UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE DIREITO
CURSO DE DIREITO

THAYNÁ GLENDA DE SOUSA SILVA COSTA

A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O VISUAL LAW: ANÁLISE DA UNIÃO DO DIREITO E DO DESIGN COMO MÉTODO DE VALIDADE DO CONSENTIMENTO

FORTALEZA
2023

THAYNÁ GLENDA DE SOUSA SILVA COSTA

A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O VISUAL LAW: ANÁLISE DA UNIÃO DO DIREITO E DO DESIGN COMO MÉTODO DE VALIDADE DO CONSENTIMENTO

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Sídney Guerra Reginaldo

FORTALEZA

2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

S698l Sousa Silva Costa, Thayná Glenda de.
A Lei Geral de Proteção de Dados (LGPD) e o Visual Law : análise da união do direito e do design como método de validade do consentimento / Thayná Glenda de Sousa Silva Costa. – 2023.
56 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2023.
Orientação: Prof. Dr. Sídney Guerra Reginaldo .

1. Proteção de dados pessoais. 2. Lei nº 13.709/2018. 3. Visual Law. I. Título.

CDD 340

THAYNÁ GLENDA DE SOUSA SILVA COSTA

A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O VISUAL LAW: ANÁLISE DA UNIÃO DO DIREITO E DO DESIGN COMO MÉTODO DE VALIDADE DO CONSENTIMENTO

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito.

Aprovada em: 28/04/2023.

BANCA EXAMINADORA

_____

Prof. Dr. Sídney Guerra Reginaldo (Orientador)

Universidade Federal do Ceará (UFC)

_____

Profª. Ma. Fernanda Cláudia Araújo da Silva

Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Francisco Paulo Brandão Aragão

Universidade Federal do Ceará (UFC)

A Deus.

Aos meus pais, Erika e Romulo.

Ao meu namorado, Matheus.

Aos meus professores.

Aos meus colegas e amigos.

AGRADECIMENTOS

Aos meus pais, Erika e Romulo, que sempre priorizaram minha educação e me ensinaram a colocar os meus estudos em primeiro lugar.

Ao Matheus, meu namorado, que me acompanhou e esteve sempre ao meu lado me dando apoio.

À minha segunda família, Leide, Ailton e Thiago, que me estenderam a mão quando mais precisei.

À Katherine, à Larissa, à Priscilla, ao Ramon e aos demais colegas de trabalho, que me trouxeram grandes ensinamentos pessoais e profissionais.

À Anna Clara, à Beatriz, à Claiz e à Gessica, que trilharam a trajetória na Faculdade de Direito comigo durante esses 4 anos e meio.

Ao Prof. Sídney, que participou e se dedicou à construção dessa pesquisa. Não poderia ter escolhido melhor orientador.

À EJUDI, ao NEDDIT e à Gestão Alumiá do Centro Acadêmico, que me forneceram as melhores experiências que pude ter dentro da faculdade.

À Jennyfer, à Thayná e à Rafinha, que, de modos distintos, tiveram importância nessa trajetória.

A todos vocês, muito obrigada.

“Comunicação não é o que você fala, mas o que o outro compreende do que foi dito.” (Autor desconhecido)

RESUMO

A Lei nº 13.709 - mais conhecida como Lei Geral de Proteção de Dados (LGPD) -, promulgada em 14 de agosto de 2018 e em vigor após 2 anos a contar desta data, traz o instituto do consentimento como uma de suas principais bases legais. Apesar da conjuntura histórica que originou a LGPD e a base legal do consentimento, na prática percebe-se uma dificuldade generalizada em respeitar os requisitos previstos na legislação para que o consentimento seja considerado como válido. Isso se dá, principalmente, pela ausência de uma comunicação que seja construída para o público-alvo dos documentos jurídicos de proteção de dados. Com isso, busca-se avaliar a capacidade do método do *Visual Law* como ferramenta aliada na obtenção da validade do consentimento fornecido pelo titular dos dados. Para tanto, objetiva-se, primeiramente, analisar o arcabouço histórico referente à proteção de dados pessoais ao redor do mundo e à construção deste regulamento no Brasil até a promulgação da LGPD. Em meio a essa avaliação, serão abordados os direitos à privacidade e à autodeterminação informativa, bem como o princípio da transparência, com o fito de associá-los à construção da base legal do consentimento. Em seguida, será avaliado o instituto do consentimento enquanto base legal da LGPD, bem como os seus requisitos de validade, a diferenciação de seu conceito em relação ao de autorização e as sanções administrativas que permeiam os casos de vício de consentimento. Por conseguinte, será descrita a relação que une a base legal do consentimento e o método do *Visual Law*. Tal estudo foi realizado com cunho exploratório e qualitativo, por meio de levantamento bibliográfico e revisão de literatura. Por fim, após o estudo de fundamentos e de casos concretos, serão apontadas as considerações finais sobre a união da LGPD e do *Visual Law* para fins de obtenção do consentimento válido.

Palavras-chave: proteção de dados pessoais; Lei nº 13.709/2018; visual law.

ABSTRACT

Law nº 13.709 - better known as the General Data Protection Law (LGPD) -, enacted on August 14, 2018 and in force after 2 years from this date, brings the institute of consent as one of its main legal bases. Despite the historical context that gave rise to the LGPD and the legal basis for consent, in practice there is a generalized difficulty in respecting the requirements set forth in the legislation for consent to be considered valid. This is mainly due to the absence of communication that is designed for the target audience of data protection legal documents. With this, we seek to evaluate the capacity of the Visual Law method as an allied tool in obtaining the validity of the consent provided by the data subject. To do so, the objective is, firstly, to analyze the historical framework regarding the protection of personal data around the world and the construction of this regulation in Brazil until the enactment of the LGPD. In the midst of this assessment, the rights to privacy and informational self-determination will be addressed, as well as the principle of transparency, with the aim of associating them with the construction of the legal basis for consent. Then, the institute of consent as the legal basis of the LGPD will be evaluated, as well as its validity requirements, the differentiation of its concept in relation to that of authorization and the administrative sanctions that permeate cases of defect in consent. Therefore, the relationship that unites the legal basis of consent and the Visual Law method will be described. This study was carried out with an exploratory and qualitative approach, through a bibliographical survey and literature review. Finally, after studying the fundamentals and concrete cases, the final considerations on the union of the LGPD and the Visual Law for the purpose of obtaining valid consent will be pointed out.

Keywords: protection of personal data; Law No. 13.709/2018; visual law.

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
Art.	Artigo
GDPR	General Data Protection Regulation
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados

SUMÁRIO

1	**INTRODUÇÃO ……**	**10**
2	**ASPECTOS INICIAIS SOBRE A PROTEÇÃO DE DADOS PESSOAIS: BASE HISTÓRICA, AUTODETERMINAÇÃO INFORMATIVA E TRANSPARÊNCIA ……**	**13**
2.1	**Um panorama histórico sobre a proteção de dados pessoais ……**	**14**
2.2	**Os antecedentes da proteção de dados no Brasil ……**	**16**
2.3	**Do direito à privacidade à autodeterminação informativa ……**	**20**
2.4	**O Princípio da Transparência na LGPD ……**	**24**
3	**O INSTITUTO DO CONSENTIMENTO FRENTE ÀS DEMAIS BASES LEGAIS DA LGPD, AO CONCEITO DE AUTORIZAÇÃO E ÀS SANÇÕES**	**27**
3.1	**Uma breve introdução às bases legais ……**	**28**
3.2	**O instituto do consentimento ……**	**30**
3.3	**Autorizar é sinônimo de Consentir? ……**	**33**
3.4	**As sanções da LGPD em meio ao vício de consentimento ……**	**35**
4	**O VISUAL LAW E O USO DO MÉTODO NA OBTENÇÃO DO CONSENTIMENTO ……**	**37**
4.1	**Visual Law ou Legal Design? ……**	**37**
4.2	**O método do Visual Law ……**	**39**
4.3	**O uso do Visual Law na LGPD sob a ótica do instituto do consentimento …**	**42**
5	**CONSIDERAÇÕES FINAIS ……**	**48**
	REFERÊNCIAS ……	**50**

1 INTRODUÇÃO

Com o crescimento da popularidade da internet e a evolução da tecnologia, houve uma série de mudanças nas dinâmicas sociais e nos comportamentos de consumo ao redor do mundo. Ao invés de ir a um restaurante, é possível pedir, muitas vezes, a comida do mesmo local por meio de aplicativo, assim como ao invés de se deslocar a alguma loja para comprar um determinado item, a internet disponibiliza uma variedade de sites onde é possível realizar tal compra.

Por conseguinte, o volume de tráfego de dados cresce de maneira exponencial, dado que, para que seja possível realizar tais tipos de ação, é solicitado que o indivíduo forneça algumas informações, como nome, e-mail, número do Cadastro de Pessoas Físicas (CPF) e endereço.

Em consequência, diz-se que o tipo de dado mais preocupante e, ao mesmo tempo, mais valioso é o dado pessoal[1], considerando que ele carrega informações capazes de fornecer a identificação do indivíduo em questão. Tal preocupação se agrava com o fato de, via de regra, o indivíduo não saber o que será feito posteriormente com o dado pessoal fornecido, quem terá acesso a tais informações e/ou se ele será utilizado para finalidade além da que lhe foi comunicada.

Nesse cenário, diversos países enxergaram a necessidade de alocar esforços para assegurar a proteção dos dados pessoais, inclusive em respeito aos direitos de privacidade e de liberdade que os indivíduos possuem e que vinham sendo prejudicados pelo uso e pelo compartilhamento desenfreado dos dados pessoais.

Com esse propósito, iniciou-se a elaboração de regulamentações destinadas à proteção dos dados pessoais, que avançaram nas últimas décadas para a criação de legislações específicas para tratar sobre o assunto, o que gerou grande impacto na dinâmica do tráfego de dados pessoais perante os agentes de tratamento de dados.

Sob esse contexto, após a promulgação da regulamentação europeia de proteção de dados pessoais em 27 de abril de 2016, consolidada no *General Data Protection Regulation* (GDPR), que é considerada a principal legislação no que concerne ao tema de proteção de dados, houve a promulgação da Lei nº 13.709 no Brasil em 14 de agosto de 2018. Mais conhecida como Lei Geral de Proteção de Dados (LGPD), esta Lei, que somente entrou

[1] Art. 5º Para os fins desta Lei, considera-se:
I - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável; (...)

em vigor em sua completude dois anos após esta data, introduziu as diretrizes para orientar o tratamento de dados pessoais no país.

Com a vigência da LGPD, tornou-se necessário que o tratamento de dados pessoais obedecesse pelo menos uma das hipóteses, também chamadas de bases legais, que concedem a permissão para que o tratamento seja realizado. A principal delas é a base legal do consentimento, que traz em si os reflexos do direito à autodeterminação informativa e do princípio da transparência, também previstos na LGPD. Esta base legal tem como intuito garantir que o titular dos dados pessoais tenha verdadeira ciência sobre o aceite que está sendo concedido ao agente que realiza o tratamento de seus dados pessoais.

Logo, nota-se que a LGPD tenta solucionar a preocupação de que os indivíduos forneçam dados pessoais sem a obtenção de todas as informações necessárias sobre o que será feito com tais dados, como noções de compartilhamento com terceiros, de finalidade e de armazenamento, para que possa decidir com clareza e consciência.

Todavia, embora a LGPD busque que os agentes de tratamento de dados sejam transparentes perante as operações realizadas com os dados pessoais, na prática verifica-se uma certa dificuldade em utilizar um linguajar que seja acessível nos documentos jurídicos que envolvem a coleta do consentimento e garantir que os usuários estão compreendendo aquilo com o que estão concordando.

Em meio a esta problemática, houve o surgimento do *Visual Law*, que pode ser definido como a aplicação de processos de *design* na elaboração de documentos jurídicos para melhorar seus aspectos visuais e, consequentemente, melhorar a acessibilidade destes. Tal prática pode ser utilizada em quaisquer âmbitos do direito, apesar de, na prática, ser observado mais comumente no direito contratual.

Sob esse panorama, nota-se que o uso do *Visual Law* nos documentos jurídicos que se relacionam com o tratamento de dados pessoais possivelmente aumenta a compreensão do titular que está a decidir se concorda ou não com o referido tratamento, de maneira a contribuir para maior veracidade nos casos de consentimento fornecido.

Como resultado, poderiam ser reduzidas as chances de aplicação de multas e de litígios que envolvessem o vício de consentimento, que tende a ser a base legal mais utilizada na LGPD, além de contribuir para uma maior consciência dos indivíduos perante os seus dados pessoais.

Isto posto, somado à influência do trabalho realizado em escritórios de advocacia, em startups e em demais empresas de tecnologia, esta pesquisa foi escolhida com o intuito de verificar se o *Visual Law* pode ser caracterizado como método capaz de reduzir as chances de

vício no consentimento fornecido pelo titular dos dados pessoais. Ademais, busca-se avaliar o potencial do *Visual Law* em fornecer uma maior compreensão àqueles que não possuem familiaridade com o linguajar jurídico no âmbito da LGPD.

Para tal finalidade, a presente pesquisa foi organizada e dividida em três partes. A primeira aborda o estudo feito com o objetivo de analisar se e como o arcabouço histórico que envolve a legislação de proteção de dados ao redor do mundo impactou em tal desenvolvimento no Brasil, especialmente no que diz respeito aos direitos à privacidade e à autodeterminação informativa e aos princípios que regem o tratamento de todos e quaisquer dados pessoais.

Em seguida, discorre-se sobre a base legal do consentimento, onde será feita a análise quanto aos requisitos exigidos pela LGPD, de modo a entender se há barreiras que dificultam a coleta da concordância concedida pelo titular dos dados pessoais para que seja caracterizada como livre de vício de consentimento. Além disso, também serão analisadas a construção por trás dessa base legal, os motivos que a tornam a principal base legal a ser utilizada e as diferenças entre os conceitos de consentimento e de autorização.

Por último, procura-se avaliar o método do *Visual Law* e o seu impacto nos documentos jurídicos que envolvem a proteção de dados pessoais, a fim de saber se é possível que haja uma correlação entre a base legal do consentimento e o uso do *Visual Law*, para fins de validade do consentimento, e de analisar a influência e o impacto que esta ferramenta causou em casos concretos.

A metodologia utilizada nesta pesquisa será de cunho exploratório e qualitativo, mediante levantamento bibliográfico e revisão de literatura, incluindo, mas não se limitando, trabalhos acadêmicos, artigos e doutrinas especializadas, além de pesquisa documental, decisões judiciais, legislações e demais atos normativos.

Entretanto, cabe pontuar que, apesar de as discussões sobre o tema de proteção de dados pessoais terem crescido no Brasil desde a promulgação da LGPD, o *Visual Law* ainda não é um tema amplamente debatido e, muito menos, aplicado no Brasil em comparação a outros países, como os Estados Unidos, que já possui universidades que incentivam o estudo e o debate sobre o tema, como ocorre na *Stanford Law School* e na *Northeastern University School of Law*.

2 ASPECTOS INICIAIS SOBRE A PROTEÇÃO DE DADOS PESSOAIS: BASE HISTÓRICA, AUTODETERMINAÇÃO INFORMATIVA E TRANSPARÊNCIA

A corrida pela elaboração de regulamentações sobre os dados pessoais se tornou mais acelerada com o avanço da tecnologia ao redor do mundo, o que interferiu diretamente na expansão da dinâmica econômica que era observada até então.

Sob essa ótica, Pinheiro (2021, p. 10) afirma que

> O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização.

Em meio à elaboração das redações dos mais diversos regulamentos nos últimos anos, o título de pioneirismo é destinado à Europa, que sinalizou sua atenção para com a proteção dos dados pessoais com décadas de antecedência em comparação ao restante do mundo.

A partir deste contexto, objetiva-se analisar historicamente os aspectos que influenciaram o desenvolvimento da proteção de dados pessoais no Brasil, com destaque para os direitos à privacidade e à autodeterminação informativa, e o princípio da transparência.

2.1 Um panorama histórico sobre a proteção de dados pessoais

A legislação referente à proteção de dados, apesar de recente no Brasil, já vem sendo abordada ao redor do mundo há algumas décadas. A Europa é tida como a grande pioneira na abordagem desse tema, tendo em vista que em meados de 1970 foi promulgado o primeiro ordenamento jurídico que envolveu a temática de proteção de dados, a Lei do *Land* alemão de Hesse[2].

Após esse marco, uma série de legislações e diretrizes surgiram com o intuito de regulamentar e desenvolver a proteção de dados pessoais nos demais Estados europeus, sob influência da Lei do *Land* alemão de Hesse, como a Lei de Dados na Suécia (1973) e a Lei Federal de Proteção de Dados da Alemanha (1977).

---

[2] A Lei de Proteção de Dados do *Land* alemão de Hesse, também conhecida como *The Hesse DPA*, foi promulgada em 30 de setembro de 1970, que tinha como intuito regular os bancos de dados informatizados de dados governamentais.

Porém, é a data de 27 de abril de 2016 que deve ser considerada como o marco do novo e principal capítulo no que diz respeito à matéria de proteção de dados pessoais, haja vista a promulgação do *General Data Protection Regulation* (GDPR), que substituiu a relevante Diretiva 95/46/EC[3], com o papel de unificar o direito europeu sobre proteção de dados.

Sendo assim, o GDPR se tornou o regulamento sobre proteção de dados de maior influência ao redor do mundo, principalmente porque introduziu uma série de temas que antes não eram tratados adequadamente ou que sequer eram abordados, como o direito ao esquecimento, o dever de *accountability*[4], a portabilidade de dados e a obrigatoriedade de notificação às autoridades de proteção de dados em caso de vazamento de dados.

Destaca-se que o impacto do GDPR nas demais nações não se deu exclusivamente por conta da maior robustez do dispositivo jurídico, mas também por conta da imposição de que as nações que efetuassem a atividade de compartilhamento de dados com a União Europeia também assegurassem um nível de proteção de dados adequado, conforme o Art. 45 (1) do GDPR[5].

Sob essa definição, se o Estado não apresentasse uma legislação de proteção de dados adequada, as organizações públicas e privadas seriam impedidas de realizar quaisquer tipos de operações que envolvessem dados pessoais, o que impactaria consideravelmente nas relações socioeconômicas do país. Diante disso, entende-se que o GDPR também contribuiu para catalisar a elaboração de legislações de proteção de dados nas mais diversas nações, segundo Fonseca (2021, p. 30), gerando uma espécie de "efeito dominó".

Consoante a essa afirmação, tem-se a anulação do acordo EU-US Privacy Shield, que havia sido firmado entre a União Europeia e os Estados Unidos em 2016 para tratar sobre a transferência de dados pessoais de usuários, pelo Tribunal de Justiça da União Europeia em 2020[6]. A justificativa apresentada pela União Europeia era de que o acordo em questão não

---

[3] A Diretiva 95/46/EC estabeleceu um conjunto de regras que tratavam sobre a atividade de processamento de dados, independentemente do meio onde ela ocorra, o que se mostrou uma novidade em comparação aos demais ordenamentos, convenções e *guidelines* anteriores.

[4] O princípio da *accountability* ou da prestação de contas (termo menos usual) não é um princípio exclusivo da proteção de dados, mas ganhou notoriedade nas legislações sobre o tema ao ser utilizado para incentivar a necessidade de os agentes de tratamento de dados serem responsáveis pela implementação dos requisitos de conformidade de privacidade e proteção de dados, e capazes de demonstrar a adoção de programas de conformidade adequados ao cumprimento das normas jurídicas.

[5] Art. 45. Transferências com base numa decisão de adequação.
1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica. (...)

[6] Justiça europeia anula acordo UE-EUA sobre transferência de dados pessoais; decisão afeta gigantes como Facebook. **O Globo**, 16 de julho de 2020. Disponível em:

era suficiente para garantir níveis de proteção de dados adequados, como previsto pelo Art. 45º (1) do GDPR.

A partir disso, alguns estados norte-americanos passaram a ter suas próprias legislações de proteção de dados, como ocorre na Califórnia, com o *California Consumer Privacy Act* (CCPA), e no Colorado, com o *Colorado Privacy Act* (CPA), para se adequarem à nova dinâmica mundial no que se refere ao tratamento de dados pessoais.

Cabe reforçar que, apesar disso, os Estados Unidos ainda não possuem uma legislação abrangente sobre proteção de dados, embora existam leis federais aplicáveis a cenários específicos, como o *Children's Online Privacy Protection Act* (COPPA). A COPPA regulamenta o tratamento de dados pessoais de crianças menores de 13 anos por operadoras de serviços de Internet e sites, de modo a impor a necessidade de coleta prévia do consentimento dos pais.

Desta forma, o impacto da promulgação do GDPR não poderia ser diferente no Brasil. Em 14 de agosto de 2018 foi promulgada, no ordenamento jurídico brasileiro, a Lei nº 13.709, popularmente conhecida como Lei Geral de Proteção de Dados ou LGPD, a qual entrou em vigor apenas em agosto de 2020. A LGPD tem como objetivo regulamentar o tratamento dos dados pessoais e proteger, principalmente, os direitos fundamentais de liberdade e de privacidade previstos na Constituição da República Federativa do Brasil.

Com forte influência do GDPR, a LGPD carrega uma série de similaridades com a legislação europeia, de modo que ambas acumulam semelhanças em aspectos de definição de dados pessoais, escopo territorial, princípios de tratamento, direitos do titular dos dados e bases legais para tratamento.

No entanto, as discussões no Brasil referentes à temática de proteção de dados não foram iniciadas com a promulgação do GDPR, apenas potencializadas, visto que o país já havia dado alguns passos a caminho da criação desta legislação.

2.2 Os antecedentes da proteção de dados no Brasil

Mesmo que a LGPD seja encarada como novidade legislativa no Brasil, é possível afirmar que o país deu início a caminhada no que concerne ao tema de proteção de dados sete

---

https://oglobo.globo.com/economia/tecnologia/justica-europeia-anula-acordo-ue-eua-sobre-transferencia-de-dados-pessoais-decisao-afeta-gigantes-como-facebook-24535366

anos antes, em meados de 2011, de maneira que tais leis também contribuíram para a construção da LGPD.

Por essa razão, ainda que seja uma temática recente no país, pode-se perceber uma certa familiaridade da população brasileira com termos como "dados pessoais" e "proteção de dados", por mais que não conheçam o significado deles. Por esse ângulo, Danilo Doneda, no livro de coordenação de Bioni (2020, p. 29), afirma que

> É muito recente a incorporação do termo "proteção de dados pessoais" ao glossário jurídico brasileiro, o que se deu principalmente na esteira do debate que antecedeu a promulgação da Lei Geral de Proteção de Dados. No entanto, questões que hoje associamos diretamente à proteção de dados não eram, de forma alguma, estranhas à práxis jurídica no País. Esses fenômenos foram, por muito tempo, associados a questões referentes seja à privacidade, ao direito do consumidor, a outras liberdades individuais, entre outras vinculações – o fato é que é muito recente no Brasil o elemento indutor que, finalmente, organizou em torno da proteção de dados toda uma verdadeira "fenomenologia" jurídica comportada por situações jurídicas nas quais o elemento principal ou determinante diz respeito a um tratamento de dados pessoais.

Entre as leis que antecederam a LGPD e que podem ser consideradas parte da trilha de proteção de dados, tem-se que uma das primeiras foi a Lei nº 12.414, promulgada e vigente em 9 de junho de 2011, também conhecida como Lei do Cadastro Positivo, que regulamentou a formação e a consulta a bancos de dados que continham informações de adimplemento para fins de formação de histórico de crédito.

A Lei do Cadastro Positivo é interessante sob a ótica da proteção de dados porque, antes mesmo de sofrer as modificações implementadas pela Lei Complementar nº 166, de 8 de abril de 2019, que trouxe alterações que envolveram a proteção de dados pessoais como conhecida atualmente, já demonstrava alguns entendimentos que foram preservados na LGPD, principalmente no que diz respeito aos direitos da pessoa cadastrada.

A título ilustrativo, em 2011 a Lei nº 12.414/2011 já previa que o uso dos dados pessoais deveria ocorrer exclusivamente para atendimento da finalidade para a qual foram coletados e que o armazenamento e o objetivo do tratamento dos dados pessoais deveriam ser informados previamente. Ou seja, a Lei do Cadastro Positivo apresentou alguns dos primeiros indícios de uma preocupação jurídica no que diz respeito à proteção dos dados pessoais do titular.

Ainda em 2011, houve a promulgação da Lei de Acesso à Informação (LAI), Lei nº 12.527, em 18 de novembro, a qual entrou em vigor 6 meses após sua publicação, que regulamentou o direito constitucional de acesso dos cidadãos a informações públicas, incluindo dados pessoais.

Cabe citar que o ponto mais marcante da LAI no que tange à proteção de dados foi a previsão de disposição que abordava sobre o modo como as informações pessoais deveriam ser tratadas, incluindo menção expressa à coleta do consentimento, nos termos do Art. 31[7], de modo a carregar semelhanças com o que a LGPD prevê em sua redação.

No ano seguinte, em 30 de novembro de 2012, houve a promulgação da Lei nº 12.737, popularmente conhecida como Lei Carolina Dieckmann, a qual teve seus dispositivos vigentes 4 meses após sua publicação, que, entre outras disposições, estabelece o crime de invasão de dispositivo informático[8] no Código Penal.

---

[7] Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
I - Terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
II - Poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
§ 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.
§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:
I - À prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
II - À realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
III - ao cumprimento de ordem judicial;
IV - À defesa de direitos humanos; ou
V - À proteção do interesse público e geral preponderante.
§ 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.
§ 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

[8] **Invasão de dispositivo informático**
Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
I - Presidente da República, governadores e prefeitos;
II - Presidente do Supremo Tribunal Federal;
III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Ainda que a Lei Carolina Dieckmann esteja situada na seara criminal, ela carrega uma relação direta com a esfera da proteção de dados ao tipificar uma conduta que envolve a segurança, incluindo de dados pessoais, no ambiente virtual.

Ademais, cabe mencionar que a Lei nº 12.737/2012 recebeu o nome da atriz por conta de um caso ocorrido com a mesma, no qual um *hacker* invadiu o seu computador pessoal, acessando e divulgando fotos pessoais de cunho íntimo na internet, o que também faz parte do rol de dados pessoais[9].

Já em 2014, no dia 23 de abril, foi promulgada a Lei nº 12.965, mais conhecida como Marco Civil da Internet, a qual entrou em vigor 2 meses após sua publicação, que foi de suma importância para a chegada da LGPD, dado que, a despeito de não ter um conteúdo que abordava a matéria de proteção de dados pessoais propriamente dita, introduziu e reiterou uma série de direitos, fundamentos, definições e princípios que conversam com o âmbito da proteção de dados.

Além disso, o Marco Civil da Internet também trouxe artigos que tratam especificamente de dados pessoais, embora estejam associados à seara de conexão e aplicação de internet, como o disposto no *caput* dos Arts. 10 e 11[10], de forma que contribuiu para uma espécie de preparo para o ordenamento jurídico brasileiro à chegada da LGPD.

Outrossim, 4 anos após o surgimento do Marco Civil da Internet houve a promulgação da LGPD, porém, antes de adentrar nesta legislação, faz-se importante mencionar o evento ocorrido no início de 2018 que foi tido como um impulsor para a existência das legislações de proteção de dados, acelerando a promulgação da LGPD no mesmo ano.

O evento em questão se trata do escândalo de privacidade da Cambridge Analytica, empresa de análise de dados envolvida com a campanha de Donald Trump para presidência dos Estados Unidos em 2016, ocorrido em meados de março de 2018.

Nessa ocasião, a Cambridge Analytica realizou a compra dos dados pessoais de usuários do Facebook coletados por um aplicativo, chamado *thisisyourdigitallife*, para fins de teste de personalidade. Contudo, este aplicativo utilizou uma brecha na política do Facebook

---

[9] Lei Carolina Dieckmann: Você sabe o que essa lei representa? **Fundação Escola Superior do Ministério Público (FMP)**, 16 de agosto de 2021. Disponível em: https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/. Acesso em: 14 jan. 2023.

[10] Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. Art. 11. 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.

que permitia a coleta de dados pessoais dos amigos do usuário por aplicativos externos. Como consequência, a Cambridge Analytica teve acesso a dados pessoais, como nome e profissão, de cerca de 50 milhões de pessoas sem o consentimento delas, que foram utilizados para fins de propaganda política[11].

Desse modo, o escândalo em questão contribuiu para uma maior preocupação da população com relação aos seus próprios dados pessoais, gerada por insegurança e desconfiança para com aqueles com quem compartilha suas informações, principalmente pelo envolvimento do Facebook, devido à sua popularidade e ao seu reconhecimento mundial. Vieira (2019, p. 11) reforça esse entendimento ao retratar que "Desde então, quem temia ter as suas atividades vasculhadas no uso da internet ou quem simplesmente não queria se expor nas redes e nem compartilhar seus dados pessoais passou a se sentir inseguro e desconfiado".

Por conseguinte, percebe-se que a LGPD foi fruto de uma série de acontecimentos e legislações que desembocaram em sua criação e contribuíram para que algumas noções basilares de extrema importância para o âmbito da proteção de dados já fossem introduzidas antes mesmo de sua promulgação, como a ideia de consentimento e de tratamento de dados pessoais.

Vale ressaltar que isso não significa que a LGPD é uma lei finalizada e que não necessita de complementos, nem que o Brasil já possui uma cultura forte de proteção de dados, mas sim que alguns conceitos indispensáveis e característicos da LGPD não foram introduzidos por ela, apenas popularizados e/ou abordados com maior profundidade.

Dito isso, a LGPD também carrega alguns conceitos que são ainda mais primitivos do que os apresentados, tanto no Brasil, quanto em outros países, e que carregam em si parte da essência do que significa a proteção de dados e estão diretamente associados à base legal do consentimento, como os direitos à privacidade e à autodeterminação informativa.

2.3 Do direito à privacidade à autodeterminação informativa

No cerne da construção de uma preocupação referente à proteção de dados pessoais, há a presença do direito à privacidade como um de seus conceitos basilares, sendo

[11] Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. BBC News Brasil, 20 de março de 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751.

essencial para entender a estrutura sobre a qual a proteção de dados foi fundamentada, o que é corroborado pelo entendimento de Mendes (2014, p. 32), que afirma que

> A disciplina da proteção de dados pessoais emerge no âmbito da sociedade de informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados *per se*, mas a pessoa que é titular desses dados.

Assim, o direito à privacidade, que faz parte do rol de direitos da personalidade, encontra reforço na LGPD como um dos fundamentos que disciplina a proteção de dados pessoais[12], além de ser tratado como um dos direitos fundamentais da Constituição da República Federativa do Brasil[13].

Aliás, interessante mencionar que o direito à proteção dos dados pessoais, que exerce correlação com o direito à privacidade, foi adicionado à Constituição da República Federativa do Brasil, mediante a promulgação da Emenda Constitucional 115/2022[14], lhe concedendo o status de direito fundamental.

Tal inclusão é um grande marco para o ramo da proteção de dados ao passo em que firma o compromisso e a seriedade em prol desta proteção, o que reforça a previsão constitucional do direito à privacidade, bem como a essencialidade de tais direitos, inclusive, como meios de possibilitar o direito à liberdade e o princípio da dignidade.

No que diz respeito ao direito à privacidade, este tem seu marco datado de 1890, quando o artigo *The right to privacy*, de Samuel Warren e Louis Brandeis, foi publicado nos Estados Unidos. Esse artigo trouxe a junção de uma série de decisões judiciais sobre a matéria de privacidade, que em conjunto resultavam na ideia do *right to be let alone* e do *right to privacy*, ou seja, o direito de ser deixado só e o direito à privacidade, respectivamente, popularizando o termo "privacidade" na seara jurídica.

Entretanto, o conceito de direito à privacidade ainda é bastante discutido, devido à ausência de clareza quanto ao significado de privacidade no âmbito jurídico. Nessa perspectiva, Leonardi (2011, p. 48) alude que

---

[12] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - O respeito à privacidade; (...)

[13] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)
X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (...)

[14] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)
LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022)

> Dependendo do doutrinador consultado, encontram-se conceitos abrangentes ou restritivos de privacidade. Assuntos como liberdade de pensamento, controle sobre o próprio corpo, quietude do lar, recato, controle sobre informações pessoais, proteção da reputação, proteção contra buscas e investigações, desenvolvimento da personalidade, autodeterminação informativa, entre outros, são excluídos ou incluídos, de acordo com a definição adotada.

Vale enfatizar que o direito à privacidade sofre ainda mais dificuldades em ter sua conceituação bem delimitada perante a nova roupagem apresentada em meio a um contexto tecnológico, o que é reforçado no artigo de Warren e Brandeis. Isso ocorre devido às novas dinâmicas sociais, uma vez que com a velocidade do acesso à informação, a vida privada e a intimidade se tornaram cada vez mais difíceis de serem preservadas, ainda mais sob um cenário em que as redes sociais estão cada vez mais populares.

Dito isso, Hirata (2017) observa que a própria ação de adicionar informações pessoais nas redes sociais em demasia, também se configura como uma espécie de ameaça à privacidade, tendo em vista a possibilidade de se extrair um perfil de comportamento do indivíduo, bem como demais dados pessoais que, a priori, o titular não cogitou que seriam acessados.

Em complementaridade ao exposto por Hirata, tem-se o entendimento de Doneda (2019, *E-book*) que afirma que o direito à privacidade como sinônimo de "direito de ser deixado só"

> não permite mais determinar parâmetros para avaliar o que ela representa em um mundo no qual o fluxo de informações aumenta incessantemente, ao mesmo tempo em que o desenvolvimento da tecnologia aumenta as oportunidades de realizarmos escolhas que podem influir diretamente em nossa esfera privada.

Entretanto, o cerne deste estudo não é tratar sobre as discussões e a amplitude do significado de direito à privacidade, razão pela qual é adotado o conceito apresentado por Leonardi (2011, p. 67), semelhante à corrente defendida por Alan Westin, autor do livro *Privacy and Freedom*, de que "O atributo básico do direito à privacidade seria, portanto, a capacidade de o indivíduo controlar a circulação de informações a seu respeito".

Por conseguinte, Santos (2019, p. 34) reforça que

> (...) a privacidade, em si, seria um conceito associado não só a individualidade, mas também ao interesse coletivo, uma vez que as regras inerentes ao íntimo moldam e impõem limites ao convívio em sociedade, relacionando-se, portanto, ao interesse coletivo.

Logo, percebe-se que o conceito de direito à privacidade envolve não somente a noção de que o indivíduo possa decidir sobre se, como, quando e quais informações pessoais

poderiam ser compartilhadas, como também o interesse coletivo, já que traz reflexos diretos na sociedade.

Todavia, a existência desse direito em meio ao campo de proteção de dados por vezes não é suficiente para garantir que de fato a vida privada será respeitada, ao passo em que o seu conceito ultrapassa a seara de proteção de dados. Assim, surge o direito à autodeterminação informativa, que faz o papel de aliado do direito à privacidade, sendo inclusive um reforço para garanti-lo.

Nesse sentido, o direito à autodeterminação informativa também não é recente no ordenamento jurídico brasileiro, muito menos ao redor do mundo, sendo o marco oficial de seu surgimento datado de dezembro de 1983, com o Tribunal Constitucional da Alemanha.

Tal surgimento se deu num contexto em que era permitida a realização de pesquisas de porta em porta referentes à coleta de dados pessoais dos cidadãos na Alemanha, os quais eram obrigados a responder sob o risco de incidência de multa. Em meio a essa coleta, os cidadãos se sentiram incomodados e invadidos pelos questionamentos, dada a ausência de clareza sobre a finalidade e sobre o destino que esses dados pessoais teriam após o uso[15].

A partir disso, originou-se uma reclamação que foi apreciada pelo Tribunal Constitucional da Alemanha, sendo a pesquisa declarada inconstitucional, pois foi considerado que ela invadia injustificadamente os direitos fundamentais dos indivíduos e gerava uma insegurança no uso futuro dos dados pessoais obtidos.

Para tanto, segundo trecho extraído do julgado do Tribunal Constitucional da Alemanha[16]

> aquele que, com segurança suficiente, não pode vislumbrar quais informações pessoais a si relacionadas existem em áreas determinadas de seu meio social, e aquele que não pode estimar em certa medida qual o conhecimento que um possível interlocutor tenha da sua pessoa, pode ter sua liberdade consideravelmente tolhida.

Entende-se, pois, que a autodeterminação informativa foi introduzida com o objetivo de buscar justamente que o indivíduo tenha o direito de decidir, de modo livre e independente, sobre a utilização, a finalidade e o descarte de seus dados pessoais. Ao traçar um paralelo com a legislação brasileira, tem-se que o não cumprimento desse direito afetaria o

---

[15] SCHWABE, Caroline. Right to informational self-determination. **Robin Data GmbH**, 02 de abr. de 2021. Disponível em: https://www.robin-data.io/en/data-protection-academy/wiki/right-to-informational-self-determination.

[16] Este trecho foi traduzido livremente por Menke (2015, p. 211). A decisão original pode ser acessada na íntegra em: http://www.servat.unibe.ch/dfr/bv065001.html.

direito à liberdade, que é um direito fundamental previsto pela Constituição da República Federativa do Brasil, conforme Art. 5º.

Dito isso, a autodeterminação informativa pode ser caracterizada como o direito que todo indivíduo tem de exercer controle sobre seus próprios dados pessoais, a fim de garantir-lhe a faculdade de decidir se o dado poderá ser objeto de tratamento, bem como quando e para que ele será utilizado.

Tal direito se caracteriza como um dos elementos mais essenciais da LGPD, dado que ele influencia substancialmente na própria lógica de proteção de dados ao determinar que o titular dos dados pessoais tenha autonomia e controle sobre o tratamento que lhes será dado.

Assim, percebe-se que o julgamento ocorrido em 1983 gerou um impacto de grande amplitude, uma vez que se tornou pilar das legislações de proteção de dados ao redor do mundo, recebendo nova relevância na conjuntura jurídica em que está inserido sob o ponto de vista da proteção de dados.

Nesse aspecto, Sombra (2020, *E-book*) afirma que

> Com a magnitude da capacidade de processamento de dados proporcionada pela big data e o *data analytics*, a autodeterminação informativa será o elemento crucial para que os demais direitos tenham uma matriz axiológica sempre voltada aos melhores interesses dos titulares dos dados pessoais.

Para tanto, a LGPD demonstra uma preocupação em trazer em sua redação a previsão de alguns direitos dos titulares que também possuem o papel de efetivar a autodeterminação informativa enquanto um dos fundamentos da Lei, como o direito de confirmação da existência de tratamento, de acesso aos dados e de informação quanto às entidades públicas e privadas com as quais o controlador realiza uso compartilhado de dados, previstos no Art. 18, I, II e VII.

Percebe-se, pois, que há uma certa dificuldade em tratar o direito à privacidade e o direito à autodeterminação informativa separadamente num contexto que se refere à proteção de dados. Aliás, nota-se que ambos possuem um papel fundamental na própria estruturação da essência da LGPD, não sendo possível tratar sobre esta Lei sem sequer abordar alguns dos conceitos abarcados por tais direitos.

Em congruência, Ruaro, Rodriguez e Finger (2011, p. 64) entendem que “para além da defesa da privacidade, o que se protege e regula, a partir de suas proposições, é o direito de acesso e o poder de controle a informações pessoais, muitas vezes que tangenciam o caráter individualista de privacidade”.

Outrossim, tais direitos também impactam diretamente na construção da base legal do consentimento, mas não são os únicos, de modo que se faz necessário destacar o papel de alguns princípios e fundamentos que a LGPD aborda em sua redação, principalmente o princípio da transparência.

2.4 O Princípio da Transparência na LGPD

A LGPD é classificada eminentemente como uma lei de caráter principiológico, ou seja, uma lei que fixa diretrizes e princípios fundamentais para determinados cenários ou relações jurídicas.

De inegável importância, a LGPD introduziu uma série de princípios que norteiam a estruturação do tratamento dos dados pessoais, os quais estão previstos em seu Art. 6º, devendo a atividade de tratamento de dados pessoais observar, além da boa-fé, os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Entre os princípios elencados, um dos de maior relevância para a formação da essência da proteção de dados é o princípio da transparência. Tal princípio guarda correlação direta com os direitos à privacidade e à autodeterminação informativa ao passo em que ele contribui como um dos responsáveis pela efetivação de ambos. Isso porque, se a LGPD busca tutelar direitos fundamentais, como os direitos supracitados, não há como garanti-los sem que haja o fornecimento e o conhecimento das informações necessárias de modo transparente para com o titular dos dados pessoais.

Em análise semelhante, Rony Vainzof, no livro de coordenação de Maldonado e Blum (2019, *E-book*), afirma que "Os três primeiros princípios dispostos na LGPD (*finalidade*, *adequação* e *necessidade*) são umbilicalmente conexos, formando, juntamente com a *transparência*, o cerne dessa norma jurídica". Para tanto, percebe-se que o princípio da transparência pode ser considerado um dos pilares que rege o próprio ordenamento de proteção de dados.

Todavia, este princípio não é novidade no sistema jurídico, porquanto encontra previsão em outras legislações, como no Código de Defesa do Consumidor, em seu Art. 4º[17], o qual reforça a necessidade de fornecimento de informações corretas e claras ao consumidor.

[17] Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios: (...)

Sob este ponto de vista, Lima (2020, p. 84) afirma que

> Portanto, o princípio da transparência é funcionalizado pelo direito/ dever de informar, uma vez que é tal interação que expurgará qualquer tipo de deslealdade na projetada relação de consumo, a ponto de racionalizar as próprias decisões do consumidor, pois "somente a vontade racional: a vontade realmente livre (autônoma) e informada, legítima, isto é, tem o poder de ditar a formação, e, por consequência, os efeitos do contrato entre consumidor e fornecedor", permitindo-lhe tomar uma decisão refletida.
> À mesma conclusão se chega analisando o sistema de proteção de dados pessoais, isto é, nos marcos regulatórios acima mencionados, bem como na LGPD brasileira, o princípio da transparência sempre menciona o direito do titular dos dados de ser amplamente informado.

Chinellato e Morato, no livro de coordenação de Bioni (2020, p. 654), reforçam e apresentam o entendimento de que "Parece-nos que o binômio transparência-informação deve estar sempre presente na interpretação das leis e resta subjacente ao consentimento informado, um dos pilares da LGPD".

Para tanto, de acordo com a LGPD, em seu Art. 6º, VI, o princípio da transparência significa fornecer a "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial", o que vai ao encontro do que o GDPR dispõe em seu Considerando 58[18] e corrobora com a influência que esta norma causou na criação da LGPD.

Em outras palavras, o princípio da transparência requer que haja clareza, precisão e acessibilidade na linguagem utilizada para alcançar o objetivo de permitir que o titular tenha a devida compreensão sobre o tratamento dos dados pessoais com o qual está concordando.

Vale ressaltar que, de acordo com Rony Vainzof, no livro de coordenação de Maldonado e Blum (2019, *E-book*), "Para fins de mitigação de riscos, é importante que os controladores considerarem os titulares sempre vulneráveis quanto ao entendimento das infinitas possibilidades de tratamento, notadamente quando ocorrer por meios digitais (...)".

---

[18] (58) O princípio da transparência exige que qualquer informação destinada ao público ou ao titular dos dados seja concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado.
Essas informações poderão ser fornecidas por via eletrónica, por exemplo num sítio web, quando se destinarem ao público.
Isto é especialmente relevante em situações em que a proliferação de operadores e a complexidade tecnológica das práticas tornam difícil que o titular dos dados saiba e compreenda se, por quem e para que fins os seus dados pessoais estão a ser recolhidos, como no caso da publicidade por via eletrónica.
Uma vez que as crianças merecem proteção específica, sempre que o tratamento lhes seja dirigido, qualquer informação e comunicação deverá estar redigida numa linguagem clara e simples que a criança compreenda facilmente.

Isso é devido ao déficit informacional que é ocasionado pela velocidade nas mudanças num mundo cada vez mais tecnológico, incluindo o próprio tratamento dos dados pessoais.

Outrossim, os agentes de tratamento devem apresentar as informações referentes ao tratamento dos dados pessoais da maneira mais eficiente e eficaz possível, devendo se preocupar em evitar ou mitigar as chances de haver um *Information Overload*[19], também conhecido como sobrecarga de informação, que possa dificultar a compreensão do leitor e, assim, frustrar a tentativa de obediência ao princípio da transparência.

Cabe mencionar que, em caso de infrações e litígios, havendo acusações e provas de ausência de preocupação com o princípio da transparência, além de respingar em outros fundamentos e princípios previstos pela LGPD, poderá ser considerado indício de má-fé, reduzindo as possibilidades de sanções mais brandas.

Por fim, tamanha é a importância do princípio da transparência que já houve grandes litígios que envolveram a ausência de transparência do polo passivo. A título exemplificativo, a Autoridade Francesa (CNIL) interpôs uma ação contra o Google que gerou uma sanção de €50 milhões, devido, entre outros motivos, à ausência de suficiente transparência[20].

Tal acusação foi baseada na dificuldade de acesso dos usuários às informações mais relevantes sobre os seus dados pessoais e na pouca compreensão sobre a base legal que era verdadeiramente utilizada pelas operações de processamento para a personalização de anúncios, entre outras.

Com isso, é possível observar que tanto o princípio da transparência, quanto o direito à privacidade e o direito à autodeterminação informativa, têm grande relevância na compreensão sobre a essência das legislações de proteção de dados. Contudo, para além dos pilares da LGPD, estes também interferem diretamente nas bases legais previstas pela legislação, principalmente no consentimento.

---

[19] A sobrecarga de informação, que também pode ser abordada como sinônimo da Síndrome da Fadiga por Informação (IFS), trata do fenômeno no qual um indivíduo é exposto a uma quantidade de informações acima do que é capaz de suportar e assimilar. A gravidade desse estado sob a ótica da proteção de dados reside no fato de que a tomada de decisão do titular fica comprometida, gerando uma sobrecarga cognitiva, além de impactos na saúde física e mental do indivíduo.

[20] The CNIL's restricted committee imposes a financial penalty of 50 million euros against GOOGLE LLC. European Data Protection Board, 21 de jan. de 2019. Disponível em: https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en.

3 O INSTITUTO DO CONSENTIMENTO FRENTE ÀS DEMAIS BASES LEGAIS DA LGPD, AO CONCEITO DE AUTORIZAÇÃO E ÀS SANÇÕES

Sabe-se que o rol de dados pessoais é muito mais amplo do que o senso comum tende a considerar, já que para ser classificado como tal basta que um dado seja capaz de causar a identificação de um indivíduo a depender do contexto em que ele está inserido.

Nessa lógica, Teixeira e Guerreiro (2022, p. 17) explicam que

> Tem-se a falsa impressão de que apenas dados pessoais diretos, como nome e documentos pessoais, poderiam identificar uma pessoa. Entretanto, alguns outros dados são capazes de identificar uma pessoa a depender das circunstâncias, são os chamados dados pessoais indiretos, como, por exemplo, a geolocalização, que a princípio não é um dado pessoal, mas que em determinado momento pode levar à identificação de um único indivíduo, tornando-se nesse caso um dado pessoal.

Dada a tamanha quantidade de possíveis dados pessoais que podem ser coletados de um mesmo indivíduo, faz-se necessário que haja um controle sobre as ações que podem ser feitas com ele. Contudo, para que esse controle seja viável, é necessário primeiro que o motivo pelo qual o dado pessoal foi coletado seja válido, pois, do contrário, todo o restante do tratamento também não será. A esse motivo, a LGPD dá o nome de base legal.

Sob essa ótica, o presente capítulo objetiva realizar uma análise sobre o instituto do consentimento, mediante introdução às bases legais da LGPD, com foco no consentimento, seguida pela diferenciação dos conceitos de consentimento e de autorização, e encerrada pelas sanções submetidas às situações de vício de consentimento.

3.1 Uma breve introdução às bases legais

Para que o controlador e o operador possam realizar a atividade de tratamento é necessário que esta esteja enquadrada em pelo menos uma das hipóteses previstas na LGPD que legitimam o tratamento dos dados pessoais, sob risco de este ter caráter de ilicitude. Assim, o controlador dos dados pessoais deve realizar o apontamento de qual hipótese, também chamada de base legal, será utilizada como fundamento para justificar o tratamento daqueles dados pessoais.

Vale ressaltar que, ainda que baste o atendimento de apenas uma base legal, a LGPD permite que haja cumulatividade entre elas. Além disso, a lista de bases legais prevista na LGPD é taxativa, não exemplificativa, de modo que obrigatoriamente a atividade de tratamento de dados precisa estar enquadrada em uma das hipóteses listadas.

Nesse aspecto, de acordo com o Art. 7º da LGPD, há 10 bases legais que permitem o tratamento dos dados pessoais, sendo elas:

a) o consentimento do titular;
b) o cumprimento de obrigação legal ou regulatória pelo controlador;
c) a execução de políticas públicas, convênios ou instrumentos congêneres pela administração pública;
d) a realização de estudos por órgão de pesquisa;
e) a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular seja parte;
f) o exercício regular de direitos em processo judicial, administrativo ou arbitral;
g) a proteção da vida ou da incolumidade física do titular ou de terceiro;
h) a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
i) o legítimo interesse do controlador ou de terceiro, quando necessário, exceto se houver o prevalecimento de direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; e
j) a proteção do crédito.

Imprescindível citar que em circunstância de tratamento de dados pessoais sensíveis[21], as bases legais para execução de contrato ou afins (f), legítimo interesse (i) e proteção de crédito (j) não poderão ser utilizadas, já que sequer encontram previsão como hipóteses no Art. 11. Por outro lado, acrescenta-se como base legal a garantia da prevenção à fraude e à segurança do titular em processos de identificação e autenticação de cadastro em sistemas eletrônicos, nos termos do Art. 11, II, g.

No entanto, faz-se relevante frisar que grande parte das bases legais são, via de regra, aplicáveis em casos excepcionais e que trazem em si circunstâncias muito específicas, nas quais a LGPD concede a permissão ao agente de tratamento para que este possa abdicar da coleta da manifestação de aceite do titular dos dados.

Segundo Pinheiro (2021, p. 18)

> A linha mestra para o tratamento de dados pessoais é o consentimento pelo titular, que deve ser aplicado aos tratamentos de dados informados e estar vinculado às finalidades apresentadas. No entanto, pode haver situações de exceção em que o

[21] Art. 5º Para os fins desta Lei, considera-se: (...)
II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (...)

> tratamento de dados pessoais ocorre sem necessidade de consentimento expresso, com finalidade específica declarada pelo titular (...).

Ainda em ideia similar, Rony Vainzof, no livro de coordenação de Maldonado e Blum (2019, *E-book*), reitera que o consentimento "(...), em razão do alto grau de transparência perante o titular, é a hipótese que pode trazer mais segurança jurídica para o controlador (...)".

Por fim, Mendes e Fonseca, no livro de coordenação de Bioni (2020, p. 91), entendem que

> Ao longo das últimas cinco décadas, muitas das discussões relacionadas à regulação da privacidade e da proteção de dados pessoais destinaram bastante foco em torno do consentimento expressado pelo titular dos dados. Nesse sentido, não é exagero afirmar que o consentimento tem figurado como instrumento regulatório central e núcleo de legitimidade prática desse regime protetivo.

Nota-se, pois, que o consentimento, além de ser a base legal mais conhecida, atua como uma das mais importantes da LGPD. Nesse aspecto, de acordo com Krieger (2019, p. 36) "O consentimento surge, portanto, como um instrumento do indivíduo que possibilita o exercício da sua autodeterminação informativa, cabendo a ele anuir (ou não) com a coleta e tratamento de suas informações".

No mesmo sentido, tem-se Malheiro (2017, p. 41), que reitera que

> A fundamentação do consentimento, portanto, reside na possibilidade de autodeterminação em relação aos dados pessoais, e ela deve ser levada em conta como elemento principal para a caracterização tanto da natureza jurídica do consentimento como para os efeitos desse consentimento.

Percebe-se, portanto, que tamanha relevância se dá porque, mesmo que não exista hierarquia entre as bases legais, o consentimento tem relação direta com o próprio fundamento que origina a proteção de dados pessoais, pois trata justamente do aceite concedido pelo titular dos dados para que o agente realize as atividades de tratamento que lhe couberem de modo protetivo até chegar o momento do descarte ou de o titular de dados retirar o consentimento concedido, salvo exceções, de acordo com o Art. 18, VI e IX da LGPD[22].

---

[22] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...)
VI - Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; (...)
IX - Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

3.2 O instituto do consentimento

De acordo com o Art. 5º, XII, da LGPD, consentimento significa a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Destarte, percebe-se que a LGPD atribuiu à base legal do consentimento três requisitos específicos para que a manifestação de concordância seja encarada como válida, devendo ela ser livre, informada e inequívoca.

Sob essa ótica, Vidigal (2021, p. 46) disserta que

> ainda que seja pressuposto de que a previsão do consentimento seja uma proteção conferida ao indivíduo, cabendo a ele mesmo ter cautela quanto à sua concessão, verifica-se que a qualificação do consentimento exige providências por parte do agente de tratamento, que deve fornecer condições para que ele possa ser manifestado de forma "plena".

Para tanto, o primeiro requisito apresentado é que a manifestação seja livre, ou seja, que o titular não pode ser obrigado a conceder o seu consentimento, bem como este não pode ser fornecido automaticamente, como ocorre em caso de padronização de caixa de texto pré-selecionada.

Além disso, o conceito de manifestação livre também reverbera na possibilidade de o titular escolher não dispor de dados que não sejam de fato imprescindíveis para o fornecimento de um produto ou prestação de um serviço.

Desse modo, dada a inspiração da LGPD no GDPR, é possível traçar como paralelo o disposto no Considerando 42 ao afirmar que "Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado"[23].

A exemplo disso, é possível citar o caso de lojas on-line que solicitam dados pessoais como o número do Registro Geral (RG) do titular como requisito obrigatório para que ele possa realizar uma compra na loja, mesmo quando o número do CPF, que por si seria suficiente, já foi fornecido para fins de identificação e/ou de requisito para envio do produto adquirido.

Nesse cenário, percebe-se que por mais que o número do RG não seja um dado pessoal imprescindível para o fornecimento do produto, o titular é obrigado a fornecer esse dado em troca de poder realizar uma compra na loja. Ora, se o titular não pode deixar de

[23] **RGPD (GDPR) - Regulamento Geral sobre a Proteção de Dados - Considerando 42**. Disponível em: https://gdpr-text.com/pt/read/recital-42/.

fornecer um dado pessoal que não é necessário para o fornecimento de um produto ou prestação de um serviço, então não se pode afirmar que houve consentimento do titular já que ele forneceu o dado pessoal para obter o produto ou serviço em questão, de maneira que não há caracterização de livre manifestação.

No que diz respeito ao segundo requisito, ou seja, que a manifestação fornecida pelo titular seja informada, o intuito é garantir que o indivíduo tenha compreensão sobre com o que está concordando para que a escolha do aceite seja feita conscientemente e livre de vícios causados pelas informações passadas pelo agente de tratamento.

À vista disso, Fonseca (2021, p. 85) afirma que

> (...) para que o consentimento seja válido, precisa ser claro, explícito, coletado de forma transparente, com o titular dos dados de posse de todas as informações sobre o que será feito com os seus dados, bem como eventuais consequências de não consentir no seu tratamento.

Logo, é perceptível a correlação direta entre a manifestação informada, o direito à autodeterminação informativa e o princípio da transparência, visto que para que este requisito seja alcançado é preciso mostrar que o titular recebeu a informação transmitida de jeito claro, simples e inteligível, para que o indivíduo possa decidir se irá conceder o seu consentimento ou não.

Outrossim, entre as informações necessárias referentes às atividades de tratamento de dados, tem-se a disponibilização da finalidade, da forma, da duração e das responsabilidades dos agentes que realizarão o tratamento, bem como dos direitos do titular, das informações sobre compartilhamento de dados e identificação e informações de contato do controlador, conforme apresentado no Art. 9º da LGPD, sob risco de o consentimento ser tido como nulo[24].

Por fim, o terceiro requisito é que a manifestação seja inequívoca, o que, em outras palavras, significa que o agente precisa coletar o consentimento do titular de maneira que não haja dúvidas sobre a aceitação das condições em questão por ele.

Tal requisito demanda que o agente de tratamento de dados realize o devido armazenamento do consentimento fornecido pelo titular, tanto para fins de comprovação de aceite, quanto do conteúdo vinculado àquela manifestação, independentemente do modo

---

[24] 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: (...)
§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. (...)

como ela foi apresentada, seja por áudio, por clique em botão ou por digitação de “Eu concordo com os termos”.

Outro caso seriam as manifestações de concordância que são refletidas por meio de uma simples ação do titular, como o fornecimento do e-mail abaixo de uma mensagem de “Deixe o seu e-mail para receber novidades e conteúdos exclusivos”.

Vale ressaltar que, ainda que não haja uma definição da LGPD quanto ao modo como o consentimento foi concedido, o agente de tratamentos deve se preocupar em escolher um modo que permita a comprovação, não apenas dos pontos já levantados, como também de que foi o próprio titular quem concedeu os dados pessoais e não um terceiro, tendo em vista, principalmente, as dificuldades em obter essa garantia no meio digital.

Esta interpretação e preocupação no que diz respeito ao modo como o qual o consentimento foi concedido em sua redação é reforçada pela LGPD. Exemplo disso, é a previsão de obrigatoriedade de cláusula separada das demais em se tratando de consentimento fornecido por escrito, com o fito de aumentar a probabilidade de o titular dos dados ter ciência sobre o conteúdo vinculado ao aceite que foi fornecido, sendo de responsabilidade do controlador o ônus da prova referente a este consentimento, nos termos do Art. 8º, §§ 1º e 2º[25].

Ademais, pertinente mencionar que, para dados pessoais sensíveis, o instituto do consentimento recebe uma roupagem ainda mais robusta, ao passo em que não basta que ele seja concedido em manifestação livre, informada e inequívoca, de modo que esta também necessita que seja específica e destacada, conforme Art. 11, I.

Para tanto, a manifestação específica se refere ao conhecimento prévio pelo titular do propósito do tratamento de dados em questão determinado pelo controlador, antes mesmo da ocorrência da coleta. Já a manifestação destacada exige que o titular tenha pleno e efetivo acesso a documento que esclareça os fatos relevante sobre o tratamento de seus dados pessoais, incluindo o destaque do trecho que trata sobre o assunto, com o fito de garantir o acesso do titular ao seu conteúdo, de acordo com Lima, no livro de coordenação de Maldonado e Blum (2019, *E-book*).

Com isso, percebe-se que o legislador reforça que haja uma maior cautela para com a atividade de tratamento de dados pessoais sensíveis, com o fito de sempre preservar o

[25] Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

direito à autodeterminação informativa e o princípio da transparência aplicados à base legal do consentimento.

3.3 Autorizar é sinônimo de Consentir?

Ainda que a LGPD traga explicitamente o conceito do instituto do consentimento em sua redação, faz-se fundamental estabelecer a diferenciação entre este e o conceito de autorização, visto que a Lei em questão faz menção ao termo "autorizações genéricas" para associar ao consentimento declarado como nulo.

De acordo com o Art. 8º, § 4º, "O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas". Isso significa que para que o consentimento seja revestido de licitude, é vedado o uso de autorização genérica e/ou universal no enquadramento desta base legal, pois se pressupõe a ausência de informações relevantes ao titular dos dados, indo de encontro ao princípio da transparência e ferindo o requisito de que a manifestação seja informada.

Desse modo, reitera-se que o agente de tratamento de dados não pode apenas se preocupar em obter o mero aceite do titular, mas também com o que está sendo repassado ao titular de dados e a maneira como o aceite foi concedido, sob o risco de este perder a sua validade. Fonseca (2021, p. 85), por esse lado, segue ao dizer que

> (...) não será considerado consentimento válido a concordância genérica com um enorme e obscuro termo de consentimento, no qual as principais informações estão diluídas ao longo do texto, sem destaque, não atendendo à boa-fé e à transparência que devem nortear o processo de tratamento de dados pessoais.

Nessa perspectiva, uma pesquisa realizada pelo InternetLab em 2018 apresentou o nível de cuidado de 13 aplicativos governamentais (Bolsa Família, Caixa, CNH Digital, ANATEL Consumidor, FGTS, DENATRAN, Meu INSS e SNE, da Administração Pública federal, e CPTM Oficial, EMTU, Metrô SP, Nota Fiscal Paulista e SP Serviços, da Administração Pública Estadual de São Paulo) no que diz respeito ao tratamento dos dados pessoais.

Como resultado, a pesquisa identificou que entre os 13, 6 aplicativos coletam o aceite do usuário titular dos dados mediante consentimento genérico, utilizado para todo e qualquer dado disponível no seu celular. Além disso, vale ressaltar que 4 aplicativos sequer

solicitavam algum tipo de consentimento do usuário, de modo que apenas 3 aplicativos coletavam o devido consentimento[26].

Dessa forma, Melo e Boulos, no livro de coordenação de Tomasevicius Filho (2021, p. 73), reiteram que "Evidentemente, um consentimento genérico, que permita ao aplicativo coletar todo e qualquer tipo de dado, sem prévio esclarecimento quanto às razões de coletar cada um, foge ao 'consentimento informado' preconizado pelo Marco Civil da Internet (...)".

Outrossim, a confusão entre os conceitos de autorização e de consentimento se agravam quando se trata da LAI, visto que essa Lei traz em seu Art. 31, § 1º, II a previsão do instituto do consentimento associado ao termo "autorização" ao afirmar que as informações pessoais "poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem".

Por essa razão, faz-se pertinente diferenciar ambas as situações. Apesar de a LAI não especificar o conceito de consentimento, o cenário mais conservador possível seria adotar a definição prevista pela LGPD, dado que esta é a legislação destinada ao tratamento da matéria de proteção de dados.

Nessa perspectiva, primeiramente, tem-se que o termo "consentimento" possui significado distinto a depender do ponto de vista que está a ser retratado. O primeiro sentido é de "consentimento" enquanto base legal, definido, portanto, nos termos do Art. 5º, XII da LGPD. A segunda definição seria a mesma prevista em um dicionário qualquer, enquanto manifestação favorável a que alguém faça algo ou de que se aprova algo, podendo ser utilizado como sinônimo de aceite, permissão ou concordância.

Nessa lógica, o termo "autorização" pode ser utilizado como sinônimo de "consentimento" no caso do segundo significado, porém, enquanto base legal, seria temeroso utilizar o termo com equivalência, já que a LGPD prevê nomenclaturas e definições bem estabelecidas no rol taxativo de bases legais, sem trazer o termo "autorização" como uma possibilidade de sinônimo.

Aliás, a LGPD diferencia expressamente "consentimento" de "autorização genérica" ao tratá-los como antônimos em seu Art. 8º, § 4º, bem como traz o termo "autorização específica" ao se referir ao compartilhamento de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, nos termos do Art. 5º, XVI.

---

[26] ESPECIAL | Por que se preocupar com o que o Estado faz com nossos dados pessoais? **InternetLab**, 21 de maio de 2018. Disponível em: https://internetlab.org.br/pt/noticias/especial-apps-do-governo/.

Com tais menções, é possível inferir que a LGPD traz o termo “autorização” como uma espécie de sinônimo para manifestação de concordância ou aceite do titular, podendo ser utilizado, portanto, como parte da definição da base legal do consentimento, mas não como igual.

Por conseguinte, ao se falar de “autorização específica” não quer dizer que automaticamente se trata da base legal do consentimento, pois não há relação com os demais requisitos do consentimento, como a manifestação livre e inequívoca, por mais que carregue semelhanças com a manifestação informada.

Em contrapartida, falar de “autorização genérica” como sinônimo de “consentimento genérico” não está equivocado, pois ao utilizar “consentimento genérico” não está a se falar do consentimento enquanto base legal, mas sim como uma palavra que tem significado similar a de outras como aceite, concordância e autorização.

Portanto, tem-se que “consentimento”, enquanto base legal, e “autorização” são termos que não se confundem, mesmo que o segundo possa ser utilizado para explicação do primeiro ou para tratar de “consentimento” numa definição geral. Tal diferenciação é relevante pois a falta de compreensão sobre a diferença entre eles pode custar a validade do consentimento concedido pelo titular.

3.4 As sanções da LGPD em meio ao vício de consentimento

A LGPD prevê em seu Art. 8º, §§ 3º e 4º, a explícita vedação ao vício de consentimento, bem como a nulidade do consentimento se houver aceite genérico para o tratamento de dados pessoais.

Uma situação concreta de aceite genérico pode ser apresentada no ocorrido em meados de abril de 2022, que, a despeito de não se tratar especificamente de proteção de dados, aplica-se o mesmo princípio desta seara. Na situação concreta, um homem faleceu após ser submetido a uma cirurgia sobre a qual os médicos não forneceram as informações devidas, claras e precisas sobre os riscos envolvidos.

Em meio aos fatos apresentados, o tribunal julgou que o consentimento concedido pelo paciente foi comprometido pela ausência de informações, reforçado pelo fato de os médicos não terem conseguido provar o contrário, o que independia de haver assinatura de termo de consentimento por escrito[27].

---

[27] BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.848.862 - RN (2018/0268921-9), da 3ª Turma. Brasília, DF, 08 de abr. de 2022. Disponível em:

Ademais, faz-se interessante chamar a atenção para a diferença existente no modo de tratamento de negócios jurídicos defeituosos na Lei nº 10.406, promulgada em 10 de janeiro de 2002 e em vigor no ano seguinte, mais conhecida como Código Civil[28], e na LGPD. Enquanto na primeira, o vício de consentimento gera, via de regra, a anulabilidade do negócio jurídico, na LGPD é ocasionada a nulidade.

Tal diferença de tratamento pode ser justificada pelo fato de o vício de consentimento na proteção de dados estar envolvido com direitos de personalidade, como o direito à privacidade, o que requer uma abordagem mais incisiva. Ao mesmo tempo, o titular de dados, inegavelmente, se encontra em uma posição de vulnerabilidade em comparação ao controlador e ao operador de dados, tendo em vista, por exemplo, a disparidade de informações sobre o tratamento de dados pessoais às quais cada parte tem acesso.

Dessa forma, na hipótese de infração, a LGPD traz uma lista de sanções administrativas em seu Art. 52 que podem ser aplicadas a depender das peculiaridades do cenário prático. Entretanto, é possível reduzir a sanção aplicada, com base na utilização de parâmetros como a existência de boa-fé do infrator, que pode ser percebida em cenários em que o agente de tratamento de dados demonstra ter adotado medidas para que o consentimento fosse concedido livre de vícios.

Cabe frisar que, além do risco de litígio, igualmente relevante é o risco reputacional ao qual o ente, principalmente privado, fica submetido em situações de incidentes que envolvam a nulidade do consentimento. Isso porque a confiança fornecida pelo titular dos dados ficaria comprometida, em meio a um cenário de insegurança jurídica, estando esse tentado a buscar uma outra instituição que lhe forneça algo semelhante à anterior e com um nível de proteção de dados mais adequado.

Com isso, um dos métodos que podem ser utilizados, tanto para prevenir litígios envolvendo o vício de consentimento, quanto contribuir para a aplicação do princípio da boa-fé, é o *Visual Law*, dado que sua aplicação reflete a preocupação do agente em obedecer ao direito à autodeterminação informativa, o princípio da transparência e os requisitos da base legal do consentimento.

---

https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=2156946&num_registro=201802689219&data=20220408&formato=PDF.

[28] Art. 138. São anuláveis os negócios jurídicos, quando as declarações de vontade emanarem de erro substancial que poderia ser percebido por pessoa de diligência normal, em face das circunstâncias do negócio.
Art. 145. São os negócios jurídicos anuláveis por dolo, quando este for a sua causa.

4 O VISUAL LAW E O USO DO MÉTODO NA OBTENÇÃO DO CONSENTIMENTO

Dadas as ponderações feitas no capítulo anterior quanto à construção da base legal do consentimento e os seus requisitos de validade, objetiva-se avaliar a influência do *Visual Law* enquanto método capaz de contribuir para a efetivação da validade do consentimento.

Com esse intuito, aborda-se, primeiramente, a diferenciação entre *Legal Design* e *Visual Law*, seguida pela análise do método do *Visual Law*, sob a perspectiva da LGPD, por intermédio de alguns casos práticos.

4.1 Visual Law ou Legal Design?

De modo simplificado, *Legal Design*, termo popularizado por Margaret Hagan[29], é a junção do *Design* e do Direito, com intenção de utilizar técnicas, ferramentas, metodologias e soluções, por vezes comuns na área do *Design*, no âmbito jurídico.

Dito isso, faz-se essencial mencionar que *design* não significa a elaboração de algo para fins exclusivamente estéticos, mas sim uma junção da criatividade e da praticidade em prol da inovação e da resolução de problemas. Steinwascher, Rossetti e Doro (2022, p. 82) dissertam que

> O Design é uma ciência que se dedica a propor soluções aos mais diversos tipos de problemas. Como ciência, possui subáreas e especialidades, mas como questão central, o design é uma resposta a um problema, dor ou necessidade. Design não é sobre estética pura, mas sobre pensar soluções para cumprir uma determinada função.

Visto isso, o *Legal Design* atua como um método que busca tornar os sistemas jurídicos mais centrados no usuário, para melhorar a usabilidade e a utilidade dos produtos e serviços. Segundo Maia, Nybo e Cunha (2020, p. 7),

> O *legal design* se baseia na ideia de que produtos e processos funcionais e bem projetados devem ser acessíveis e disponibilizados a todos. Podemos e devemos exigir soluções esteticamente mais agradáveis, fáceis de usar e atrativas para nossos problemas jurídicos diários.

Para tanto, tais autores apresentam ainda o entendimento de que o termo *Legal Design* pode ser definido como "a aplicação de princípios e elementos de *design* e a experiência do usuário na concepção e na elaboração de documentos ou produtos jurídicos".

---

[29] Margaret Hagan é Diretora Executiva do Legal Design Lab da Stanford Law School e autora do livro online e aberto Law By Design, que inclusive se encontra sob construção na data de acesso para este estudo.

Além do Direito e do *Design*, também é possível mencionar a adição do campo da Tecnologia no que diz respeito ao *Legal Design*, visto que ela exerce um indispensável papel em aprimorar a eficiência e a eficácia jurídica.

Sob essa ótica, Hagan (tradução livre) defende que na esfera do *Legal Design*, é possível dividir o *design* em 5 categorias, as quais são aplicadas a depender do tipo de problema que está para ser resolvido, sendo elas:

a) Design Sistêmico: trata da coordenação de projetos de larga escala e de sistemas complexos, como a organização do ordenamento jurídico;
b) Design Organizacional: voltado à organização de times e gestão de pessoas, e à análise de aplicação de metodologias à equipe, como a reestruturação das áreas de um departamento jurídico;
c) Design de Serviços: envolve a preocupação com a jornada de resolução de um problema como um todo em busca de encontrar soluções que melhorem a experiência do usuário, como a utilização de um *help desk* jurídico;
d) Design de Produtos: essa categoria busca o desenvolvimento de ferramentas e soluções que sejam capazes de solucionar um problema ou de auxiliar no cumprimento de uma atividade, como a criação de plataformas de assinatura eletrônica;
e) Design de Informação: envolve a elaboração de documentos e apresentações. É o tipo de *design* que envolve ferramentas gráficas e visuais, e que se preocupa com a aparência e o valor estético além da funcionalidade. Essa é a categoria do *Legal Design* que abarca o chamado *Visual Law*.

Sob essa perspectiva, o *Visual Law* se mostra como um método que busca utilizar elementos visuais para aprimorar o entendimento e a compreensão do destinatário da mensagem, podendo, ainda, ser vista como a fase final de um projeto de *Legal Design*.

Em outras palavras, *Visual Law* é a face do *Legal Design* que pretende simplificar e trazer clareza à informação jurídica transmitida por meio do uso de recursos visuais, como fluxogramas, *QR codes*[30], gráficos, ícones, imagens, *storyboards*[31] e hierarquia tipográfica[32].

---

[30] Os *QR codes*, também conhecido como "*Quick Response Code*" ou "código de resposta rápida", são códigos de barra bidimensionais que podem ser escaneados para fins diversos, como checar um produto no estoque de uma loja ou acessar um vídeo.
[31] O *storyboard* é uma sequência de desenhos ou imagens, quadro a quadro, com o intuito de simular a passagem de um evento ou uma situação, por exemplo.
[32] A hierarquia tipográfica é a variação de tamanho, fonte, cor, entre outros, em um texto para trazer um senso de níveis de importância diferentes no conteúdo apresentado.

Vale ressaltar que essa separação entre ambos os conceitos corresponde a um entendimento majoritário, porém há doutrinadores que defendem que o *Visual Law*, na verdade, trata exclusivamente do uso de elementos visuais, independentemente de finalidade ou funcionalidade, razão pela qual este seria um termo incorreto, enquanto *Legal Design* seria o mais apropriado a ser utilizado[33].

Todavia, para fins deste estudo, será considerado que o método do *Visual Law* parte como subcategoria do método do *Legal Design*. Isso porque o *Legal Design* abrange diversos cenários e situações, em consonância com o demonstrado na divisão apresentada por Margaret Hagan, que podem ou não incluir casos que sejam contemplados pelo *Visual Law*.

Aliás, o uso genérico do termo *Legal Design* poderia prejudicar a compreensão do leitor em entender o contexto no qual o seu uso está inserido, tendo em vista os múltiplos significados que ele poderia exercer num cenário concreto.

4.2 O método do *Visual Law*

Parte do motivo que fundamenta a relevância do *Visual Law* e sua eficácia é o fato de a natureza humana ser direcionada para a informação visual, que é absorvida melhor do que informações exclusivamente textuais, dado que podem ser reconhecidas e processadas mais facilmente.

Segundo Hockley (2008, p. 1351, tradução livre), em seu artigo sobre o efeito da superioridade da imagem,

> Foi claramente estabelecido que imagens são melhor relembradas do que palavras em testes de recordação e testes de reconhecimento de itens (ver, por exemplo, Durso & O'Sullivan, 1983; Gehring, Toglia, & Kimble, 1976; Juola, Taylor, & Young, 1974; Madigan, 1974; Nelson, Reed, & McEvoy, 1977; Nelson, Reed & Walling, 1976; Paivio & Csapo, 1973; Paivio, Rogers & Smythe, 1968; Snodgrass & Burns, 1978; Snodgrass, Volvovitz & Walfish, 1972; Snodgrass, Wasser, Finkelstein e Goldberg, 1974). (...) Uma das primeiras explicações do efeito da superioridade da imagem foi em termos da teoria da dupla codificação de Paivio (1971, 1976). Nesta teoria, imagens são mais prováveis de serem codificadas, tanto em representações

[33] Segundo Maia, Nybo e Cunha (2020) "existem profissionais que adotam a nomenclatura *visual law* para se referirem à prática de criação de documentos jurídicos esteticamente agradáveis. Aqueles que defendem o termo *visual law* defendem que ele se refere apenas ao uso de recursos gráficos (por isso, visuais) nos documentos jurídicos. (...) Para que sejam usadas técnicas de *legal design*, é necessário que o criador do documento utilize os recursos gráficos e, assim, atinja a funcionalidade pretendida para o documento. Isso é feito durante a fase de análise da experiência do usuário, uma das fases do processo de criação. Dentro da prática do *legal design* não se coloca nenhum elemento visual que não tenha uma finalidade ou funcionalidade clara e objetiva aos usuários do documento. (...) No entanto, se os usuários do termo *visual law* vierem a defender, alegando que ele serve para facilitar o entendimento desses documentos jurídicos por meio de recursos visuais, essa prática já está compreendida no termo *legal design* – justamente porque, além da forma estética, existe uma função atrelada a ela: a de facilitar a leitura e a compreensão. Por isso, de uma forma ou de outra, entendemos que o termo não deve ser utilizado por não fazer sentido como conceito".

> verbais, quanto visuais, do que palavras, aumentando assim a probabilidade de rememorar posteriormente.

Nesse sentido, Coelho e Holtz (2020, p. 18) discutem que

> (...) a evolução do ser humano e da comunicação no mundo moderno tem alterado sensivelmente esse cenário, especialmente por essa digitalização de tudo. Hoje não precisamos mais procurar o livro todo na estante. O assunto que nos interessa está em um capítulo que acessamos on-line, num artigo compartilhado na internet, em um vídeo de seu canal na web preferido ou em um infográfico. Mais do que ler, hoje precisamos saber onde procurar. Assim como precisamos entender como oferecer o conteúdo que as pessoas procuram, no formato que elas preferem e com a linguagem adequada para cada público.

Percebe-se, pois, que o Direito, enquanto área que utiliza dialeto próprio e que lida majoritariamente com a linguagem textual ou verbal, até então, vinha na contramão daquilo que a ciência já havia definido sobre o modo de absorção e compreensão humana.

À vista disso, Coelho e Holtz (2020, p. 19) afirmam que falta no Direito a preocupação em organizar as informações necessárias e em pensar naqueles que serão os destinatários dela, principalmente quando estes forem indivíduos sem qualquer formação jurídica e que se sentem distanciados da área, tendo em vista que não compreendem a linguagem.

Por essa razão, diz-se que o *Visual Law* é um método que possui a capacidade de democratizar o Direito, visto que facilita a compreensão das informações jurídicas, principalmente, por aqueles que não estão inseridos em meio ao ramo jurídico, que tende a ser carregado de jargões e tecnicismos que contribuem para dificultar o entendimento e estabelecer barreiras no relacionamento entre o emissor e o destinatário da mensagem.

Vale ressaltar que isso se aplica independentemente do âmbito do Direito, de modo que não importa se é processual ou consultivo ou se é cível ou penal, pois o *Visual Law* traz tais benefícios para qualquer uma dessas opções.

Nesse aspecto, a pesquisa realizada pelo grupo VisuLaw “Elementos visuais em petições na visão da magistratura estadual”, com 503 juízes estaduais em 2022, apontou que 77,9% dos juízes estaduais concordam que os elementos visuais são capazes de facilitar a análise de petições, enquanto 99,2% afirmaram que uma redação mais objetiva torna a petição mais agradável para leitura e análise.

Com isso, a ideia é justamente elaborar um documento que seja pensado e estruturado especialmente para o público-alvo daquele texto, utilizando uma linguagem mais clara, concisa e didática, ao mesmo tempo em que associa a linguagem textual e a visual.

Nesse sentido, destaca-se que a linguagem visual não significa o uso carregado de imagens e ícones coloridos, mas sim uma estratégia que busque tornar o documento mais agradável visualmente, sem perder a funcionalidade. O simples fato de transformar um parágrafo de 10 linhas, que apresenta tópicos e estatísticas percentuais, em um infográfico, independentemente de utilizar ou não elementos como cores e variação tipográfica, ilustra essa estratégia.

Ademais, fato é que o *Visual Law* permite que o emissor utilize uma vasta gama de ferramentas e recursos que podem ser combinados entre si para alcançar o seu objetivo de transmitir a mensagem do modo mais eficiente possível.

Dessa forma, além de garantir uma maior compreensão sobre o conteúdo que quer repassar, também recebe a satisfação do destinatário em sentir que houve uma preocupação com o seu entendimento, reforçando valores como transparência e confiança para com o emissor.

Para tanto, a título de exemplo, é possível citar o contrato de trabalho elaborado em 2016 pela Creative Contracts para a Indigo Fruit (Pty) Ltd, empresa agrícola que cultiva e fornece ClemenGold, o qual se tornou um dos maiores *cases* de sucesso no que refere ao uso de *Visual Law*.

Parte do motivo pelo qual esse contrato recebeu tanto destaque foi por conta da sua estrutura inovadora, uma vez que foi elaborada completamente em formato de quadrinhos, chamado de *Comic Contract* pelos idealizadores, totalmente ilustrado, conforme apresentado na Figura 1, para possibilitar a compreensão e a interpretação correta dos funcionários da empresa, num cenário onde grande parte deles era analfabeto ou analfabeto funcional.

Tamanho foi seu sucesso que após a implementação do contrato, o tempo de leitura dos funcionários foi reduzido de 4 horas para 40 minutos[34]. Além disso, em entrevista para o livro de Maia, Nybo e Cunha (2020, p. 20), Robert de Rooy, criador dos *Comic Contracts*, afirmou que sua experiência

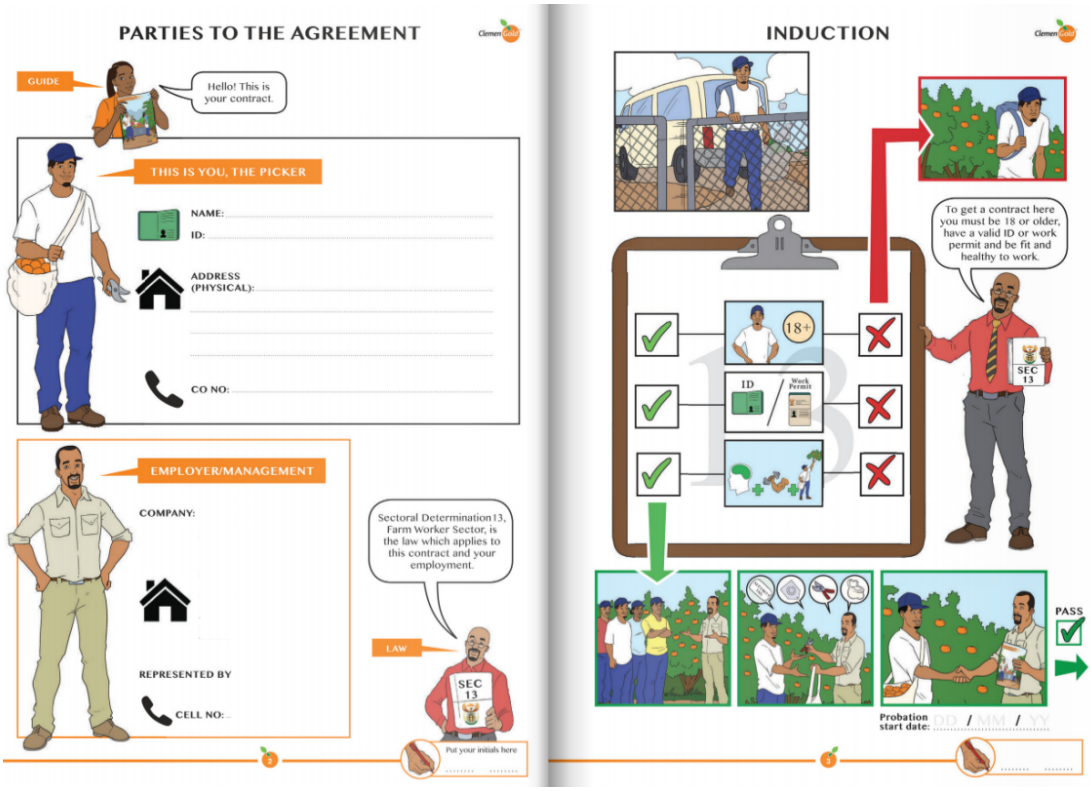
> mostra que disponibilizar informações para pessoas vulneráveis e analfabetas de uma forma clara e compreensível não significa apenas tornar as informações mais fáceis de entender, mas também honrar a dignidade das pessoas. Trata-se de mostrar às pessoas vulneráveis que é importante que entendam o que se espera delas e o que podem esperar em termos de suas obrigações e direitos. (...)

Além do mais, ele ainda reforça que "cada vez que uma empresa fornece informações a uma pessoa vulnerável de uma forma que ela não pode razoavelmente

[34] ClemenGold Comic Contract. **Creative Contracts (Pty) Ltd and ComiContracts**. África do Sul, maio de 2016. Disponível em: https://creative-contracts.com/clemengold/.

entendê-la, sua capacidade de viver uma vida autônoma e responsável, bem como sua dignidade, estão sendo violadas".

Figura 1 - Página do contrato de trabalho elaborado pela Creative Contracts para a Indigo Fruit (Pty) Ltd



Fonte: Creative Contracts (Pty) Ltd and ComiContracts™ (2016)

Logo, é inegável que o uso de um método com uma proposta tal como a do *Visual Law* também se apresenta como sinal de empatia para com o indivíduo, bem como contribui para respeito ao princípio da dignidade da pessoa humana, previsto no Art. 1º, III da Constituição da República Federativa do Brasil.

4.3 O uso do *Visual Law* na LGPD sob a ótica do instituto do consentimento

Se antes já se questionava a eficiência da redação utilizada nos documentos jurídicos, com a LGPD isso se tornou ainda mais frequente. Afinal, via de regra, a maior parte dos documentos jurídicos relacionados à proteção de dados não são elaborados para serem lidos pelos funcionários do agente de tratamento de dados, nem pelo Poder Judiciário, nem por juristas, mas sim por terceiros, que, geralmente, não tem qualquer tipo de familiaridade com as nomenclaturas, com as expressões ou com os termos jurídicos.

Destaca-se, a própria LGPD reforça a preocupação com a falta de compreensão dos titulares dos dados pessoais na escolha dos direitos e dos princípios que envolvem tal legislação, principalmente o direito à autodeterminação informativa e ao princípio da transparência.

Nessa perspectiva, Pinheiro (2021, p. 10) reforça que, em meio a um cenário onde as instituições públicas e privadas precisam resgatar e repactuar o compromisso de proteção e de direitos fundamentais, como o direito à privacidade, com os cidadãos, por mais que a liberdade tenha um papel basilar no restabelecimento dessa relação de confiança, é a transparência que contribui para o fortalecimento e mantimento da mesma.

Ora, se o titular dos dados não é capaz de compreender as informações fornecidas referentes ao tratamento de seus dados pessoais, não há como defender que há transparência para com ele, nem que seu direito à autodeterminação informativa está sendo garantido e protegido.

Tal situação merece ainda mais atenção quando o tratamento de dados pessoais utiliza a base legal do consentimento, pois não há como afirmar que o indivíduo forneceu o aceite válido se a redação da Política de Privacidade e/ou dos Termos e Condições de Uso não está clara.

Nesse aspecto, a falta de clareza pode se dar, a título de ilustração, por indução ao erro ou a uma interpretação equivocada ou pela presença de um linguajar carregado de tecnicismos, tanto do âmbito do Direito, quando do da Tecnologia, levando em consideração que, devido à proximidade destas áreas numa conjuntura de proteção de dados, é comum o uso de conceitos e termos menos usuais fora do digital, como *cookies*[35].

Alinhado ao exposto, foi retratado no relatório emitido pela Comissão Europeia em 2020[36], no qual foi constatado que 90% dos britânicos aceitam termos e condições de uso sem compreender com o que estão concordando. Entre os motivos apontados, tem-se que a linguagem é muito complexa e/ou prolixa, dificultando o entendimento do usuário.

Corroborando com esse entendimento, é possível citar a apresentação da artista Dima Yarovinsky exibida no evento Visualizing Knowledge de 2018[37], que trouxe a

[35] Os *cookies* funcionam como pequenos arquivos que armazenam preferências, dados de comportamento e outras informações que são usadas nas páginas visitadas pelo indivíduo. Por essa razão, é comum que os *sites* possuam as chamadas "Políticas de *Cookies*" ou "Aviso de *Cookies*" para informar e coletar a permissão do usuário para fornecer este acesso. Vale ressaltar que existe uma categoria de *cookies*, chamada de "Essenciais", que são estritamente necessários para que o site ou a plataforma funcione, razão pela qual o usuário não pode negar acesso a eles.

[36] What does your phone know about you? **Thinkmoney**, 03 de nov. de 2020. Disponível em: https://www.thinkmoney.co.uk/blog/what-phones-know-about-you/. Acesso em: 18 jan. 2023.

[37] I AGREE. Visualizing Knowledge 2018. Disponível em: https://vizknowledge.aalto.fi/archive/2018/category/showcase/. Acesso em: 18 jan. 2023.

impressão dos Termos e Condições de Uso do Facebook, do Snapchat, do Instagram, do Twitter, do Tinder, do WhatsApp e do Google, como modo de enfatizar a fragilidade do indivíduo perante a concordância "cega" com o tratamento de dados por parte dessas empresas em meio a redações extensas, prolixas e sem polidez com o leitor.

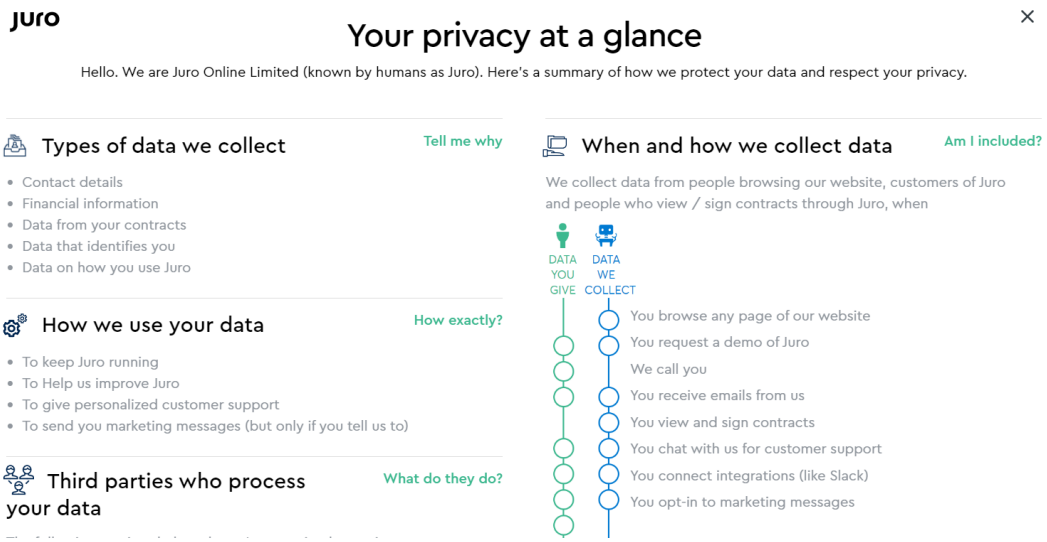
Desse modo, perceptivelmente há uma falha do agente de tratamento em respeitar os requisitos contidos para uso da base legal de consentimento, principalmente com relação ao de manifestação informada pelo titular.

Salienta-se que a LGPD não especifica o modo como a transparência deverá ser garantida para fins de obtenção do consentimento, conforme Art. 8º, o que possibilita que o agente tenha liberdade de escolher o método que desejar, seja por meio de vídeo, áudio ou texto, desde que não abdique de apresentar uma linguagem clara, simples e objetiva.

Dito isso, em meio a promulgação das legislações de proteção de dados ao redor do mundo, diversas instituições começaram a direcionar esforços para a elaboração de documentos jurídicos que facilitassem a compreensão do titular dos dados, bem como as fizessem atuar em conformidade com os direitos, os princípios e os requisitos de consentimento previstos.

Sob essa ótica, um dos maiores *cases* de sucesso no que diz respeito ao uso do *Visual Law* em documentos que envolvem a proteção de dados, é o da Política de Privacidade da Juro[38], apresentando uma versão resumida que aparece logo ao clicar em "*Privacy Policy*", visualizada na Figura 2, e uma versão estendida para mais informações.

Figura 2 - Imagem dos Termos de Uso da Juro



Fonte: The Juro Privacy Policy

[38] The Juro Privacy Policy. **Juro**. Disponível em: https://juro.com/privacy.

Um dos pontos mais interessantes dessa Política é que ela não utilizou uma grande variedade de recursos visuais, estando o seu diferencial justamente na escolha de mantê-la o mais sóbria possível, por meio da reordenação dos tópicos, da transformação da linguagem para a mais concisa possível e do uso de pequenos ícones apenas para facilitar a absorção e criar uma espécie de memória visual.

Semelhante ao exposto, pode-se citar no Brasil os Termos e Condições de uso da Koin Administradora de Cartões e Meios de Pagamento S.A., que foi estruturado em três versões diferentes (fluxo, resumo e texto expandido) para que a escolha da melhor versão para fins de leitura e compreensão ficasse a critério exclusivamente do leitor[39].

Contudo, faz-se importante ressaltar que somente a versão completa seria juridicamente vinculativa, conforme aponta Serafino (2022, p. 53), figurando as demais como acessórias para facilitar o entendimento do leitor.

Além disso, a empresa tornou o documento mais interativo, o que contribui para a atração do leitor, e utilizou recursos visuais que permitiram que a leitura fosse mais agradável, conforme Figura 3, por meio do uso de ícones, esquemas e marcações no texto.

Figura 3 - Imagem dos Termos e condições de uso da Koin

Fonte: Koin Administradora de Cartões e Meios de Pagamento S.A. (2021)

[39] Termos e condições de uso. **KOIN Adm. de Cartões e Meios de Pagamento S.A**, 09 de nov. de 2021. Disponível em: https://termos.koin.com.br/.

Por fim, apesar dos recursos utilizados, a escolha da linguagem utilizada pela Koin é um dos pontos que mais se destaca nos seus Termos e Condições de Uso, a qual contribui para imprimir a personalidade da empresa no documento, bem como para se aproximar do leitor, com o uso de uma linguagem com características coloquiais e informais, de fácil acesso e de muita didática, como "é quase mágica" ou "A análise da Koin é diferentona s2" ou "Não vale emprestar seu CPF nem usar o CPF de outra pessoa para comprar com a Koin, hein!".

Além da Koin, merece destaque o Termo de Uso do banco Will Bank[40], que criou uma versão do documento em vídeo e outra em texto para trazer mais acessibilidade ao leitor e otimizar a comunicação, sendo, até mesmo, utilizado como caso prático nos mais diversos painéis e congressos sobre temas que envolvem *Visual Law* e proteção de dados no Brasil.

Para isso, o documento prioriza a interatividade e o uso de uma linguagem objetiva, clara e com um pouco de informalidade, que conta com o auxílio de ícones para trazer mais dinamicidade e facilitar ainda mais a compreensão do leitor sobre o documento, conforme Figura 4, semelhante ao apresentado nos Termos e Condições de Uso da Koin.

Figura 4 - Imagem dos Termos de Uso da Will Bank

Fonte: Will S.A Instituição de Pagamento

[40] Disponível em: https://www.willbank.com.br/termos-uso/

Nessa lógica, com o intuito de tornar a experiência do cliente na leitura deste documento melhor, que pode impactar na escolha por aderir ao serviço da empresa em questão, Steinwascher, Rossetti e Doro (2022, p. 85) explicaram que foi feito um trabalho de arquitetura funcional do conteúdo dos Termos de Uso para separá-lo hierarquicamente, priorizando aquilo que fosse essencial que o cliente soubesse, seguido pela reescrita do documento com a utilização de linguagem simples que permitisse que, independentemente do nível de conhecimento sobre serviços financeiros, qualquer pessoa pudesse compreender.

Por fim, há uma série de outros *cases* de sucesso no que diz respeito ao *Visual Law* na seara da proteção de dados, bem como ainda surgirão vários outros, cada vez mais inovadores.

Isso posto, Antunes (2021, p. 21) aduz que

> (...) propor uma nova arte para o direito consiste em harmonizar as demandas da modernidade líquida, juntamente com os fenômenos jurídicos, utilizando-se do design para cocriar um novo modo de prestar o serviço jurisdicional. Não é uma arte constituída de adereços bonitos e inúteis, ou tecnologias mirabolantes, nem tão pouco, métodos ineficazes de resolução, mas técnicas mensuráveis para propor um direito mais humano, inteligente e moderno.

Tomando base no que foi apresentado, é possível notar que o *Visual Law* é capaz de atuar como um método capaz de contribuir para a democratização do conhecimento e do Direito, bem como para a validade do consentimento e, consequentemente, para a concretização do princípio da transparência, ao passo em que ele consegue simplificar informações longas, conteudistas e prolixas em documentos objetivos, claros e didáticos, por meio de simples mudanças no formato, que ficam a exclusivo critério de escolha do agente de tratamento.

5 CONSIDERAÇÕES FINAIS

Em concordância com o que fora exposto, viu-se que, com o avanço tecnológico, as dinâmicas sociais e comportamentais foram modificadas ao redor do mundo, tornando as relações cada vez mais estreitas e dependentes do meio digital.

Para tanto, tornou-se imprescindível a elaboração de legislações que tivessem seus interesses destinados à proteção da privacidade e das informações pessoais dos indivíduos, como meio de frear o acesso e o compartilhamento descontrolado, que, geralmente, ocorriam sem que o titular sequer tivesse ciência.

Nesse sentido, por mais recente que seja e por mais que ainda tenha deficiências em sua redação, a LGPD foi construída com base num aporte histórico robusto, tanto por influências externas, como o GDPR e o escândalo do Cambridge Analytica, quanto internas, como a Lei do Cadastro Positivo, a LAI e o Marco Civil da Internet.

Isso contribuiu para que a LGPD já apresentasse conceitos de extrema relevância para a ótica da proteção de dados desde a sua promulgação, como a autodeterminação informativa e o princípio da transparência, os quais, por sua vez, desembocam em uma das principais bases legais, que é o consentimento.

Esse conjunto basilar aponta parte da essência da proteção de dados ao passo em que busca regular o acesso e o controle dos dados pessoais por parte dos agentes de tratamento, afinal de contas o dado pessoal pertence ao indivíduo, não à instituição pública ou privada com a qual ele optou por compartilhar.

Logo, a proteção de dados faz jus ao direito que o indivíduo tem em ter o conhecimento sobre as atividades que serão realizadas com o seu dado pessoal e com base em seu próprio discernimento decidir se vai concordar com o fornecimento dele ou não, sob a ótica do consentimento.

Nessa lógica, o próprio instituto do consentimento prevê mecanismos que atuam como requisitos para que o controlador ou o operador tenha a autorização para realizar a atividade de tratamento. Entre eles, um dos que mais causou impacto na maneira como as instituições lidavam com os documentos jurídicos de proteção de dados foi a garantia de que houvesse a manifestação devidamente informada por parte do titular no momento em que ele concedeu o consentimento.

Isso porque o Direito é uma área que naturalmente é carregada de jargões e tecnicismos que não são compreendidos por aqueles que não tem formação jurídica. Ademais, essa situação é agravada haja vista o exercício da profissão incentivar o uso constante destes

termos, dificultando que haja criticidade em reconhecer quem é a pessoa que de fato vai ler o documento jurídico em questão.

À vista disso, documentos como Políticas de Privacidade e Termos e Condições de Uso precisaram ser repensados e reestruturados, uma vez que, com a LGPD, já não bastava apenas o conteúdo que era colocado no documento - que, muitas vezes, não continha informações verídicas e/ou completas -, mas também o modo como aquilo era repassado.

Desse modo, coletar a simples autorização do titular deixou de significar que ele de fato concordou com aquilo, devendo ser levada em análise toda a conjunção sob a lente dos requisitos do consentimento.

Para tanto, o surgimento do método do *Visual Law*, que não coincidiu ou se deu em razão da proteção de dados, se mostrou um verdadeiro aliado no que diz respeito ao cumprimento dos requisitos do consentimento, principalmente em relação à manifestação informada, e, consequentemente, ao princípio da transparência e ao direito à autodeterminação informativa, o que é perceptível na análise dos casos concretos da Creative Contracts, da Juro, da Koin e do Will Bank

A explicação dessa correlação parte do pressuposto de que o ser humano tem, por natureza, maior facilidade na compreensão das informações visuais do que das textuais. Levando isso em consideração, é fácil inferir que o modo de produção dos documentos jurídicos se dava na contramão da maneira como a ciência já havia orientado.

Portanto, o *Visual Law* surge com o intuito de associar o Direito a ferramentas que vinham sendo utilizadas na área do *Design*, de modo que os documentos jurídicos, de um modo geral, passariam a ter uma roupagem selecionada com base em técnicas e conceitos apresentados pelo *design*, com o intuito primário de tornar o documento mais simples, conciso e didático, permitindo que qualquer pessoa, independentemente da formação, conseguisse compreender.

Assim, por mais que o *Visual Law* seja um método já bastante utilizado em algumas áreas do Direito, como Contratos, ainda podem e devem ser difundida na de proteção de dados, pois os benefícios são inumeráveis, como o respeito aos fundamentos da proteção de dados, a presunção de boa-fé, o diferencial competitivo, a melhora da reputação, o estabelecimento de uma relação de confiança com o titular dos dados, entre outros, conforme percebido nas instituições que já vem aplicando tal método.

Com base nesse entendimento, é interessante a realização de estudo posterior para avaliar, na prática, o impacto gerado pelo uso do *Visual Law* em meio à proteção de dados,

tanto em algumas instituições públicas, quanto em privadas, a fim de popularizar o uso dessa ferramenta e gerar uma cultura mais fortificada de proteção de dados nos indivíduos.

REFERÊNCIAS

ANTUNES, Andreza Martins. **Legal Design: Um Futuro Necessário Para O Direito 4.0**. 2021. 28 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Centro Universitário de João Pessoa, João Pessoa, 2021. Disponível em: https://publicacoes.even3.com.br/tcc/legal-design-um-futuro-necessario-para-o-direito-4o-428714. Acesso em: 18 jan. 2023.

BIONI, Bruno Ricardo (Coord.). **Tratado de Proteção de Dados Pessoais**. 1. ed. Rio de Janeiro: Forense, 2020. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 04 jan. 2023.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 04 jan. 2023.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 05 jan. 2023.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 17 jan. 2023.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 04 jan. 2023.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 04 jan. 2023.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 04 jan. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 04 jan. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 dez. 2022.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.848.862 - RN (2018/0268921-9), da 3ª Turma. Brasília, DF, 08 de abr. de 2022. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=2156946&num_registro=201802689219&data=20220408&formato=PDF. Acesso em: 17 jan. 2023.

COELHO, Alexandre Zavaglia; HOLTZ, Ana Paula Ulandowski. **Legal Design | Visual Law: comunicação entre o universo do Direito e os demais setores da sociedade**. São Paulo: Thomson Reuters Brasil, 2020. *E-book.* Disponível em: https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/white-paper/legal-one-e-book-visual-law-2020.pdf. Acesso em: 18 jan. 2023.

ClemenGold Comic Contract. **Creative Contracts (Pty) Ltd and ComiContracts**. África do Sul, maio de 2016. Disponível em: https://creative-contracts.com/clemengold/. Acesso em: 06 jan. 2023.

DONEDA, Danilo. **Da privacidade à Proteção de Dados Pessoais**. 2 ed. São Paulo: Thomson Reuters Brasil, 2019.

Elementos visuais em petições na visão da magistratura estadual. **VisuLaw**, 2022. Disponível em: https://opiceblum.com.br/wp-content/uploads/2022/02/pesquisa-magistratura-estadual.pdf. Acesso em: 18 jan. 2023.

Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **BBC News Brasil**, 20 de mar. de 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 16 jan. 2023.

ESPECIAL | Por que se preocupar com o que o Estado faz com nossos dados pessoais? **InternetLab**, 21 de maio de 2018. Disponível em: https://internetlab.org.br/pt/noticias/especial-apps-do-governo/. Acesso em: 16 jan. 2023.

FONSECA, Edson Pires. **Lei Geral de Proteção de Dados - LGPD**. 1. ed. Salvador: Juspodivm, 2021.

HAGAN, Margaret. **Law by Design**. Disponível em: https://lawbydesign.co/. Acesso em: 05 jan. 2023.

HIRATA, Alessandro. Direito à privacidade. **Enciclopédia jurídica da PUC-SP**. Tomo Direito Administrativo e Constitucional. 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade. Acesso em: 18 jan. 2023.

HOCKLEY, William E. The picture superiority effect in associative recognition. **Memory & Cognition**, v. 36, p. 1351–1359. Wilfrid Laurier University, Ontario, 09 de jun. de 2008. Disponível em: https://doi.org/10.3758/MC.36.7.1351. Acesso: 18 jan. 2023.

I AGREE. Visualizing Knowledge 2018. Disponível em: https://vizknowledge.aalto.fi/archive/2018/category/showcase/. Acesso em: 18 jan. 2023.

Information Overload: tudo o que você precisa saber. **Kaptiva**, 29 de nov. de 2019. Disponível em: https://www.kaptiva.com.br/information-overload-tudo-o-que-voce-precisa-saber/. Acesso em: 17 jan. 2023.

Justiça europeia anula acordo UE-EUA sobre transferência de dados pessoais; decisão afeta gigantes como Facebook. **O Globo**, 16 de jul. de 2020. Disponível em: https://oglobo.globo.com/economia/tecnologia/justica-europeia-anula-acordo-ue-eua-sobre-transferencia-de-dados-pessoais-decisao-afeta-gigantes-como-facebook-24535366. Acesso em: 16 jan. 2023.

KRIEGER, Maria Victoria Antunes. **A análise do instituto do consentimento frente à lei geral de proteção de dados do Brasil (Lei n° 13.709/18)**. 2019. 83 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Santa Catarina, Florianópolis, 2019. Disponível em: https://repositorio.ufsc.br/handle/123456 789/203290. Acesso em: 17 jan. 2023.

LEONARDI, Marcel. **Tutela e privacidade na Internet**. 1. ed. São Paulo: Saraiva, 2011.

Lei Carolina Dieckmann: Você sabe o que essa lei representa? **Fundação Escola Superior do Ministério Público (FMP)**, 16 de agosto de 2021. Disponível em: https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/. Acesso em: 14 jan. 2023.

LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados**: de acordo com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015). São Paulo: Almedina, 2020. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788584936397/. Acesso em: 17 jan. 2023. p. 84.

MAIA, Ana Carolina; NYBO, Erik Fontenele; CUNHA, Mayara. **Legal design: criando documentos que fazem sentido para os usuários**. São Paulo: Saraiva, 2020. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788553613687/. Acesso em: 06 jan. 2023.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). **Lei Geral de Proteção de Dados Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. *E-book*. Acesso em: 06 jan. 2023.

MALHEIRO, Luíza Fernandes. **O consentimento na proteção de dados pessoais na Internet: uma análise comparada do Regulamento Geral de Proteção de Dados Europeu e do Projeto de Lei 5.276/2016**. 2017. 86 f. Trabalho de Conclusão de Curso (Graduação em

Direito) - Universidade de Brasília, Brasília, 2017. Disponível em: https://bdm.unb.br/handle/10483/18883. Acesso em: 18 jan. 2023.

MELO, Rodrigo Amaral Paula de; BOULOS, Henrique Maciel. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e a Administração Pública - Desafios na Aplicação. In: TOMASEVICIUS FILHO, Eduardo (Coord.). **A Lei Geral de Proteção de Dados Brasileira: uma análise setorial**. 1. ed. São Paulo: Almedina, 2021. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786556271705/. Acesso em: 17 jan. 2023.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. 1. ed. São Paulo: Saraiva, 2014.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (Coord.). **Direito, Inovação e Tecnologia**. São Paulo: Saraiva, 2015. v. 1.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. 3. ed. São Paulo: Editora Saraiva, 2021. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555595123/. Acesso em: 28 dez. 2022.

RGPD (GDPR) - Regulamento Geral sobre a Proteção de Dados. Disponível em: https://gdprinfo.eu/pt-pt. Acesso em: 30 dez. 2022.

RGPD (GDPR) - Regulamento Geral sobre a Proteção de Dados - Considerando 42. Disponível em: https://gdpr-text.com/pt/read/recital-42/. Acesso em: 17 jan. 2023.

RGPD (GDPR) - Regulamento Geral sobre a Proteção de Dados - Considerando 58. Disponível em: https://gdpr-text.com/pt/read/recital-58/. Acesso em: 17 jan. 2023.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. **O direito à proteção de dados pessoais e a privacidade**. Revista da Faculdade de Direito da UFPR, Curitiba, n. 53, p. 45 - 66, 2011. Disponível em: https://revistas.ufpr.br/direito/article/view/30768/19876. Acesso em: 18 jan. 2023.

SANTOS, Viviane Bezerra de Menezes. **Lei Geral de Proteção de Dados: fundamentos e *compliance***. 2019. 55 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal do Ceará, Fortaleza, 2019. Disponível em: http://www.repositorio.ufc.br/bitstream/riufc/49370/1/2019_tcc_vbmsantos.pdf. Acesso em: 17 jan. 2023.

SCHWABE, Caroline. Right to informational self-determination. **Robin Data GmbH**, 02 de abr. de 2021. Disponível em: https://www.robin-data.io/en/data-protection-academy/wiki/right-to-informational-self-determination. Acesso em: 17 jan. 2023.

SCHOOL, Stanford Law. **The Legal Design Lab**. Disponível em: https://law.stanford.edu/organizations/pages/legal-design-lab/#slsnav-publications-articles-and-press. Acesso em: 04 jan. 2023.

SERAFINO, Danielle Campos Lima. Ícones de Privacidade e Lei Geral de Proteção de Dados. In: SOUZA, Bernardo de Azevedo; OLIVEIRA, Ingrid Barbosa. **Visual law: como os elementos visuais podem transformar o direito**. 2. Ed. São Paulo: Thomson Reuters Brasil, 2022.

SOMBRA, Thiago Luís Santos. **Fundamentos da Regulação da Privacidade e Proteção de Dados Pessoais:** pluralismo jurídico e transparência em perspectiva. 1. ed. São Paulo: Thomson Reuters Brasil, 2020. *E-book*. Acesso em: 06 jan. 2023.

STEINWASCHER, Aline; ROSSETTI, Caio Carvalho; DORO, Meiriely Cortes. Legal Design: Muito além do Visual Law. In: FEIGELSON, Bruno; MARQUES, Daniel; PERALTA, Maria Alice Lima; et al (coord.). **Departamento Jurídico 4.0 e Legal Operations**. São Paulo: Saraiva, 2022, p. 82 - 85. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555599145/. Acesso em: 05 jan. 2023.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados Pessoais (LGPD): comentado artigo por artigo**. 4. ed. São Paulo: Saraiva, 2022. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555599015/. Acesso em: 12 jan. 2023.

Termos de Uso. **Will S.A Instituição de Pagamento**. Disponível em: https://www.willbank.com.br/termos-uso/. Acesso em: 18 jan. 2023.

Termos e condições de uso. **KOIN Adm. de Cartões e Meios de Pagamento S.A**, 09 de nov. de 2021. Disponível em: https://termos.koin.com.br/. Acesso em: 18 jan. 2023.

The CNIL's restricted committee imposes a financial penalty of 50 million euros against GOOGLE LLC. **European Data Protection Board**, 21 de jan. de 2019. Disponível em: https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en. Acesso em: 17 jan. 2023.

The Juro Privacy Policy. **Juro**. Disponível em: https://juro.com/privacy. Acesso em: 18 jan. 2023.

UNIVERSITY, Northeastern. Northeastern University School of Law. **NuLawLab**. 2020. Disponível em: https://www.nulawlab.org/. Acesso em: 04 jan. 2023.

VIDIGAL, Alessyara Giocássia Resende de Sá Rocha. **Os limites do consentimento: uma análise crítica do instituto tutelado como ferramenta de resguardo dos direitos do titular e de legitimação do tratamento de dados pessoais**. 2021. Dissertação (Mestrado em Direito Político e Econômico) - Universidade Presbiteriana Mackenzie, São Paulo, 2021. Disponível em: https://dspace.mackenzie.br/handle/10899/28734. Acesso em: 18 jan. 2023.

VIEIRA, Victor Rodrigues Nascimento. **Lei geral de proteção de dados: uma análise da tutela dos dados pessoais em casos de transferência internacional**. 2019. 77 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Uberlândia, Uberlândia, 2019. Disponível em: https://repositorio.ufu.br/handle/123456789/26233. Acesso em: 16 jan. 2023.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890. Disponível em: https://doi.org/10.2307/1321160. Acesso em: 04 jan. 2023.

What does your phone know about you? **Thinkmoney**, 03 de nov. de 2020. Disponível em: https://www.thinkmoney.co.uk/blog/what-phones-know-about-you/. Acesso em: 18 jan. 2023.