados pessoais, a finalidade desses dados, com quem são compartilhados e como os titulares podem exercer seus direitos.

Geralmente, esses textos são complexos, com termos técnicos e muitas informações em um mesmo parágrafo, o que dificulta a compreensão do conteúdo. Assim, o primeiro passo

para arquitetura de documentos inteligíveis e que cumpram com os princípios da transparência e da finalidade dispostos na LGPD é a sua estruturação em linguagem que seja acessível a todos os usuários. Para essa estruturação, existem regras e princípios da linguagem simples.

Inicialmente, é necessário utilizar palavras que sejam conhecidas pela maioria dos usuários. Posteriormente, é importante que as frases sejam curtas, para que a informação que se deseja passar seja identificada de forma rápida e precisa. Por fim, deve-se atentar para o design da informação, ou seja, para a estruturação do documento de maneira a facilitar a leitura e a localização das informações relevantes ao usuário. Devem ser levados em consideração, principalmente, os diferentes dispositivos em que os documentos serão disponibilizados, seja por escrito, seja por um computador ou smartphone.

É inegável que devemos levar em conta que estamos inseridos em uma sociedade em que as relações sociais, políticas e de direito se estabelecem pela troca de dados, ou seja, a informação. A tecnologia proporcionou a chamada sociedade sem fronteiras. O desenvolvimento tecnológico faz com que a evolução na sociedade aconteça de forma mais acelerada e, muitas vezes, sem tempo de assimilação. Esse cenário torna cada vez mais difícil garantir aos usuários o direito à privacidade e à proteção de dados. É extremamente necessária a existência de mecanismos que facilitem aos usuários a interação com esse cenário.

Por seu lado, com a transformação digital, principalmente a partir dos anos 2000, a linguagem simples ganha mais força e passa a ser reconhecida mundialmente, principalmente com a *Plain writing act* (*Lei da redação clara*), assinada por Barack Obama em 2010 (FISCHER, 2018). A demanda pela linguagem simples no Brasil intensifica-se, considerando não só as dimensões continentais do país, mas também o elevado número de pessoas com baixa ou nenhuma escolaridade (INAF, 2023). De acordo com a LGPD, as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Na sociedade da informação, em que cada vez mais a proteção de dados ganha relevância, os avisos de privacidade devem garantir o princípio da transparência comunicando as informações de forma claras, precisas e facilmente acessíveis quanto as operações de tratamento (art. 6º, VI, LGPD). Os avisos de privacidade, sendo o instrumento vocacionado para informar os titulares sobre o tratamento dos seus dados, a utilização da Linguagem Simples favorece na sua acessibilidade e compreensão para o público.

Para sua utilização é recomendável a utilização de palavras comuns e amplamente conhecidas, em substituição aos termos técnicos e uso de jargões ou “juridiquês”. A utilização

de frases curtas, diretas, e voz ativa, favorece a comunicação da informação de forma clara e objetiva, além da arquitetura de design, a depender da plataforma, para se tornar compatível e eficaz para o usuário.

Dessa forma, a utilização da Linguagem Simples, além do cumprimento do princípio da transparência disposto na LGPD, aumenta a empatia, respeito e confiança com os usuários, favorecendo a construção de uma sociedade mais justa, igualitária e promovendo responsabilidade social.

4.2 Boas práticas em *privacy by design*

A privacidade é conhecida como o direito do indivíduo de ficar sozinho e não ser incomodado. Esse direito é caracterizado como uma liberdade negativa, ou seja, de se eximir do acesso da informação pública; portanto, é um direito subjetivo. Já a proteção de dados é apresentada como uma liberdade positiva. A autodeterminação informativa possibilita ao indivíduo controlar o fluxo de suas informações pessoais. A Lei Geral de Proteção de Dados Pessoais não é vocacionada a retirar as informações disponibilizadas por anos e que, sem dúvida, culminou no desenvolvimento da sociedade da informação. A ideia é voltar para o indivíduo a sua titularidade, de forma que ele possa determinar como e, principalmente, por que seus dados trafegam pelo mundo.

Para que o indivíduo possa exercer a titularidade sobre seus dados pessoais, é necessário o design da informação de todo esse processo, permitindo a compreensão e a percepção da perspectiva coletiva desses dados. Deve-se lembrar que a LGPD possibilitou diversas outras bases legais para legitimar o tratamento dos dados, superando a ideia central de consentimento disposta no Marco Civil da Internet. Portanto, o uso do design está relacionado com a exposição de regras que processam o uso dessas informações. A aplicabilidade do design no Direito está intimamente ligada à própria concepção da palavra, em que lhe é atribuída a função de dar significado, ou seja, adequar-se a um propósito.

A LGPD, no capítulo relacionado à segurança e às boas práticas, dispõe aos agentes de tratamento (controladores e operadores) que eles deverão adotar medidas de segurança, técnicas e administrativas, desde a concepção do produto ou serviço até sua fase de execução, proporcionais ao tratamento de dados realizado. Isso também é reforçado no art. 6, VIII da LGPD, sobre o princípio da prevenção, vocacionado a modificar a forma livre e descuidada como os dados pessoais eram tratados, passando por um filtro de mitigação de riscos e construção de parâmetros e mecanismos internos para minimizar eventuais danos identificados.

Dessa forma, o procedimento de *privacy by design* está alinhado com o contexto em que a sociedade de dados está inserida, bem como com a identificação de alguma mudança de pensamento sobre as relações entre indivíduo e organizações. As leis de privacidade, *compliance* e consumidor sugerem a mudança de estado de posse dos dados pessoais, principalmente pelas *big techs*, para a titularidade dos dados pessoais à pessoa natural a que se referem, com direito amplo de acesso aos dados que pertencem a ela. Nesse ambiente, também é fortalecida a ideia de confiança nas relações comerciais, favorecendo companhias que promovem relacionamento ao invés de transações estáticas; busca-se, ainda, um cenário conveniente e informativo para as partes envolvidas.

O *privacy by design* é um instrumento para orquestrar os princípios de privacidade, viabilizando negócios que gerem confiança aos titulares. Trata-se de criar no titular a competência de aprendizado sobre como, quando e por que seus dados são coletados, e de fomentar a escolha consciente e o poder de controle sobre suas informações. A coleta de dados deve atender a uma finalidade, que deve igualmente entregar valor para o modelo de negócio. Contudo, o usuário precisa de transparência, acesso e controle sobre o uso desses dados durante sua experiência (DONEDA; MENDES; CUEVA, 2020).

É fundamental, dentro do contexto de construção dos documentos de privacidade vocacionados a informar o titular sobre o uso de seus dados pessoais, o exercício de análise sob a perspectiva dos diversos usuários daquele produto ou serviço. Por não ser uma tarefa fácil, é necessária a utilização do design para comunicar informações complexas, auxiliando no entendimento do fluxo dos dados para uma tomada de decisão mais assertiva. Além do mais, é preciso identificar melhorias sob o ponto de vista do próprio usuário, tornando sua experiência intuitiva, útil e agradável.

O desenvolvimento dessa técnica é fundamental. Ela deve ser executada com rigor, para se evitarem generalismos que não atendam ao usuário final. A identificação da persona deve respeitar os atributos relevantes e valorizados pelos clientes – o que é diferente da segmentação da base de clientes, em que existe divisão de perfis respaldada em aspectos demográficos, geográficos ou comportamentais que não conseguem atingir, em sua maioria, a necessidade do titular individualizado.

Sobre a importância da utilização de recursos visuais, a professora Viviane Maldonado destacada que esta é uma tendência iniciada na União Europeia na vigência do GDPR (MALDONADO, 2021, p.37):

Ora, como o próprio Regulamento Europeu recomenda, quando adequada, a utilização de recurso visual para os avisos de privacidade, tornou-se comum o uso de linguagem iconográfica, ou seja, a que adota o emprego de imagens e de símbolos em substituição à comunicação que se dá por meio de palavras. Esse modelo traz indiscutíveis vantagens, que vão desde a redução do tempo para leitura até a maior efetividade da compreensão, jornada essa que, inquestionavelmente, entrega uma melhor experiência ao usuário. Bem por isso, também aqui no Brasil inicia-se a utilização de elementos visuais em documentos de toda sorte, incluídos os relativos aos avisos de privacidade, e o que tenderá a crescer sobremaneira durante os processos de adequação à LGPD dentro das empresas, sejam elas públicas ou privadas.

Nesse sentido, o *privacy by design* promove a ponte entre os interesses comerciais, as exigências jurídicas e regulatórias e a expectativa do usuário. Não é incomum que o desenvolvedor de aplicativos não tenha ideia de como traduzir dispositivos legais abstratos para o caso concreto (THE CONVERSATION, 2021). Portanto, a privacidade por design vai além das políticas de privacidade, tendo sido estabelecidos sete princípios fundamentais, cunhados por Ann Cavoukian (TEPEDINO; FRAZÃO; OLIVA, 2019).

O primeiro princípio, definido como proativo (e não reativo), preventivo (e não corretivo), estabelece o compromisso da alta administração em gerar o engajamento e o patrocínio das ações ligadas à proteção de dados, traduzindo os indicadores em ações implementadas e com definição de responsabilidades para todos os agentes envolvidos no processo.

Já com base nesse primeiro princípio é possível analisar que a Lei Geral de Proteção de Dados é uma oportunidade para que as organizações entendam seus processos e fluxos de informações. Assim, além de gerar efetividade nos procedimentos internos, com as descobertas encontradas, elas podem, ainda, gerar valor quanto a diagnósticos e prognósticos mais rápidos e assertivos (THE CONVERSATION, 2021). A implementação desses padrões de privacidade favorece o engajamento dos colaboradores no cumprimento das diretivas estabelecidas, proporciona o planejamento de investimentos de forma preventiva e internaliza a cultura de inovação e proteção desde a concepção do produto, reduzindo custos com sanções regulatórias, ressarcimentos por defeitos em produtos e serviços, além de intangível dano reputacional.

O segundo princípio é conhecido como *privacy by default* (TEPEDINO; FRAZÃO; OLIVA, 2019), que quer dizer “princípio da privacidade”, padrão em que é gerada a expectativa de proteção da privacidade dos usuários de forma natural, sem que se exijam grandes conhecimentos técnicos para customizar o produto ou o serviço de forma “mais segura”. Esse

princípio exige que a finalidade do tratamento de dados seja definida e informada antes da coleta, e que exista uma limitação para o uso dos dados fora das expectativas apresentadas ao titular. Além disso, é estabelecido o prazo de retenção dos dados e as estratégias para que não sejam utilizados para outras finalidades, não informadas aos titulares.

O terceiro princípio é o da privacidade incorporada ao design, ou seja, é a aplicação do *privacy by design* em todo o ciclo de vida para análise dos impactos envolvendo privacidade e proteção de dados. Esse princípio estabelece a exigência de pesquisas e normas setoriais correspondentes, avaliação e relatório de impacto de proteção de dados e medidas de segurança ou anonimização de dados, quando pertinentes.

O quarto princípio é o da funcionalidade total (ou soma positiva diferente de zero) (BIONI *et al*., 2020). Esse princípio estimula a busca por soluções alternativas no caso de riscos à privacidade, tanto para manter a usabilidade do produto ou serviço quanto para assegurar a proteção dos dados. Atrelado a ele está o quinto princípio, que é o de segurança de ponta a ponta e proteção durante todo o ciclo de vida dos dados. Esse princípio reforça a ideia da análise do ciclo de vida dos dados, desde a coleta, o registro, a classificação, o compartilhamento e o descarte. Estabelece também a necessidade de medidas de segurança, como criptografia, forma de destruição dos dados após o esgotamento da finalidade e requisitos para compartilhamento seguro dos dados pessoais.

Quantos aos dois últimos princípios – sem prejuízo dos demais –, eles são mais relevantes para a análise do presente trabalho, uma vez que estão diretamente vinculados a formas de efetivação da proteção de dados através do design. São eles: visibilidade e transparência, e respeito pela privacidade do usuário. O princípio da visibilidade e transparência prevê que as políticas de proteção de dados sejam públicas e de fácil acesso a todos os usuários e, principalmente, que as informações sejam claras e concisas sobre o tratamento de dados, especialmente em relação à coleta, ao uso e ao compartilhamento.

Além do mais, é necessária a existência de meios de facilitar o contato com o controlador (essencialmente na pessoa do encarregado pela proteção de dados, quando houver) e de canal para exercício dos direitos dos titulares previstos nos art. 17 a 22 da LGPD. Esse princípio permeará todo o trabalho, principalmente ao tratarmos sobre a utilização de linguagem simples, a facilitação do entendimento de direitos, essencialmente de proteção de dados, e o design como facilitador para a compreensão dos avisos de privacidade.

O último princípio do *privacy by design* é o respeito pela privacidade do usuário. Esse princípio abarca todo o ciclo de privacidade do desenvolvimento do produto ou serviço e vai além, tendo em vista que fornece subsídios para que a privacidade e a proteção de dados sejam

internalizadas de forma constante. Prevê que as configurações de privacidade estejam habilitadas por padrão, as modificações em funcionalidades ou avisos de privacidade sejam comunicadas ao titular, o acesso às informações quanto à finalidade, o compartilhamento e o monitoramento sejam facilitados, além de medidas de remediação quanto aos exercícios dos direitos dos titulares.

Para estrutura do projeto, é recomendável a idealização de uma “persona”, que funciona como um avatar baseado com os dados e objetivos que a empresa pretende alcançar. Em continuidade, deve ser simulado a jornada do usuário dentro do protótipo e, por fim, a validação com base em testes. “Nessa fase é necessário buscar um equilíbrio entre o objetivo do designer de não carregar a interface com muito texto e, ao mesmo tempo, uma redação com a clareza necessária que a legislação exige”. (FERREIRA et al., 2020).

O procedimento de *privacy by design* favorece o a cultura de proteção de dados. A colocação em prática destes princípios internaliza a cultura de inovação, em conjunto a proteção de dados, desde a sua fase de concepção, reduzindo além de custos operacionais, atuando de forma preventiva ao eventual dano.

5 APLICAÇÃO DO *LEGAL DESIGN* NOS AVISOS DE PRIVACIDADE

Conforme exposto durante os capítulos anteriores, o *Legal Design* é uma metodologia vocacionada a tornar o Direito mais acessível, considerando que as leis são elaboradas para regular as relações entre toda a sociedade, não apenas aos letrados. A combinação com o design, como forma de resolver problemas, tem apresentado resultados significativos para a facilidade de compreensão dos avisos de privacidade.

Os avisos de privacidade informam aos titulares a forma como será realizado o tratamento dos seus dados. E, conforme artigo citado pela professora e advogada Danielle Serafino, o principal objetivo da utilização do *Legal Design* para os avisos de privacidade não é tão somente para cumprimento de uma obrigação legal, mas, essencialmente, para criação de um vínculo de confiança e empatia com os usuários.

Em reforço a esse entendimento, o mestre, e sempre homenageado, Danilo Doneda enfatiza que a tomada de decisão sobre privacidade não é uma tarefa simples, e que a autodeterminação informativa, enquanto fundamento da LGPD, é vocacionada a proporcionar aos titulares decidirem, por si próprios, a forma de tratamento dos seus dados.

Nesse sentido, é possível extrair a interpretação de que os avisos de privacidade não são apenas uma formalidade legal. Para o cumprimento da Lei Geral de Proteção de Dados Pessoais será necessário que esse aviso compreenda a declaração das organizações de forma clara e efetiva para os titulares, contendo a finalidade do tratamento, a garantia dos seus direitos, hipóteses de compartilhamento, entre outros. Para estar em conformidade com a LGPD, além da definição adequada de uma das bases legais previstas para o tratamento (arts. 7º e 11) e assegurar o exercício dos direitos dos titulares (arts. 17 a 22), é necessário, também, adequar o tratamento aos princípios estabelecidos (art. 6º).

O *Legal Design* pode auxiliar o titular no aculturamento da proteção de dados e auxiliar na sua tomada de decisão mais consciente. Essa transformação da forma de comunicação faz a leitura do público-alvo, para a utilização de linguagem simples e representações gráficas com o propósito de apresentar finalidade legítima, específica e explícita ao titular, além de elevar a transparência e a confiança entre as partes, sendo esta uma boa prática estabelecida pela Lei no art. 50, §2º, I, alínea “e”:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações

> específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
> § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
> e) 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).

Não é difícil verificar que os avisos de privacidade são de difícil compreensão de termos técnicos e justificativas opacas. Dessa forma, os avisos de privacidade devem informar o titular de maneira efetiva, demonstrando a ele o que (e como) será feito com seus dados pessoais, criando um vínculo de confiança e transparência. Nesse sentido:

> Mais uma vez, trata-se de buscar o equilíbrio entre os requisitos legais e a experiência do usuário, valorizada pelo próprio regulamento europeu de maneira expressa. As recomendações para superar esse desafio são: 1. Escreva conteúdo livre de jargões técnicos e concentre-se em benefícios orientados ao usuário, em vez de recursos orientados ao sistema. 2. Comunicar claramente aos usuários o que eles receberão em troca. 3. Não solicite acesso a recursos sem fornecer valor aos usuários, pois eles podem suspeitar de seu produto, serviço e marca, além dessa coleta de dados poder ser considerada excessiva pelos reguladores. 4. Evite frases vagas, como para oferecer uma melhor experiência ao usuário ao explicar por que o aplicativo requer acesso. 5. Teste suas solicitações de permissão com os usuários para descobrir se eles entendem o texto (FERREIRA; CABELLA, 2020. p. 144).

O aviso de privacidade do site da Skol é um exemplo positivo da utilização adequada da técnica do *Legal Design* identificando seu público e direcionando as informações de forma leve, íntegra e inteligível. A Figura 10 cria uma relação imediata de empatia com o usuário direcionando de forma orgânica para os pontos principais de privacidade:

Figura 10 - Aviso de privacidade Skol

Fonte: https://www.skol.com.br/politica-de-privacidade.

É possível observar na Figura 10 que a abordagem ao titular levou em consideração a categoria de usuários que fazem uso daquele determinado produto. Na sequência, o aviso já chama a atenção do usuário sobre o significado da Lei Geral de Proteção de Dados Pessoais e seus principais conceitos para a efetiva compreensão destes, em linguagem simples e direcionada ao público-alvo.

Mais adiante, o aviso de privacidade traduz um termo técnico e ainda exemplifica de forma a proporcionar ao titular a compreensão do seu conteúdo.

A utilização do *Legal Design* no aviso de privacidade da Skol evidencia que toda a sua estrutura foi pensada e direcionada ao seu público. A linguagem, a inserção não aleatória de ícones e a formatação mais fluida imputam ao usuário uma conversa sobre privacidade, totalmente diferente da experiência com um texto corrido, com linguagem padrão e sem explicações adequadas aos titulares.

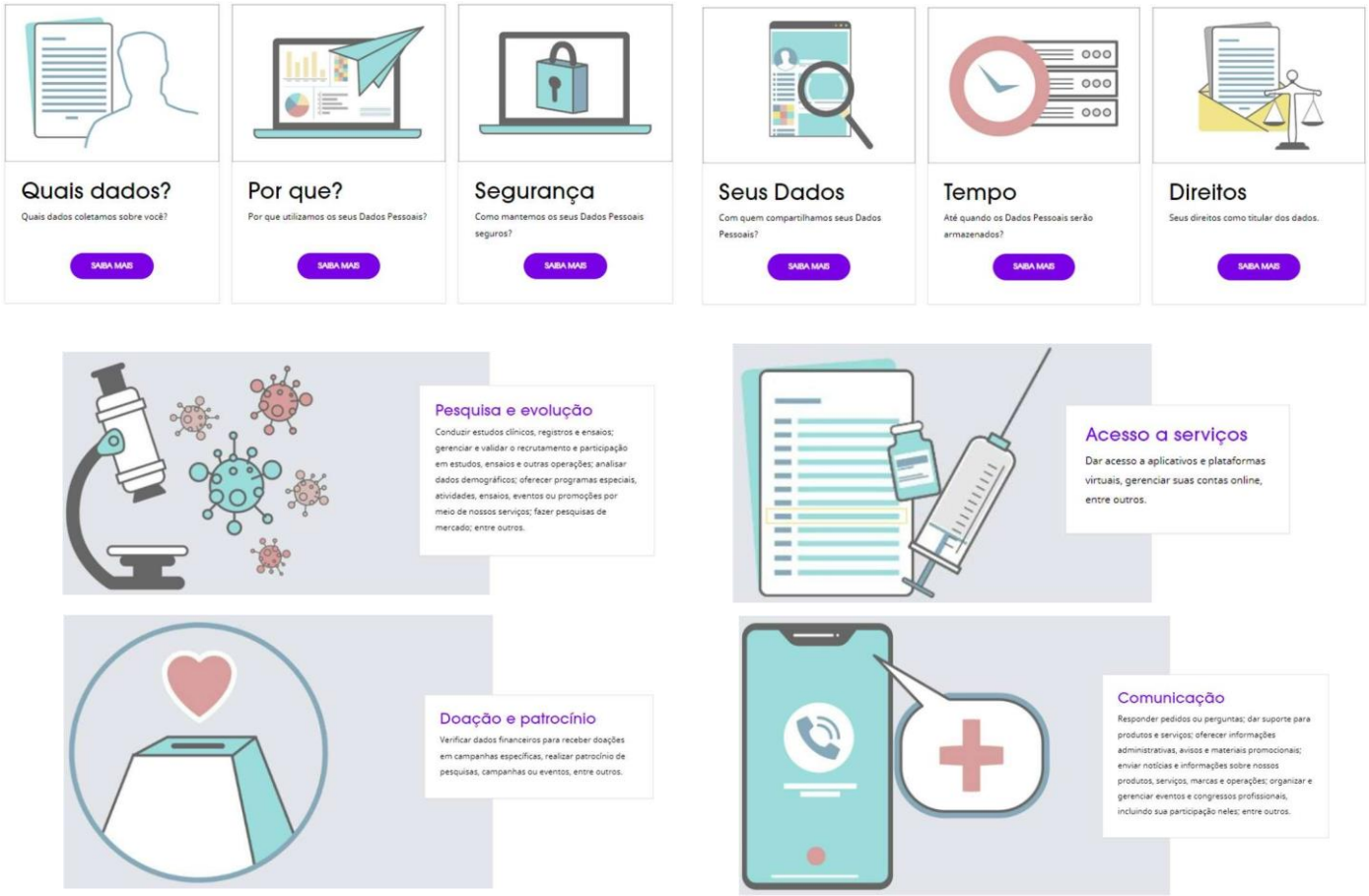
Em análise do aviso de privacidade da L'Oréal Brazil também é utilizado o *Legal Design* orientado pelo perfil do usuário da marca e informando de forma rápida e eficaz como será a forma de tratamento dos dados pessoais dos titulares.

Figura 11 - Aviso de privacidade L'Oréal Brazil

Fonte: https://www.loreal.com/en/brazil/pages/grupo/privacy-policy-brazil/.

Em outro exemplo, da empresa Sanofi, foi utilizada uma abordagem em camadas, ou seja, dividindo as informações em blocos para facilitar a localização da informação no aviso de privacidade. Além do mais, o uso de fonte e ícones em tamanho aumentado facilita a compreensão do público-alvo da organização.

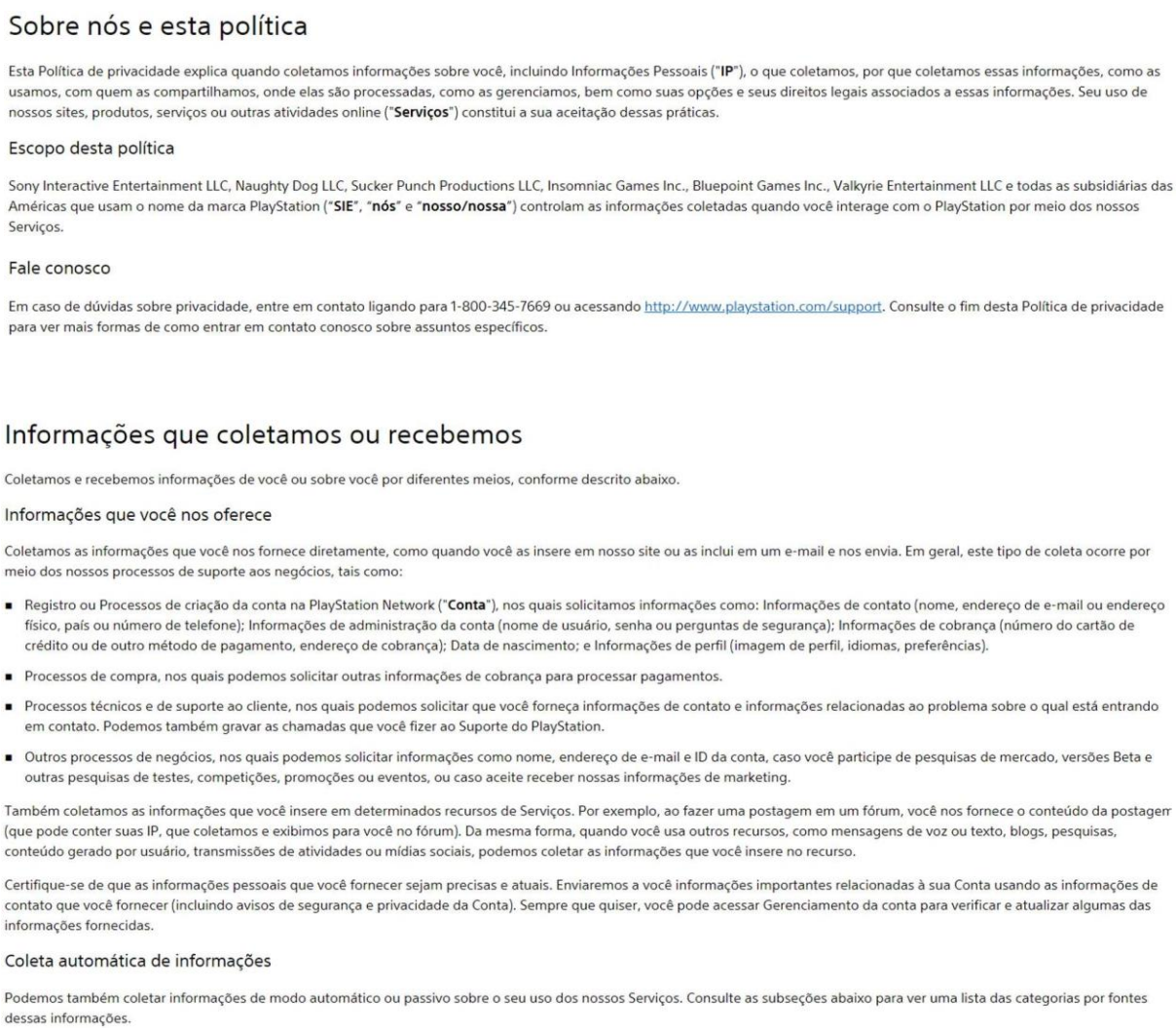
Figura 12 - Aviso de privacidade Sanofi



Fonte: https://www.sanofi.com.br/pt/politica-de-privacidade

O último exemplo é bastante elucidativo, porque nos permitiu analisar dois avisos de privacidade da PlayStation, sendo que o do site brasileiro não utilizou técnicas de *Legal Design*, já o do Reino Unido fez uma abordagem diferente, direcionada para os usuários adolescentes. Ao acessar o aviso de privacidade do Reino Unido, as informações estão na língua inglesa; assim, para facilitar a visualização, foi utilizado o recurso *Google Translate*.

Figura 13 - Aviso de privacidade PlayStation Brasil



Sobre nós e esta política

Esta Política de privacidade explica quando coletamos informações sobre você, incluindo Informações Pessoais ("**IP**"), o que coletamos, por que coletamos essas informações, como as usamos, com quem as compartilhamos, onde elas são processadas, como as gerenciamos, bem como suas opções e seus direitos legais associados a essas informações. Seu uso de nossos sites, produtos, serviços ou outras atividades online ("**Serviços**") constitui a sua aceitação dessas práticas.

Escopo desta política

Sony Interactive Entertainment LLC, Naughty Dog LLC, Sucker Punch Productions LLC, Insomniac Games Inc., Bluepoint Games Inc., Valkyrie Entertainment LLC e todas as subsidiárias das Américas que usam o nome da marca PlayStation ("**SIE**", "**nós**" e "**nosso/nossa**") controlam as informações coletadas quando você interage com o PlayStation por meio dos nossos Serviços.

Fale conosco

Em caso de dúvidas sobre privacidade, entre em contato ligando para 1-800-345-7669 ou acessando http://www.playstation.com/support. Consulte o fim desta Política de privacidade para ver mais formas de como entrar em contato conosco sobre assuntos específicos.

Informações que coletamos ou recebemos

Coletamos e recebemos informações de você ou sobre você por diferentes meios, conforme descrito abaixo.

Informações que você nos oferece

Coletamos as informações que você nos fornece diretamente, como quando você as insere em nosso site ou as inclui em um e-mail e nos envia. Em geral, este tipo de coleta ocorre por meio dos nossos processos de suporte aos negócios, tais como:

- Registro ou Processos de criação da conta na PlayStation Network ("**Conta**"), nos quais solicitamos informações como: Informações de contato (nome, endereço de e-mail ou endereço físico, país ou número de telefone); Informações de administração da conta (nome de usuário, senha ou perguntas de segurança); Informações de cobrança (número do cartão de crédito ou de outro método de pagamento, endereço de cobrança); Data de nascimento; e Informações de perfil (imagem de perfil, idiomas, preferências).
- Processos de compra, nos quais podemos solicitar outras informações de cobrança para processar pagamentos.
- Processos técnicos e de suporte ao cliente, nos quais podemos solicitar que você forneça informações de contato e informações relacionadas ao problema sobre o qual está entrando em contato. Podemos também gravar as chamadas que você fizer ao Suporte do PlayStation.
- Outros processos de negócios, nos quais podemos solicitar informações como nome, endereço de e-mail e ID da conta, caso você participe de pesquisas de mercado, versões Beta e outras pesquisas de testes, competições, promoções ou eventos, ou caso aceite receber nossas informações de marketing.

Também coletamos as informações que você insere em determinados recursos de Serviços. Por exemplo, ao fazer uma postagem em um fórum, você nos fornece o conteúdo da postagem (que pode conter suas IP, que coletamos e exibimos para você no fórum). Da mesma forma, quando você usa outros recursos, como mensagens de voz ou texto, blogs, pesquisas, conteúdo gerado por usuário, transmissões de atividades ou mídias sociais, podemos coletar as informações que você insere no recurso.

Certifique-se de que as informações pessoais que você fornecer sejam precisas e atuais. Enviaremos a você informações importantes relacionadas à sua Conta usando as informações de contato que você fornecer (incluindo avisos de segurança e privacidade da Conta). Sempre que quiser, você pode acessar Gerenciamento da conta para verificar e atualizar algumas das informações fornecidas.

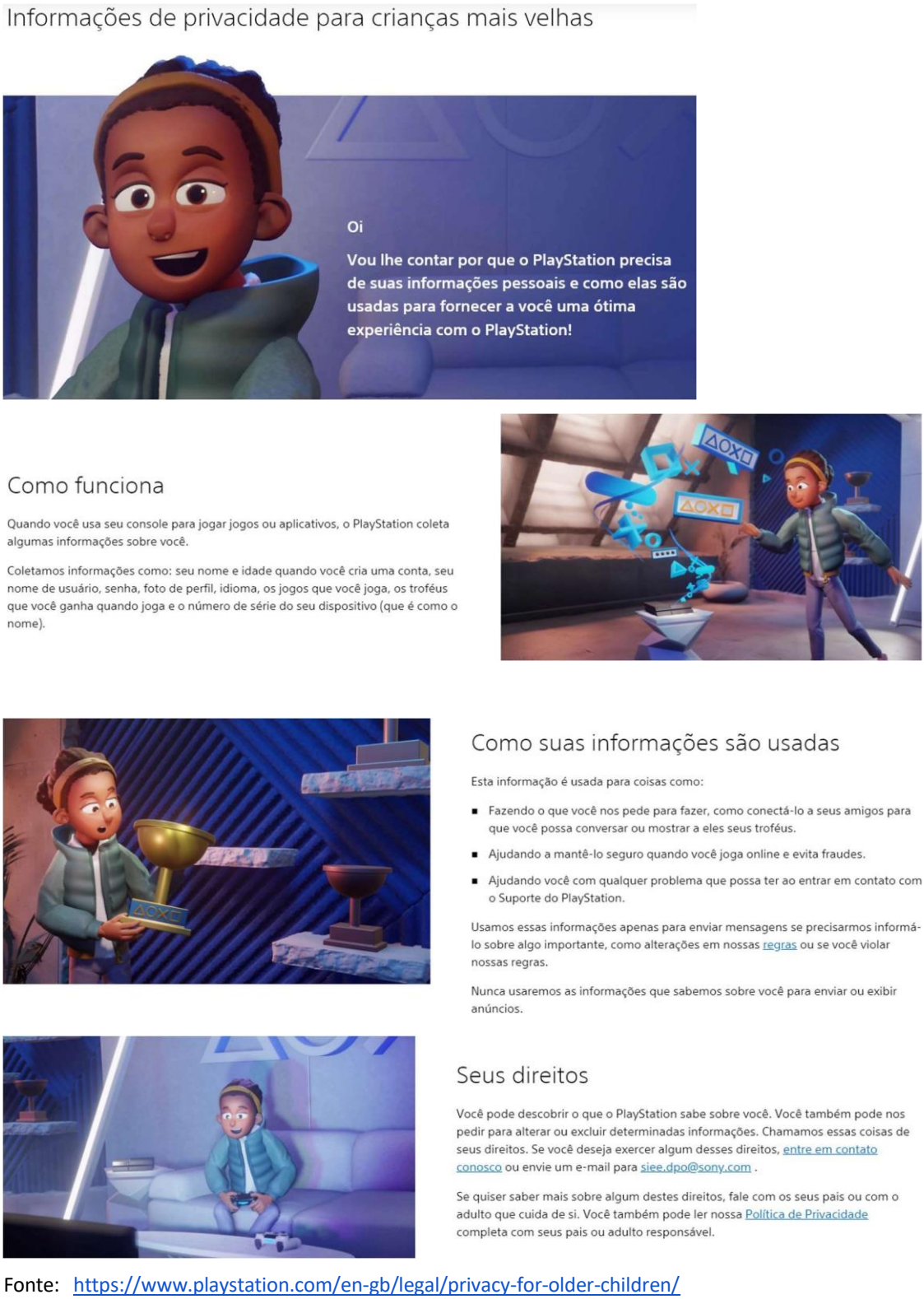
Coleta automática de informações

Podemos também coletar informações de modo automático ou passivo sobre o seu uso dos nossos Serviços. Consulte as subseções abaixo para ver uma lista das categorias por fontes dessas informações.

Fonte: https://www.playstation.com/pt-br/legal/privacy-policy/

Este aviso de privacidade pode gerar dúvidas de compreensão aos adolescentes, em razão da linguagem técnica e dos termos específicos, que não são comuns a esses usuários. Além do mais, esse documento não é atrativo e, facilmente, passará apenas por uma mera formalidade, o que é ruim, pois é importante que os adolescentes sejam devidamente informados sobre como seus dados pessoais poderão ser usados, ainda mais porque essa categoria de titulares ainda não tem o total discernimento sobre a exposição dos seus dados a longo e médio prazos, podendo impactar na sua vida pessoal e profissional.

Figura 14 - Aviso de privacidade PlayStation UK



Fonte: https://www.playstation.com/en-gb/legal/privacy-for-older-children/

A comparação entre os dois avisos de privacidade da PlayStation nos permite perceber, em primeiro lugar, a abordagem do documento que proporciona uma identificação visual com os usuários adolescentes. Em segundo lugar, percebe-se que a linguagem foi estruturada para conversar com o titular, inclusive exemplificando conceitos de forma acessível, como é feito no aviso de privacidade do Reino Unido: “Coletamos informações como: (...) os jogos que você joga, os troféus que você ganha quando joga e o número de série do seu dispositivo (que é como o nome)”. E também: “Você pode descobrir o que o PlayStation sabe sobre você. Você também pode nos pedir para alterar ou excluir determinadas informações. Chamamos essas coisas de seus direitos”.

Neste exemplo, é possível observar que a estratégia de fornecer um aviso de privacidade em uma versão simplificada, destacando os principais pontos, ajuda na compreensão e na tomada de decisão dos adolescentes.

O aviso de privacidade deve conversar com os seus usuários e deve ser estruturado de acordo com a plataforma em que será visualizado. Para ajudar o titular na sua tomada de decisão sobre privacidade, o design poderá favorecer, ou prejudicar, essa abordagem. As organizações devem buscar meios inovadores, criativos e empáticos para elaboração dos seus avisos de privacidade. Assim,

> De modo geral, o aviso de privacidade é uma forma de as organizações delimitarem a própria responsabilidade, divulgando as práticas adotadas e proporcionando a si mesmas o máximo de flexibilidade em relação ao uso dos dados do consumidor. Tendo ciência de tais limitações e das exigências do RGPD por uma maior transparência, as empresas devem explorar maneiras de oferecer avisos mais relevantes e de fácil compreensão e desenvolver novas formas de proteger a privacidade do consumidor, em vez de depender de avisos e de um controle ilusório. (NEIDITZ, 2019).

A elaboração de documentos através do *Legal Design* traduz a boa-fé das organizações em equilibrar a relação com o titular dos dados e buscar maior interação de forma transparente. Ou seja, o objetivo não é apenas disponibilizar um documento para cumprimento de um dispositivo legal; vai além, ao pretender demonstrar a responsabilidade e a preocupação da organização com a privacidade.

Para além da privacidade do titular, existem outros motivos, e vantagens, que favorecem as organizações através da criação de vínculos mais empáticos com seu público. O respeito pela privacidade considerando o usuário no centro do desenvolvimento dessas políticas pode melhorar a marca da empresa e a confiança do público, reduzir riscos de violação de dados, aumentar a receita com vendas cruzadas e marketing direto, oferecer um diferencial

competitivo, agregar valor e cumprir sua função social dentro da sociedade (DENSMORE, 2019).

CONCLUSÃO

A presente pesquisa buscou responder como o uso do *Legal Design*, aplicado nos documentos de privacidade, pode torná-los mais acessíveis e eficazes na conscientização da forma de tratamento, considerando a Lei Geral de Proteção de Dados (LGPD). Os avisos de privacidade informam os usuários das plataformas digitais a forma de tratamento dos dados pessoais coletados, finalidade, compartilhamento, prazo de retenção, entre outras disposições. Através da análise destes documentos, bem como, diversas pesquisas sobre sua eficácia, foi possível concluir que a aplicação do *Legal Design* nos documentos de privacidade torna as informações mais compreensíveis aos titulares de dados, aumentando a confiança com os agentes de tratamento e fomentando a cultura de proteção de dados.

A utilização massiva de dados pessoais, seja por órgãos estatais, seja por organizações privadas, com a utilização de tecnologias avançadas da informação, atualmente é observado como sendo um grande desafio para a garantia do direito à privacidade. Tais organismos têm se utilizado das mais diversas técnicas automatizadas, buscando obter informações em relação ao cidadão, buscando ser um tipo de influência na questão econômica, política e também social.

Cabe também mencionar que apesar de a tecnologia se desenvolver de maneira cada vez mais rápida, os princípios que vigoram no âmbito do ordenamento jurídico devem necessariamente ser respeitados dentro dessa relação de dados. Assim, os princípios da informação, da transparência e da proteção são importantes instrumentos legais que garantem a proteção de dados pessoais do titular, dos quais este pode se munir caso possua algum direito individual violado.

A questão relativa à violação de privacidade, dentro da atual sociedade da informação, deve ser compreendida em toda a sua amplitude; não basta que se observe na tecnologia o único responsável pelo problema de vazamento de dados, por exemplo. Desse modo, deve-se fomentar o debate, a respeito da proteção de dados pessoais, a partir de um viés jurídico e econômico, buscando falar a respeito das funções que a tecnologia deve assumir dentro da sociedade, sem que se exerça controle sobre ela. A proteção de dados pessoais ganha maior relevância à medida que a tecnologia tem se tornado cada vez mais presente na sociedade.

A Lei Geral de Proteção de Dados tem o objetivo de garantir aos titulares o controle sobre o fluxo de seus dados pessoais. A utilização do *Legal Design* é vocacionada em transformar informações completas, em simples, apresentando de forma acessível ao público- alvo que foi idealizado.

O presente trabalho também conseguiu concluir que, quando se fala a respeito de uma linguagem técnica própria de determinada área do conhecimento, deve-se entender que ela possui uma notória taxa de pessoas que não detém conhecimento nesta área especifica e não encontra visibilidade, o que significa que uma parcela bem pequena da população consegue compreender o que o documento está querendo dizer. A complexidade de compreensão dos documentos de privacidade se mostra como um óbice para efetivação dos direitos de proteção de dados. Da mesma forma, o *design* pode ser utilizado como ferramenta de manipulação para que os titulares de dados tomem decisão enviesadas e, até prejudiciais. O *Legal Design*, nesse sentido, possui diversas práticas que estão relacionadas a outras áreas do conhecimento, como por exemplo, linguagem simples, *design*, psicologia que, em conjunto com as demais estruturas que compõem os documentos jurídicos, possuem a capacidade de transformar este conceito.

O uso do *Legal Design* nos avisos de privacidade se mostrou uma solução eficaz para o cumprimento formal e material da Lei, dando transparência, controle e aculturamento da proteção de dados, através de documentos mais acessíveis e compreensíveis. A utilização de linguagem simples e técnicas de design tem o potencial de apresentar informações complexas de forma mais clara e intuitiva, promovendo maior confiança entre os titulares de dados. Pesquisas apontaram que o uso do *Legal Design* é uma ferramenta importante para conformidade com as normas de privacidade e proteção de dados e que deve ser estimulada.

Além disso, foi possível observar que os recursos utilizados no âmbito dessa temática têm como objetivo a sua transformação, mesmo que necessitem de uma metodologia específica para aplicação do *Legal Design*. Sobretudo, eles possuem uma finalidade construtiva, buscando fazer o embelezamento do aviso de privacidade. Essas técnicas apresentam vantagens como: redução do tempo de leitura, maior efetividade na compreensão, atração do usuário de forma empática para o documento, gerando maior confiança e cultura de proteção de dados.

Em um mundo cada vez mais digital e tecnológico, não se pode renunciar à proteção de dados, principalmente para conscientização e educação da sociedade para essa era. É inegável os benefícios da tecnologia e inovação, contudo, também trouxe novos desafios. É necessário permitir contribuições de outras áreas, para o que Direito acompanhe essas mudanças e ofereça soluções eficazes, com tecnologia e inovação, para garantir uma sociedade mais justa, equitativa e saudável.

REFERÊNCIAS

AGÊNCIA NORUEGUESA DE PROTEÇÃO AO CONSUMIDOR. Disponível em: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design.

ASSAD, Alessandra. **Liderança tóxica**. Rio de Janeiro: Edição Alta Books, 2017.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. ANPD divulga orientações aos usuários sobre a nova política de privacidade do Whatsapp. **Notícias**, 31 out. 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/a-nova-politica-de- privacidade-do-whatsapp.

BASAN, Arthur Pinheiro; PROTO, Rhaissa Souza. *Legal Design* e a utilização de nudges nos contratos de consumo. In: COELHO, Alexandre Zavaglia *et al.* **Legal design** [recurso eletrônico]: teoria e prática. Coordenado por José Luiz de Moura Faleiros Júnior, Tales Calaza. Indaiatuba: Editora Foco, 2021.

BAUDRILLARD, Jean. **A sociedade de consumo**. Lisboa: Edições 70, 2009. BENJAMIN,

Antônio Herman V. *et al.* **Código Brasileiro de Defesa do Consumidor**: comentado pelos autores do anteprojeto: direito material e processo coletivo. Volume único. Colaboração: Vicente Gomes de Oliveira Filho e João Ferreira Braga. 12. ed. Rio de Janeiro: Forense, 2019.

BENJAMIN, Antônio Herman V.; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. **Manual de direito do consumidor**. São Paulo: Revista dos Tribunais, 2016.

BESSA, Leonardo Roscoe. **O consumidor e seus direitos**: ao alcance de todos. 3. ed. Brasília: Brasília Jurídica, 2006.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. p. 155.

BIONI, Bruno *et al*. **Tratado de proteção de dados pessoais**. São Paulo: Editora Forense, 2020. E-book. p. 177.

BLUVSHTEIN, Chris. The 20 most difficult to read privacy policies on the internet. **VPNoverview**, 26 set. 2022. Disponível em: https://vpnoverview.com/research/most- difficult-to-read-privacy-policies/. Acesso em: 31 set. 2022.

BOFF, Salete Oro; FORTES, Vinícius Borges. A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. **Sequência**, Florianópolis, n. 68, p. 109-127, jun. 2014. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2177-70552014000100006&lng=en&nrm=iso. Acesso em: 1 jul. 2022.

BRANDIMARTE, L.; ADJERID, I.; ACQUISTI, A. Gone in 15 seconds: the limits of privacy transparency and control. **IEEE Security & Privacy**, v. 11, n. 4, p. 72-74, 201. Acesso em: ago. 2022.

BRASIL. Presidência da República. Lei nº 13.709. Lei Geral de Proteção de Dados Pessoais. **Diário Oficial da União**, Brasília, DF, 14 ago. 2018.

BRASIL. Presidência da República. Medida Provisória n. 954, de 17 de abril de 2020. **Diário Oficial da União**, Brasília, 14 abr. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm.

BRASIL. Presidência da República. Autoridade Nacional de Proteção de Dados. **Guia orientativo cookies e proteção de dados pessoais**. Brasília, out. 2022a. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf.

BRASIL. Presidência da República. Autoridade Nacional de Proteção de Dados. **Nota técnica nº 49**, 2022b. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt_49_2022_cfg_anpd_versao_publica.pdf.

BRASIL. Senado Federal. **Parecer sobre Projeto de Lei da Câmara nº 53.** 2018. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7751566&ts=1630450893276&disposition=inline Acesso em: 1 jul. 2022.

BRASIL. Supremo Tribunal Federal. **ADI nº 6.649/DF**. Relator: Gilmar Mendes.

BRIGNULL, Harry. Bringing dark patterns to light. **Médium**. 6 jun. 2021. Disponível em: https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf . Acesso em: 2 nov. 2022.

CALDAS, Diogo Oliveira Muniz. A liberdade de expressão, o direito ao esquecimento e a proteção da intimidade: uma análise jurídica dos conflitos na era digital. **Revista Interdisciplinar de Direito**, Faculdade de Direito de Valença, v. 17, n. 1, p.119-136, jan./jun. 2019.

CAMPOS, M. M. L. **A nuvem computacional e os contratos de serviço de armazenamento e transformação de dados regulados pelo ordenamento jurídico brasileiro**. 2019. Artigo científico Pós-Graduação Lato Sensu (Escola de Magistratura do Estado do Rio de Janeiro) – Rio de Janeiro, 2019.

CARDOSO, Rafael. **Design para um mundo complexo**. São Paulo: Ubu Editora, 2016. p. 10. E-book.

CAVALIERI FILHO, Sérgio. **Programa de direito do consumidor**. 5. ed. São Paulo: Atlas, 2019.

COELHO, Alexandre Zavaglia, BATISTA, Vynara de Souza. Design de Serviços Jurídico. In: FALEIROS JUNIOR, José Luiz de Moura; CALAZA, Tales. **Legal Design**. Indaiatuba: Editora Foco, 2021. p. 119. E-book.

COELHO, Alexandre Zavaglia; HOLTZ, Ana Paula Ulandowski. ***Legal Design*/Visual Law**: comunicação entre o universo do Direito e os demais setores da sociedade. 1. ed. São Paulo: Thomson Reuters/Revista dos Tribunais, 2020. E-book.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais. **Revista Brasileira de Direito Civil em Perspectiva**. Belém, v. 5, n. 2, p. 2-41, jul./dez. 2019.

DECEPTIVE DESIGN. **O que são padrões enganosos?**. Disponível em: https://www.deceptive.design/. Acesso em: 4 maio 2022.

DENSMORE, Russel. Introdução à Gestão do Programa de Privacidade. In: IAPP. **Privacy Program Management (Locais do Kindle 400)**. Edição do Kindle.

DESJARDINS, Jeff. How long does it take to hit 50 million users. **Visual Capitalist**, 8 jun. 2018. Disponível em: https://www.visualcapitalist.com/how-long-does-it-take-to-hit-50-million-users/. Acesso em: 24 set. 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Thomson Reuters/Revista dos Tribunais, 2021. p. 172-173. E-book.

DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas. **Lei geral de proteção de dados (Lei nº 13.709/2018)**: a caminho da efetividade: contribuições para a implementação da LGPD (p. 59). São Paulo: Thomson Reuters/Revista dos Tribunais, 2020. E-book.

DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel. **Estudos sobre proteção de dados pessoais**. Expressa Jur, 2021. p. 13. E-book.

DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JR., Otavio Luiz. **Tratado de proteção de dados**. São Paulo: Editora Forense, 2021. E-book.

EUROPEAN COMISSION. Article 29 Data Protection Working Party (WP29). Guidelines on Transparency under regulation 2016/679. **Newsroom**, 22 ago. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227. Acesso em: 2 maio 2022.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 3/2022 on dark patterns in social media platform interfaces**: how to recognise and avoid them, 21 mar. 2022. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en. Acesso em: 2 jun. 2022.

FALEIROS JUNIOR, José Luiz de Moura; CALAZA, Tales. **Legal design**. Indaiatuba: Editora Foco, 2021. E-book.

FEDERAL TRADE COMMISSION. Relatório da FTC mostra aumento em padrões escuros sofisticados projetados para enganar e prender os consumidores. FTC, 15 set. 2022. Disponível em: https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report- shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers. Acesso em: 16 set. 2022.

FERREIRA, Raissa Moura; CABELLA, Daniela Motta Monte Serrat. Escrevendo e implantando os avisos de privacidade (privacy notices) na coleta do consentimento válido. In: BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretii. **Data protection officer (encarregado)**: teoria e prática de acordo com a LGPD e GDPR. São Paulo: Thomson Reuters/Revista dos Tribunais, 2020. p. 139. E-book.

FISCHER, Heloisa. **Clareza em textos de e-gov, uma questão de cidadania**. Rio de Janeiro: Com Clareza, 2018. p. 30. E-book.

FORBRUKARRÅDET. Facebook og google manipulerer oss til a dele personinformasjon. 27 juni. 2018. Disponível em: https://www.forbrukerradet.no/siste-nytt/facebook-og-google-manipulerer-oss-til-a-dele-personinformasjon/. Acesso em: 8 out. 2020.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

GRINOVER, Ada Pellegrini *et al*. Colaboração de Vicente Gomes de Oliveira Filho e João Ferreira Braga. **Código Brasileiro de Defesa do Consumidor**. 12. ed. Rio de Janeiro: Forense, 2019.

HAGAN, Margaret. **Law by design**. [*s. d.*]. Disponível em: http://www.lawbydesign.co/en/legal-design/. Acesso em: 8 out. 2020.

HAIKAL, Beatriz; BEXKER, Daniel; GUEIROS, Pedro. Termos de uso e política de privacidade: *Design e Visual Law* como promotores do princípio da transparência. In: COELHO, Alexandre Zavaglia [et al.]. ***Legal Design***. São Paulo: Editora Foco, 2021. p. 409. E-book.

INAF. **Indicador de Alfabetismo Funcional**. 2023. Disponível em: https://alfabetismofuncional.org.br. Acesso em: 1 ago. 2022.

INFORMATION COMMISSIONER'S OFFICE. **Transparência (cookies e avisos de privacidade)**. Disponível em: https://ico.org.uk/for-organisations/sme-web-hub/frequently- asked-questions/transparency-cookies-and-privacy-notices/#whatinformation. Acesso em: 1 ago. 2022.

JIMENE, Camilla; SICUTO, Guilherme. Segurança da Informação sob a perspectiva da legislação brasileira: aspectos convergentes. In: MONTANARO, Domingo *et al*. **Cyber risk**: estratégias nacionais e corporativas sobre riscos e segurança cibernética. São Paulo: Thomson Reuters/Revista dos Tribunais, 2021. p. 55. E-book.

LOMAS, Natasha. A maioria dos avisos de consentimento de cookies da UE não têm sentido ou são manipulativos, segundo estudo. **Techcrunch**, 10 ago. 2019. Disponível em: https://techcrunch.com/2019/08/10/most-eu-cookie-consent-notices-are-meaningless-or-manipulative-study-finds/. Acesso em: 1 jul. 2022.

LOWDERMILK, Travis. **Design Centrado no Usuário**. Novatec Editora, 2019. p. 89. E- book.

LUPIÁÑEZ-VILLANUEVA, F.; BOLUDA, A.; BOGLIACINO, F., *et al*. **Estudo comportamental sobre práticas comerciais desleais no ambiente digital**: padrões obscuros

e personalização manipuladora: final relatório, Serviço das Publicações da União Europeia, 2022. Disponível em: https://data.europa.eu/doi/10.2838/859030. Acesso em: 2 jun. 2022.

MACHADO, Joana de Moraes Souza. A tutela da privacidade no controle de dados pessoais no direito brasileiro. **Arquivo Jurídico**. Teresina, v. 2, n. 2, p. 43-65, jul./dez. 2015.

MAIA, Ana Carolina; NYBO, Erik Fontenele; CUNHA, Mayara. **Legal Design**: criando documentos que fazem sentido para os usuários São Paulo: Expressa/Saraiva Jur., 2020. p. 15. E-book.

MALDONADO, Viviane Nóbrega. Avisos de Privacidade e *Legal Design.* In: OPICE BLUM, Renato. **Proteção de Dados**. São Paulo: Forense. p. 310. E-book.

MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (coord.). **LGPD**: Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters/Revista dos Tribunais, 2019. E- book.

MEDEIROS NETO, Elias Marques de; MARCATO, Ana Cândida Menezes; CASTRO, Daniel Penteado de; TARTUCE, Fernanda; COELHO, Glaucia Mara; BARIONI, Rodrigo; AMENDOEIRA JR, Sidnei (coord.). **Reflexões sobre os cinco anos de vigência do CPC/15**: estudos dos membros do Centro de Estudos Avançados de Processo - Ceapro. São Paulo: Escola Superior de Advocacia OAB SP, 2021. p. 718. E-book.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 17. ed. São José dos Campos: Saraiva Jur., 2022. p. 1059. E-book.

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

MINCKLER, V. As pessoas levam sua privacidade mais a sério do que você esperaria – as marcas também deveriam. **Think with Google**, set. 2022.

MIRAGEM, Bruno. **Curso de Direito do Consumidor**. 6. ed. São Paulo Thomson Reuters/Revista dos Tribunais, 2016.

MORAES, Alexandre de. **Direito Constitucional**. São Paulo: Atlas, 2022. p. 216-217. E- book.

NASCIMENTO, Valéria Ribas do. Direitos fundamentais da personalidade na era da sociedade da informação: transversalidade da tutela à privacidade. **Revista de Informação Legislativa: RIL**, v. 54, n. 213, p. 265-288, jan./mar. 2017. Disponível em: <http://www12.senado.leg.br/ril/edicoes/54/213/ril_v54_n213_p265>. Acesso em: 1 jul. 2022.

NEIDITZ, Jon. Direitos do Titular de Dados. In: IAPP. Privacy Program Management (Locais do Kindle 3208). Edição do Kindle.

NUNES, Rizzatto. **Curso de direito do consumidor**. 12. ed. São Paulo: Saraiva Educação, 2018.

OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS. **Spyware e vigilância**: crescentes ameaças à privacidade e aos direitos humanos, alerta relatório da ONU. 16 set. 2022. Disponível em: https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report. Acesso em: 25 set. 2022.

OLIVEIRA, Marco Aurélio Bellize; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters/Revista dos Tribunais, 2019. E-book.

OPICE BLUM, R. **Como construir avisos de privacidade aplicando técnicas de visual law**. Disponível em: https://opiceblum.com.br/wp-content/uploads/2021/02/Cartilha_Avisos-de-Privacidade_Visual_Law.pdf. Acesso em: 2 jul. 2022.

OPICE BLUM, R. **Relatório Anual de Jurimetria 2022**. [S. l.] Disponível em: https://opiceblum.com.br/wp-content/uploads/2019/07/09-relatorio-jurimetria-2022.pdf. Acesso em: 20 fev. 2023.

PAHL, Chris. Building a program that provides value: making your communication matter. **IAPP**, 29 nov. 2016. Disponível em: https://iapp.org/news/a/building-a-program-that-provides-value-making-your-communication-matter/. Acesso em: 2 maio 2022.

PALHARES, Felipe (coord.). **Temas atuais de proteção de dados** São Paulo: Thomson Reuters/Revista dos Tribunais, 2020. p. 9. E-book.

PRIVACY PATTERNS. Disponível em: https://privacypatterns.org/. Acesso em: 2 jul. 2022.

RODRIGUES, Rosemberg Augusto Pereira. Proteção de dados pessoais como um direito fundamental: O que muda em sua vida com a inclusão dessa garantia na Constituição Federal? **Serpro Notícias**, 17 fev. 2022. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2022/protecao-de-dados-pessoais-como-um-direito-fundamental.

RODRIGUES, W. C. **Metodologia científica**. Paracambi: FAETEC/IST, 2007.

ROSA, Angélica Ferreira; NUNES, Taís Zanini de Sá Duarte; ASSUNÇÃO, Nicolle Oliveira. Do direito à privacidade: análise da proteção de dados ante o advento da Lei 13.709/2018. **Conhecimento & Diversidade**, Niterói, v. 13, n. 30, p. 192-205, maio/ago. 2021.

SANTOS, Diego Ferreira dos. A proteção dos dados pessoais como nova espécie de direito da personalidade. **Revista Esmat**, [S. l.], v. 13, n. 21, p. 129–148, 2021. Disponível em: http://esmat.tjto.jus.br/publicacoes/index.php/revista_esmat/article/view/432.

SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2016. p. 15.

SERAFINO, Danielle. Ícones de Privacidade e Lei Geral de Proteção de Dados. In: SOUZA, Bernardo de Azevedo e; OLIVEIRA, Ingrid Barbosa. **Visual law**: como os elementos visuais

podem transformar o direito. São Paulo: Thomson Reuters/Revista dos Tribunais, 2021. p. 39. E-book.

SERAFINO, Danielle; CARDOSO, Paula. Legal Design e Visual Law na prática. In: VAINZOF, Rony; SERAFINO, Danielle; STEINWASCHER, Aline (coord.). **Legal Innovation**: o futuro do direito e o direito do futuro. São Paulo: Thomson Reuters/Revista dos Tribunais, 2022. p. 82.

SILVA BARBOSA, Adriana *et al*. Relações Humanas e Privacidade na Internet: implicações Bioéticas. **Rev. Bioética y Derecho**, Barcelona, n. 30, p. 109-124, 2014. Disponível em: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872014000100008&lng=es&nrm=iso. Acesso em: 1 jul. 2022.

SOUZA, Bernardo de Azevedo e; OLIVEIRA, Ingrid Barbosa. **Visual law**: como os elementos visuais podem transformar o direito. São Paulo: Thomson Reuters/Revista dos Tribunais, 2021. E-book.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet**: construção e aplicação. Juiz de Fora: Editar Editora Associada Ltda, 2016. p. 25.

SOUZA, Thiago Pinheiro Vieira de. **A proteção de dados pessoais como direito fundamental e a [in]civilidade do uso de *cookies***. 65 f. Monografia – Faculdade de Direito. Universidade Federal de Uberlândia, Uberlândia, Minas Gerais, 2018. Disponível em: https://repositorio.ufu.br/bitstream/123456789/23198/3/Prote%C3%A7%C3%A3oDadosPessoais.pdf. Acesso em: 1 jul. 2022.

TARTUCE, Flávio; NEVES, Daniel Amorim Assumpção. **Manual de Direito do Consumidor**: direito material e processual, 10. ed. São Paulo: Método, 2021.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters/Revista dos Tribunais, 2019. E-book.

THALER, Richard H.; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Editora Objetiva, 2019. p. 28.

THE CONVERSATION. A abordagem de 'privacidade por design' para aplicativos móveis: por que não é suficiente. **The Conversation**, 26 jul. 2021. Disponível em: https://theconversation.com/the-privacy-by-design-approach-for-mobile-apps-why-its-not-enough-164090. Acesso em: 8 ago. 2022.

THE NEW YORK TIMES.
https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html?mtrref=noomis.febraban.org.br&gwh=10B36FF69300AA06D9C8B52860A59CC1&gwt=pay&assetType=PAYWALL

TIROLE, Jean. **Economia do bem comum**. São Paulo: Zahar, 2020. p. 421. E-book.

TOLER, Rodrigo. *Legal Design* e a experiência do usuário no Poder Judiciário. **Análise**, 19 out. 2020. Disponível em: https://analise.com/opiniao/legal-design-e-a-experiencia-do-usuario-no-poder-judiciario. Acesso em: 2 mar. 2022.

UNIÃO EUROPEIA. Tribunal. **Pedido de decisão prejudicial**. Processo C-673/17. Relator: A Rosas. UE. Acordão de 1 out. 2019. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&do clang=EN&mode=req&dir=&occ=first&part=1&cid=1420044. Acesso em: 1 jan. 2022.

VAINZOF, Rony. Dados pessoais, tratamento e princípios. In MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Comentários ao GDPR**: regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters/Revista dos Tribunais, 2018. E-book.

VAINZOF, Rony. Disposições Preliminares. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (coord.). **LGPD**: Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters/Revista dos Tribunais, 2019. E-book.

VAINZOF, Rony; SERAFINO, Danielle; STEINWASCHER, Aline (coord.). **Legal Innovation**: o futuro do direito e o direito do futuro. São Paulo: Thomson Reuters/Revista dos Tribunais, 2022.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. 16. ed. São Paulo: Atlas, 2016.

VIEIRA, I. **Código de Defesa do Consumidor**: lei e regulamento. 6. ed. São Paulo: Lipel, 2020.

WALD, Arnold. A Contribuição do Superior Tribunal de Justiça na Consolidação do Princípio da confiança. **Doutrina do STJ** -Edição Comemorativa 15 anos, 2005.

WOODROW, Hartzog. **Privacy's blueprint**: the battle to control the design of new Technologies. Harvard: Harvard University Press, 2018.

ZONARI, Mariana Luz. Plain Legal by Design. In: VAINZOF, Rony; SERAFINO, Danielle; STEINWASCHER, Aline (coord.). **Legal Innovation**: o futuro do direito e o direito do futuro. São Paulo: Thomson Reuters/Revista dos Tribunais, 2022. p. 104.