UNIVERSIDADE PRESBITERIANA MACKENZIE

FERNANDO OLIVEIRA MELO

LEI GERAL DE PROTEÇÃO DE DADOS: Impactos e Imposições às Redes Sociais

São Paulo

2022

FERNANDO OLIVEIRA MELO

LEI GERAL DE PROTEÇÃO DE DADOS: Impactos e Imposições às Redes Sociais

Monografia apresentada à Universidade Presbiteriana Mackenzie – Campus Higienópolis, para obtenção do título de Bacharel em Direito.

ORIENTADOR: PROF. DR. LUIZ GUSTAVO FRIGGI RODRIGUES

São Paulo

2022

FERNANDO OLIVEIRA MELO

LEI GERAL DE PROTEÇÃO DE DADOS: Impactos e Imposições Às Redes Sociais

Monografia apresentada à Universidade Presbiteriana Mackenzie – Campus Higienópolis, para obtenção do título de Bacharel em Direito.

Aprovado em _____/_____/_____

BANCA EXAMINADORA

_____

Examinador(a): _____

_____

Examinador(a): _____

_____

Examinador(a): _____

AGRADECIMENTOS

Aos meus familiares e amigos pelo incondicional apoio em inúmeras adversidades encontradas no decorrer destes 5 (cinco) anos de curso e por toda a fé depositada em mim. Obrigado pela ajuda e apoio de vocês, sou e sempre serei grato.

Agradeço a todos os docentes do curso de direito da Universidade Presbiteriana Mackenzie, dos quais, demonstraram-se exímios profissionais, extremamente brilhantes e capacitados, que possibilitam diariamente a formação de inúmeros operadores do direito e, acima de tudo, carregam consigo uma didática humanizada, registando e eternizando em nossas memórias experiências únicas vivenciadas em sala de aula.

Por fim, gostaria de agradecer, em especial, ao meu professor e orientador Dr. Luiz Gustavo Friggi, cuja assistência manteve-se inabalável ao decorrer de toda a orientação, colocando-se à disposição para eventuais dúvidas sempre que possível, demonstrando-se extremamente acessível, caminhando paralelamente a mim.

RESUMO

Implementada em 2020, a Lei Geral de Proteção de Dados surge com escopo definido pelo legislador: regulamentação e amparo legal ao titular de dados. É notório que, antes da LGPD, a legislação nacional carecia de instrumentos protetivos contra coleta e tratamento abusivo de dados pessoais, problemática amplamente minada com a implementação da referida lei.

Em mercados paralelos, dados pessoais atingem valores imensuráveis econômica e socialmente falando, permitindo que organizações realizem: análises de público, perfilamento de consumidores, impulsionamento de determinados produtos, serviços ou interesses políticos, através do uso de marketing direcionado, sem intermediários, gerando um retorno financeiro ou de influência bruta considerável.

Um exemplo notório dessa prática foi o caso da *Cambridge Analytica*, envolvendo a venda de dados coletados pelo Facebook contendo informações pessoalmente identificáveis de até 87 milhões de usuários e seu consequente uso para razões políticas impactando as eleições presidenciais norte americanas.

Em razão da importância dos dados exemplificados, este estudo tem como finalidade reforçar a necessidade de proteger os titulares de dados, para que seus direitos e intimidades mantenham-se invioláveis, à luz dos direitos fundamentais amparados constitucionalmente.

Portanto, abordaremos, especificamente, o papel das redes sociais no tratamento de dados pessoais, quais foram os impactos, adequações e imposições exigidas pela Lei 13.709/2018 a essas plataformas massivas e, paralelamente, analisaremos o cenário vigente do tratamento de dados nacional.. Tudo isso, através de extensiva análise e pesquisa dos mais diversos materiais científicos, analíticos, artigos e relatórios disponíveis em nossa doutrina.

Palavras-chave: Tratamento de dados; Imposições e Adequação; Redes Sociais.

ABSTRACT

Implemented in 2020, Law 13.709/2018 – LGPD had a defined scope under the regulators eyes: regulation and legal protection of data subjects. It is notable that, before LGPD, national legislature lacked protection instruments against abusive collection and treatment of personal data, problematic widely mined with the law implementation.

In parallel markets personal data assets reach immeasurable values, socially and economically speaking, allowing organizations: to analyze audiences, profile consumers, boost certain products, services and even political interests using direct marketing tools without intermediaries, generating a much higher gross profitability or influence.

A notorious example of this practice was Cambridge Analytica Case involving commercialization of data collected by Facebook containing personally identifiable information of up to 87 million users and its subsequent usage for Political reasons impacting the North American presidential elections.

Considering the importance of the aforementioned data, this study aims on reinforcing the need for protection of the data subjects, in order that their rights and intimacy are kept inviolable, under the light of Fundamental Rights sustained by the Constitution.

This put, we will address specifically the role of social media on the treatment of personal data, the impacts, adequations and requirements imposed by Law 13.709/2018 to those massive platforms and, concurrently, analyze the current national scenario on data processing. All of which will be carried by means of thorough analysis and research of diverse scientific materials, analytics, articles and reports available in our doctrine.

Keywords: Data Processing; Impositions and suitability; Social networks.

SUMÁRIO

INTRODUÇÃO

Atualmente, a economia cada vez mais é marcada por modelos de negócios que utilizam os dados pessoais para as mais diversas finalidades. Na era do *big data*, definida simplificadamente por Marco Garcia como:

> (...) um conjunto de técnicas capazes de se analisar grandes quantidades de dados para a geração de resultados importantes que, em volumes menores, dificilmente seria possível.
> Em tese, podemos definir o conceito de Big Data como um conjunto de dados extremamente amplos que, por isto, necessitam de ferramentas especiais para comportar o grande volume de dados que são encontrados, extraídos, organizados, transformados em informações que possibilitam uma análise ampla e em tempo hábil (CETAX, 2022).

O principal enfoque é a coleta máxima de dados que se conseguir antes mesmo de saber se tais informações serão úteis. Isso porque esses dados podem ser tratados de forma a auxiliar a tomada de decisão, bem como serem submetidos a procedimentos que podem agregar bastante valor às organizações empresárias.

Também são frequentes as situações onde os indivíduos fornecem seus dados pessoais para poderem utilizar serviços “gratuitos”, caso esse diretamente relacionado às redes sociais, do qual abordaremos especificamente nesse estudo.

São diversos serviços de grande utilidade fornecidos, principalmente na internet, e que podem ser usufruídos sem uma contrapartida pecuniária, no entanto, na imensa maioria das vezes, a utilização dessas aplicações exige que os usuários compartilhem seus dados com as organizações provedoras de tais serviços.

Os chamados “gigantes da tecnologia”, como o Google, Facebook, Twitter, Instagram e YouTube são exemplos disso. Assim, em razão das facilidades que essas organizações oferecem à sociedade, as pessoas toleram fornecer seus dados pessoais em troca desses serviços.

Hoje, é impossível imaginar um mundo no qual os indivíduos não queiram utilizar o mecanismo de busca do Google, redes sociais ou até mesmo smartphones, que coletam dados como informações de geolocalizações mesmo com a desabilitação no dispositivo da opção que permite a coleta dessas informações.

Em contrapartida aos serviços oferecidos, as organizações coletam uma imensa quantidade de nossos dados pessoais. Mas por que oferecer um serviço em troca dessas informações? Qual o valor dos dados pessoais para as organizações empresárias? A

monetização desses dados é legalmente possível? Quais os impactos que a Lei Geral de Proteção de Dados impôs na adequação dessas plataformas sociais a respeito do tratamento de dados pessoais?

O presente trabalho propõe-se a responder essas questões, partindo da hipótese de que a monetização de dados pessoais é legal, entretanto, deve observar parâmetros éticos e jurídicos. Para tanto, será realizada uma pesquisa bibliográfica/documental sobre o tema, bem como serão feitas algumas breves considerações acerca da economia da informação e da monetização de dados pessoais nesse cenário. Em seguida, analisar-se-ão as disposições da LGPD que deverão ser observadas nesse tipo de tratamento de dados e o impacto dessa legislação às maiores plataformas de gerenciamento de dados do mundo, as redes sociais.

1 MOTIVAÇÃO E ORIGEM HISTÓRICA DA LEI GERAL DE PROTEÇÃO DE DADOS

Antes de aprofundarmos os aspetos singulares da referida lei, neste capítulo, consolidaremos primeiramente os fundamentos, as necessidades, e as referências que a originaram, deste modo, analisaremos o contexto político, histórico e socioeconômico à luz das iniciativas tomadas pelos vossos legisladores.

O caráter globalizado que as redes mundiais de computadores nos permitiram vislumbram a partir do início deste milênio faz com que reflitamos acerca da nossa total dependência a esse sistema, e a imprevisibilidade de prosseguirmos em um futuro próximo ou longo sem o auxílio desta é totalmente inimaginável, à luz da conectividade das novas gerações às redes sociais, aplicativos, mercados digitais (no sentido mais amplo possível) e todas as possibilidades que a Internet pode nos prover.

O papel do direito nesse contexto de ultra-conectividade, é, além de regular as relações dela inerentes, acima de tudo, defender os direitos fundamentais que ali estão inseridos, especialmente, o direito à privacidade, que é, sem dúvida, o escopo para a estruturação da LGPD.

Embora a necessidade de proteger a privacidade pareça decorrer do progresso tecnológico, do eminente processo de globalização e do desenvolvimento das plataformas digitais, a preocupação com a proteção da privacidade é antiga e precede a consolidação dos direitos humanos pós Segunda Guerra Mundial, como bem demonstra Warren e Brandeis (1890) em um dos artigos científicos, mais antigos acerca da temática, dissertado no ano de 1890:

> Que o indivíduo deve ter total proteção pessoal e patrimonial é um princípio tão antigo quanto o *common law*; mas tem sido considerado necessário, de tempos em tempos, definir novamente a natureza exata e a extensão de tal proteção. Mudanças políticas, sociais e econômicas implicam o reconhecimento de novos direitos, e o *common law*, em sua eterna juventude, cresce para atender às novas demandas da sociedade. Assim, em tempos muito antigos, a lei dava remédio apenas para a interferência física na vida e na propriedade, para transgressões *vi et armis*. Então, o "direito à vida" servia apenas para proteger o sujeito da agressão em suas várias formas; liberdade significava liberdade de restrições atuais; e o direito à propriedade assegurava ao indivíduo suas terras e seu gado. Mais tarde, veio o reconhecimento da natureza espiritual do homem, de seus sentimentos e seu intelecto. Gradualmente, o escopo desses direitos legais foi ampliado; e agora o direito à vida passou a significar o direito de aproveitar a vida – o direito de ser deixado em paz; o direito à liberdade assegura o exercício de amplos privilégios civis; e o termo "propriedade" cresceu para incluir todas as formas de posse – tanto intangíveis quanto tangíveis (g.n.).

É imprescindível a implementação destes princípios no ordenamento jurídico para que transpareçam e emanem em uma sociedade segura e harmônica, tendo caráter basilar na estruturação até mesmo constitucional, assim, na visão de Krieger (2019), a proteção de dados no Brasil começa a florescer em nossa égide máxima, especificamente em seu Art. 5º, IX, X e XIV, sobretudo, tratando das seguintes garantias fundamentais:

> 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:
> IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
> 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;
> XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional (BRASIL, 1988).

Nesse passo, tratando-se do território nacional, os primeiros instrumentos legais que alcançavam a proteção de dados pessoais e mudavam a concepção sobre a sua importância, foram instituídos a partir da década de 90, um exemplo de legislação nesse sentido é o Código de Defesa do Consumidor (Lei 8.078/90), do qual, em suas disposições, possibilitava ao consumidor acessar informações existentes em cadastros, registros, fichas de dados pessoais e de consumo arquivados sobre ele, permitindo, ainda, a correção ou a alteração desses dados (BRASIL, 1990).

Tomamos também como marco na regulação dos dados pessoas no Brasil a Lei do remédio constitucional Habeas Data (Lei 9.507/97), que regulou o rito do livre acesso de qualquer cidadão a informações relativas a sua pessoa, constantes de registros, fichários ou bancos de dados de entidades governamentais, ou de caráter público (BRASIL, 1997).

No cenário mundial da época, nota-se que cada nação possuía a sua própria legislação protecionista, acerca dos dados pessoais e privacidades individuais.

Em face da inevitável circulação de informações entre países e organizações internacionais, evidenciou-se a necessidade da existência de um controle normativo que permitisse a proteção destes dados, não havendo uma harmonização quanto à sua aplicabilidade, quanto a isto, surge, principalmente na Europa uma tentativa de nortear e harmonizar todas as leis já existentes anteriormente, sendo ela a diretiva 95/46.

Ademais, a Carta Europeia de Direitos Humanos já reconhecia, em seu artigo 8º, a proteção de dados como direito fundamental autônomo, separado do direito à intimidade.

> Artigo 8º. Protecção de dados pessoais
> 1. Todas as pessoas têm direito à protecção dos dados de caráter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente (UNIÃO EUROPEIA, 2000).

Basicamente, o papel fundamental dessa diretiva consistia em reforçar as antigas diretrizes existentes em leis nacionais e gerar segurança jurídica quanto ao processamento de dados em ambientes eletrônicos. O mais importante nesta diretiva foi a padronização, pois exigia-se que todos os países da União Europeia editassem as suas leis a respeito da proteção e do processamento de dados, sendo uma das principais antecessoras da GDPR - *General Data Protection Regulation*.

Em 23 de julho de 2013, mediante matéria da WikiLeaks, fora revelado ao mundo um dos maiores escândalos envolvendo, espionagem, quebra visceral de privacidade e disseminação de dados pessoais da nossa história recente, estamos falando do caso Edward Snowden, do qual, ganhou uma adaptação aos cinemas no ano de 2016, chegando ao Brasil com o título de ‘’Snowden – Herói ou Traidor’’.

Edward Snowden, um ex-técnico da CIA (*Central Intelligence Agence*) de 29 anos acusado de espionagem, vazou informações confidenciais de segurança dos EUA e detalhou alguns dos programas de vigilância que o país usa para espionar americanos utilizando servidores de empresas como Google, Apple e Facebook em vários países da Europa e da América Latina, incluindo o Brasil.

De acordo com as notícias da época fornecidas pelo portal G1 (2013), os detalhes expostos por Edward diziam respeito, sobretudo, a utilização de softwares, em especial o *PRISM*, do qual tinha a funcionalidade de vigiar em escala global as informações transmitidas na rede mundial de computadores. Esses mecanismos de captação de dados, garantiam uma capacidade de coleta de informações massivas, o seu uso não somente era direcionado ao combate ao terrorismo, como, também, para espionagem política, uma vez que qualquer indivíduo poderia ter a sua privacidade facilmente violada, desde um mero cidadão até um presidente da república.

Isso pois, no Brasil, a situação foi extremamente crítica, Snowden revelou na época que avaliaram as conversas entre a presidente Dilma Rousseff (PT-SP) e seus principais assessores. A mobilização nacional foi imediata, o governo vigente revelou publicamente sua indignação com o acontecido e afirmou que faria alianças com outras nações atingidas pela afronta direta da inteligência norte-americana para reverter a situação.

Esse episódio lamentável ampliou ainda mais o senso de urgência em relação a aprovação do Projeto de Lei 2126/11, vindo se tornar o Marco Civil da Internet, passando a vigorar em 2014 abordando em sua legislação princípios garantidores da privacidade individual e proteção de dados, sendo uma lei basilar para a disseminação da consciência de dados no Brasil, abrindo o caminho para legislações futuras, tais como a LGPD.

Em seu Art. 3º e 7º (Marco Civil da Internet - Lei 12.965/2019) podemos notar claramente a preocupação da Lei de estabelecer e propagar esses princípios:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet.
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei (BRASIL, 2014).

O controle digital é essencial quando se entende que a comunicação e o próprio fluxo de informações constituem uma forma de poder sobre as informações descritas, de modo que a relação entre os agentes que controlam esse fluxo de informações e a pessoa que fornece suas informações é desequilibrada “torna-se evidente, portanto, que o poder da informação em um contexto em que a tecnologia está baseada na comunicação e na transferência de informação e dados pode ser tão nefasto quanto o poderio bélico almejado, por séculos, pelas nações, como um indicador de poder e de domínio sobre os povos” (FORTES, 2016).

O Marco Civil regulamenta não apenas as práticas e condutas na Internet, mas também os direitos e garantias dos usuários da Internet, com ênfase especial nos conteúdos considerados essenciais ao fluxo da Internet, comunicações e dados. Ademais, expandir exponencialmente

os tópicos abarcados pela legislação brasileira em relação aos serviços prestados por provedores de Internet e sites em geral, foi instrumental na expansão da proteção de dados mais alinhado ao paradigma da privacidade, dedicando uma seção própria para a matéria, cobrindo até aquele ponto a necessidade de resguardar a privacidade do usuário diante dos possíveis abusos que pudesse surgir contra o internauta.

1.1 GDPR – INSPIRAÇÃO À LGPD

Em 27 de abril de 2016, fora aprovada a GDPR – *General Data Protection Regulation*, passando a vigorar somente em 2018.. A GDPR, sucessora da Diretiva 95/46/EC, apresenta-se como uma lei de força coercitiva e alcance mais amplo, incorpora em seu texto conceitos modernos sobre a aquisição e disseminação de dados para cidadãos europeus que utilizam a Internet. Ainda preocupado com a dimensão internacional da questão, segundo Ronaldo Lemos, o GDPR é uma legislação de caráter "viral" (LEMOS; PACETE, 2018), pois visa criar um efeito dominó, enfatizando que sites e empresas, mesmo fora do território europeu, devem obedecê-la, quando forem utilizados por cidadãos europeus.

Podemos citar como alguns dos objetivos das GDPR:

> a) contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico e social, a consolidação e a convergência das economias no nível do mercado interno e para o bem-estar das pessoas físicas;
> b) assegurar um nível coerente de proteção das pessoas físicas no âmbito da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno;
> c) garantir a segurança jurídica e a transparência aos envolvidos no tratamento de dados pessoais, aos órgãos públicos e à sociedade como um todo;
> d) impor obrigações e responsabilidades iguais aos controladores e processadores, que assegurem um controle coerente do tratamento dos dados pessoais;
> e) possibilitar uma cooperação efetiva entre as autoridades de controle dos diferentes Estados-Membros (INTERSOFT CONSULTING, 2016).

Segundo Patrícia Peck Pinheiro (2018), o referido dispositivo além de inovar as legislações já existentes padroniza e normaliza o que seriam os atributos qualitativos da proteção dos dados pessoais, esses atributos buscam equilibrar as relações em um cenário de negócios digitais sem fronteiras, caso omissos, gerariam sérios impactos às esferas sociais, econômicas e políticas.

Para efeitos no Brasil, a GDPR impulsionou a criação de uma legislação nacional que tratasse de proteção dos dados pessoais com uma maior abrangência do que aquela apresentada

anteriormente pela Lei 12.965/2019 (Marco Civil da Internet), espelhando-se diretamente nas implementações de caráter internacional, pois a GDPR não autoriza que empresas europeias que estejam relacionadas com o tratamento de dados de alguma maneira, relacionem-se com empresas de outros países caso essas não possuíssem algum tipo de legislação referente ao tratamento de dados do usuário ou privacidade. A sua implementação impactou demasiadamente as relações de mercado na Internet criando um efeito dominó, demandando que os sites e prestadores de serviço se adequassem a norma, caso desejassem continuar exibindo suas propagandas e anúncios e, consequentemente, mantendo a rotatividade de vendas.

Nesse passo, a legislação brasileira não encontrou outra alternativa senão a elaboração um diploma nesse sentido, a Lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

Importantíssima também é, a contextualização do escândalo envolvendo a empresa britânica *Cabridge Analytica* e o Facebook, servindo ainda mais como propulsor à elaboração e desenvolvimento da LGPD (MACIEL, 2019, p. 15). O episódio alarmante e midiático envolveu a gigante das redes sociais, onde foram expostas informações acerca da coleta irregular dos dados pessoais dos usuários, com o intuito de armazená-los em um enorme banco de dados, traçando o perfil comportamental, gostos e referências deles. As investigações indicam uma utilização dos dados direcionados a impactar o resultado das eleições norte-americanas (GOGANI, 2018) e brasileiras, através da atuação política direta. Além disso, os dados de aproximadamente 50 milhões de usuários foram encaminhados ao envio de publicidade na Grã-Bretanha, levantando-se inúmeras suspeitas, na época, que o referido armazenamento desses dados contribuiu na votação para a saída do Reino Unido da União Europeia.

Elucida, Bruno Ricardo Bioni (2018, p. 1), o caráter alarmista que o incidente despertou, sendo a demanda por uma legislação mais protecionista simplesmente imediata:

> Ainda faltava o ingrediente mais quente para eclodir a pauta da proteção de dados pessoais em 2018: o escândalo da *Cambridge Analytica* escancarou como a desproteção de dados pessoais impacta não só a vida de um cidadão em específico, mas de toda uma coletividade e os alicerces do que se entende por democracia. Logo depois, houve uma sessão temática no Senado para debater, pela primeira vez no plenário em uma das Casas do Congresso Nacional, o tema. E, em maio de 2018, a Câmara dos Deputados realizou também um seminário como decorrência do referido escândalo.

Por fim, ainda citando Bioni (2019), ele separa a consolidação das regulamentações de dados pessoais em quatro gerações. A primeira evidencia a preocupação com o processamento em larga escala de dados pessoais na esfera governamental, as normas, em sua maioria, possuíam um caráter rígido, regulando o uso da tecnologia, no que diz respeito ao processamento e coleta dados pessoais dos que compõem o governo. A segunda geração pende ao caminho regulatório, envolvendo não apenas dados pessoais de funcionários do governo, mas também dados pessoais de domínio privado e, portanto, transferindo a responsabilidade de mantê-los seguros aos seus próprios detentores, as informações que poderiam ser utilizadas dependiam tão somente do consentimento de a quem elas cabiam. A terceira, aborda a esfera participativa do indivíduo durante o decorrer do processo de coleta ao compartilho da informação. A quarta e última geração de dados, até o momento, trata da regulamentação dos dados pessoais sensíveis, com leis que priorizam os titulares dos dados frente a terceiros que possam manipular suas informações pessoais, retirando a autonomia do indivíduo e passando-a ao Estado.

2 PRIVACIDADE DIGITAL

Abordamos no tópico anterior a importância magistral da privacidade na harmonização social, tanto individual quanto coletivamente, e como, ao longo das décadas, esse direito foi consolidando-se como a base estrutural da nossa vida quotidiana, reformulando-se e aprimorando-se por meio de diversas legislações, no Brasil e no mundo, para alcançar o máximo de proteção possível ao indivíduo.

A LGPD em seu Art. 1º, tem com base justamente o combate a violação da privacidade individual e a segurança dos direitos fundamentais a liberdade e privacidade:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Dito isto, trataremos desse direito fundamental tão importante em um cenário de inúmeras possibilidades, em um contexto de hiper-conectividade, a internet. A privacidade na internet, consequentemente, manifesta-se através dos dados pessoais de seus usuários, sendo assim, vislumbraremos como esses dados podem ser resguardados para garantir a vossa blindagem.

A liberdade de expressão cumulada a autonomia na divulgação de dados, permite com que o indivíduo produza na rede uma vasta gama de detalhes sobre a sua vida, isso somado a uma necessidade de conectividade, seja para interesses profissionais ou para manter uma vida social ativa, faz com que a distinção entre a vida privada e a vida pública encurtem-se cada vez mais, ou seja, a intimidade da vida privada não pode ser interpretada da mesma forma de décadas atrás.

A facilidade para encontrarmos algum conhecido ou amigo em comum, através de algoritmos e softwares de busca só comprova a narrativa acima, uma vez que as redes socais propiciam uma visibilidade e exposição avassaladora, viabilizando também a possibilidade de divulgação e compartilhamento de informações pessoais por terceiros. Nas palavras de Rodotá (2008, p. 92) a privacidade digital pode ser caracterizada pela condição que o indivíduo detém o controle sobre as suas próprias informações, prevalecendo o livre-arbítrio, e valorizando o novo poder do indivíduo sobre o tratamento de seus dados. Ademais, ele relaciona a proteção de dados diretamente ao direito de personalidade e não de propriedade, haja vista que a

propriedade relaciona-se diretamente aos meios econômicos, enquanto, os dados pessoais sensíveis não estão, teoricamente, relacionados a fins negociais.

Na medida que o fortalecimento e a autonomia do indivíduo sobre as suas informações se fortalecem, os riscos gerados pela exposição às inseguranças nas redes emergem paralelamente, seja pela ameaça na disseminação de dados, ataques *hacker*, compartilhamento de conteúdo abusivo ou vexatório, ou qualquer outra possibilidade da qual comprometa a privacidade do usuário, deste modo, cabe ao legislador tutelar esse meio, coibindo qualquer tipo de interferência e mantendo esse direito inabalável.

A grande dificuldade de blindarmos totalmente o direito fundamental à privacidade na era da informação é justamente pelo caráter dinâmico e conectado que ela demanda, além disso, um dos fatores determinantes para a flexibilização desse direito se dá justamente pela retenção de dados pessoais indiscriminadamente, em virtude da segurança pública (fiscalização, vigilância e registro governamental), através da coleta de dados dos cidadãos mediante atuação da administração pública, e, bem como, em decorrência das práticas de mercado, nas quais há uma coleta e retenção de dados massiva por parte das empresas, com o intuito de distribuí-los, vendê-los e usá-los em benefício próprio, seja para pesquisas comerciais, artifícios publicitários, prospecção de clientes, ou outras diversas possibilidades.

Conforme aduz Mendes e Branco (2015, p. 294), a privacidade restringe-se observando a natureza da vida social, o interesse coletivo e público conforme exemplificamos acima. Os direitos fundamentais são impassíveis da renúncia integral, contudo, existem autolimitações, preservando a dignidade humana em qualquer hipótese, a exemplo disso, circunstâncias em que o indivíduo renuncia expressamente ao seu direito à privacidade, exibindo a sua vida pessoal em suas redes sociais, seja compartilhando fotos de sua família, amigos, gostos e pensamentos, esse princípio não é violado.

Conclui ele que, tratando-se do interesse público, casos jornalísticos, midiáticos e de grande cobertura da imprensa, quando coexistirem os direitos e conflitos entre à liberdade de informação e a privacidade do noticiado, deve ser levado em conta se o interesse público sobreleva a dor íntima que o informe provocará, portanto, a lei deve promover mecanismos de combate a conteúdos que assediem de qualquer forma o indivíduo objeto da notícia, pautando-se na ética, bom-senso e empatia, dando autonomia ao indivíduo para controlar o processamento das suas informações pessoais, sob pena de afrontar a sua privacidade.

A privacidade digital constitui-se, portanto, do respaldo legal que indivíduo tem acerca da proteção de seus dados pessoais e sensíveis, podendo, em ocasiões circunstanciais, ser

renunciada em prol da divulgação ou exposição feita por ele. Para tanto, precisamos compreender como ocorre a proteção desses dados por parte das plataformas digitais, empresas, redes sociais e derivados.

2.1 PARADOXO DA PRIVACIDADE E RELAÇÃO DE CONSUMO NAS REDES SOCIAIS

Na definição de Kokolakis (2017), o paradoxo da privacidade é um fenômeno impulsionado pela ascensão das atividades comerciais, sociais e de lazer no ambiente digital, para haver o acesso a esses serviços, consolidando uma relação mutualista, tais atividades estão diretamente atreladas ao fornecimento de informações/dados pessoais pelo usuário, propiciando, consequentemente, a fragilização dessa privacidade.

Em suma, ele ocorre quando há uma violação da privacidade pela vontade e consentimento do próprio sujeito, observa-se, na verdade, uma necessidade de ‘’pertencimento’’ irresistível ao cenário das redes sociais, quando o simples fato de não integrá-lo abraça uma ideia de ruptura das relações interpessoais, de modo que Taddicken (2013) identifica que a relevância social, seja pelo benefício das redes sociais, contagia os usuários a disponibilizarem suas informações ao utilizarem tais ferramentas. Os benefícios sociais dos usuários das redes sociais são tão significativos que são explícitas as flexibilizações quanto à cautela no âmbito da privacidade, havendo uma redução na tolerância significativa referente a coleta de dados por parte de empresas como Facebook, WhatsApp e Instagram, permitindo a compilação, coleta e utilização desses dados para fins de propaganda.

Um meio eficaz para que possamos estabelecer um ambiente mais seguro nas redes são as políticas de privacidade. Tais adereços têm o papel de informar ao usuário, quais serão os dados e informações solicitadas a ele, como serão coletadas, a finalidade desta coleta e por quanto tempo serão armazenadas. Na esmagadora maioria dos aplicativos e serviços on-line precisamos confirmar a nossa confirmação de leitura das políticas de privacidade para ingressarmos ao uso do serviço, isso é notório, contudo, esses documentos são amplamente conhecidos por seu tamanho, em muitas vezes, excessivos e desproporcionais, com terminologias técnicas que ocasionam o desinteresse do leitor, propiciando uma aceitação consentida, mas também a ‘’ocultação’’ das condições impostas.

Segundo Loewenstein (2015), ao passo do desenvolvimento das relações informacionais na era digital, compreende-se que natureza dos riscos apresentados pela Internet relacionados à

privacidade, representados pela exposição que as informações pessoais podem causar aos usuários, faz com que crie-se um senso de preocupação quanto à privacidade digital, ocasionando uma mudança gradual. No entanto, como observado acima, os benefícios sociais, emocionais e econômicos, ainda desempenham um papel na mitigação das preocupações com a privacidade, retardando esse processo.

Conclui-se a existência de um impasse, cabe ao indivíduo a opção da escolha nessa relação de perdas e ganhos, deve ele determinar o quão valorosa e inviolável é a sua privacidade, na medida que, os ganhos sociais, econômicos e emocionais das redes sociais são uma realidade, além de aumentarem a produtividade, dinamismo e agilidade (WhatsApp, Telegram, Messenger) até mesmo no ambiente profissional , contudo, é necessário compreender que estará ele a mercê das políticas de privacidade supracitadas, ficando refém dos termos estipulados pelos prestadores de serviço para coleta, tratamento e armazenamento de dados.

Por outro lado, a relação de consumo estabelecida entre essas plataformas pode gerar algumas indagações por parte do consumidor. As redes sociais, ao ofertarem seus serviços gratuitamente a qualquer cidadão podem gerar a falsa impressão de que o próprio usuário é o produto, fonte de um marketing específico, ofertando ao usuário diretamente a mercadoria correspondente ao seu perfil, e consequentemente, a rede é financiada por outros investidores e anunciantes.

O fundador do Facebook, Mark Zuckerberg, em seu testemunho ao Comitê de Energia e Comércio da Câmara dos Estados Unidos, relatou que o Facebook consegue traçar o perfil até de pessoas que não estão dentro da rede social: "Em geral, coletamos dados de pessoas que não se inscreveram no Facebook para fins de segurança" (CRUZ, 2018).

Ou seja, essa prática de coleta é obviamente comum no mercado das redes sociais e ocorre até mesmo com usuários que sequer estão cadastrados no Facebook, que dirá os que estão, a conduta da venda de dados a empresas investidores não restringe-se somente ao Facebook, podendo ocorrer com qualquer outra rede.

Contudo, caracterizar o usuário como produto deslegitima a relação com a administradora das redes sociais, minimizando-o e rotulando-o, criando um afastamento entre ele e suas garantias na medida que não reconhece-se mais o estado de vulnerabilidade dele, desumanizando e despersonalizando o sujeito, e com ele, os seus direitos fundamentais.

O usuário é um legítimo consumidor do serviço, não podendo ser confundido como um ‘’produto subjetivo’’ pelo viés gratuito da plataforma utilizada, isso pela interpretação plena do Art. 2º e 3º do Código de Defesa do Consumidor:

> Art. 2° Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final.
>
> Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços (BRASIL, 1990).

Por fim, é necessário deixar claro que no Código de Defesa do Consumidor, como direito, é completamente possível por parte do usuário solicitar correções de quaisquer erros que possam ser encontrados em seu cadastro, dando o prazo de até cinco dias para a empresa corrigi-lo, conforme dispõe o seu Art. 43, § 3:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
>
> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

A LGPD aborda o mesmo assunto, concedendo ao usuário detentor dos dados o poder de ter sua informação corrigida de qualquer inexatidão existente. A diferença entre os ordenamentos, no entanto, é o meio pelo qual poderá pleitear esse direito, não sendo necessário o titular dos dados ir até um local físico para realizar a mudança, podendo realizá-la pela internet ou por telefone celular, bastando acessar o site da prestadora dos serviços.

2.2 DOS DADOS PESSOAIS

De acordo com o site do Governo Federal (MINISTÉRIO DA CIDADANIA, 2021) podemos classificar os dados pessoais em quatro espécies: não sensíveis, sensíveis, dados públicos e dados anonimizados. Os dados não sensíveis correspondem ao domínio privado de seu titular, são aqueles que possibilitam a identificação, direta ou indireta, da pessoa viva (ex: RG, CPF, Nome, Endereço), respaldados pelo Art. 5º, I da LGPD: "Art. 5º Para os fins desta

Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018).

Enquanto, os dados sensíveis, na própria concepção da União, são aqueles que:

> (...) estão sujeitos a condições de tratamento específicos, ou seja, que exigem maior atenção: sobre crianças e adolescentes; e os "sensíveis", que são os que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa (MINISTÉRIO DA CIDADANIA, 2021).

E, nos moldes do Art. 5º, II da LGPD:

> 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 (BRASIL, 2018).

Ainda sobre os dados sensíveis, abordando e tutelando os direitos dos menores de idade e sua preservação, a orientação aponta que:

> (...) é imprescindível obter o consentimento específico de um dos pais ou responsáveis e se ater a pedir apenas o conteúdo estritamente necessário e não repassar nada a terceiros. Sem o consentimento, só podem ser coletados dados para urgências relacionadas a entrar em contato com pais ou responsáveis e/ou para proteção da criança e do adolescente. Sobre os dados sensíveis, o tratamento depende do consentimento explícito da pessoa e para um fim definido. E, sem consentimento do titular, a Lei Geral de Proteção de Dados Pessoais define que isso é possível quando for indispensável em situações ligadas: a uma obrigação legal; a políticas públicas; a estudos via órgão de pesquisa; a um direito, em contrato ou processo; à preservação da vida e da integridade física de uma pessoa; à tutela de procedimentos feitos por profissionais das áreas da saúde ou sanitária; à prevenção de fraudes contra o titular (MINISTÉRIO DA CIDADANIA, 2021).

Os dados públicos são enquadrados pelo Art. 7º, § 4º da Lei 13.709:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I – mediante o fornecimento de consentimento pelo titular; (…)
> § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta lei (g.n.) (BRASIL, 2018).

O seu titular, mediante previsão deste dispositivo, tem a possibilidade de tornar o seu dado pessoal público caso seja de sua vontade, observando a boa-fé, o interesse público e o princípio constitucional da publicidade.

Por fim, os dados anonimizados são aqueles que, originalmente, eram referentes a um indivíduo, mas, através do seu processamento, não é possível traçar um caminho que vincule esse dado ao seu titular de origem. Se um dado for anonimizado, então a LGPD não se aplicará a ele.

Os grandes problemas decorrentes das conceitualizações de dados sensíveis estão relacionados as avaliações necessárias para seu uso. Os dados só são sensíveis quando usados de forma discriminatória, portanto, seu destino afeta suas características. Qualquer dado pode ser considerado sensível se usado de maneira incorreta, assim como os dados considerados sensíveis podem ser utilizados em uma atividade não discriminatória. Por isso, é de suma importância e significância a proteção de todos os dados, por mais que aparentem ser menos importante, podendo eles virem a tornarem-se sensíveis, a depender do tipo de tratamento a que serão expostos.

Nas palavras de Tatiana Malta Vieira (2007):

> Ressalte-se que, mesmo os dados não sensíveis podem necessitar de proteção – garantindo-se sua integridade, autenticidade e confidencialidade – uma vez que, ao serem confrontados com outros dados, podem revelar aspectos que o titular gostaria de manter em sigilo, por afrontarem diretamente seu direito à privacidade. Ainda que certos dados pessoais não deixem transparecer mensagem significativa, quando analisados isoladamente, devem ser submetidos a procedimentos e medidas especiais de proteção, pois, uma vez agrupados, permitem a definição do perfil de seu titular.

Os dados pessoais sensíveis são os mais impactantes por toda a sua conjuntura abrangente e por velarem, resguardarem, a intimidade do indivíduo, de forma, que a ruptura ou exposição desses dados poderia gerar um enorme impacto emocional, profissional e consequencias inimagináveis ao usuário.

3 UTILIZAÇÃO DOS DADOS PESSOAIS E MUDANÇAS IMPLEMENTADAS PELA LGPD NAS REDES SOCIAIS

Conforme apontado acima no tópico paradoxo da privacidade, os termos de privacidade compõem o contrato de adesão na rede social, implicando na submissão do usuário às medidas e normas da plataforma para a sua permanência nela, não existindo, espaço para negociação de cláusulas ou privilégios. Dito isto, apontaremos os riscos e quais são as medidas das redes para a proteção dos dados dos internautas.

Um pequeno parênteses somente para lembrarmos que nenhuma empresa é isenta do cumprimenta das normas impositivas da Lei Geral de Proteção de Dados, sendo irrelevantes os quesitos da sua dimensão, faturamento ou abrangência, no sentido mais amplo possível da palavra, para que a a aplicabilidade legal incorra sobre ela. A lei abrange o ramo empresarial de direito público e privado, tendo essas empresas, a obrigação de adequarem-se a norma.

Primeiramente, vale ressaltar que é muito interessante para as plataformas sociais manterem a manutenção ativa e constante de seus usuários, principalmente para o aumento do compartilhamento dos dados, impulsionando e movimentando a iniciativa das empresas parceiras face às informações colhidas. É necessário que fique muito claro que, teoricamente (vista os escândalos de vazamento de dados analisados anteriormente), as redes sociais são terminantemente proibidas de vender os dados dos usuários. O Facebook, por exemplo, assegura que não vende a seus anunciantes os dados pessoais identificáveis ou os dados agregados, o que é vendido, na verdade, é a possibilidade de que um anunciante alcance, entre os usuários da plataforma, o seu público-alvo, multiplicando assim a eficácia de sua campanha.

Ryan Matzner (2018), cofundador do Fueled (empresa de desenvolvimento de aplicativos) faz as seguintes considerações sobre o tratamento de dados no Facebook: "o Facebook não está no negócio da venda de dados, está no de venda de pixeis".

A Meta, dona do Instagram, WhatsApp e Facebook, apresenta em suas políticas de privacidade as seguintes diretrizes, nesse caso tomaremos exemplo as políticas do Facebook, pelo seu caráter generalista, explicando o porquê do tratamento das informações dos usuários e como isso é feito:

> Personalização dos Produtos da Meta: nossos sistemas tratam automaticamente as informações que coletamos e armazenamos sobre você e outras pessoas. O objetivo disso é avaliar e compreender seus interesses e suas preferências, bem como proporcionar experiências personalizadas nos Produtos da Meta de acordo com os nossos termos. É assim que nós:

> Personalizamos recursos e conteúdos (como o Feed de Notícias e o Feed do Instagram e o Stories);
> - personalizamos os anúncios que as pessoas veem; e
> - apresentamos sugestões para você (como pessoas que talvez você conheça, grupos ou eventos que podem ser do seu interesse ou tópicos que você pode querer seguir) dentro e fora dos nossos produtos.
> Fornecimento e melhoria dos nossos Produtos da Meta: o fornecimento dos Produtos da Meta inclui a coleta, o armazenamento e, quando relevante, o compartilhamento, a definição de perfil, a análise e a seleção e, em alguns casos, não apenas o tratamento automático de dados, mas também a análise manual (humana) para fazer o seguinte:
> - Criar e manter sua conta e seu perfil;
> - facilitar o compartilhamento de conteúdo e de status;
> - oferecer e selecionar recursos;
> - fornecer serviços de envio de mensagens, a capacidade de fazer ligações de voz e de vídeo e se conectar com outras pessoas;
> - fornecer novos produtos de publicidade; e
> - realizar análises (g.n.) (META, 2022).

Nesse passo, a Meta enquadra também inúmeras informações que coleta dos usuários, em uma breve análise pode-se observar que basicamente tudo que se é publicado, postado ou comentado está sob a sua sentinela, não escapando uma mísera informação dos olhos, ou melhor, das linhas de código do algoritmo:

> - O conteúdo criado, como publicações, comentários ou áudios.
> - O conteúdo fornecido por meio do nosso recurso de câmera, das configurações do rolo da câmera ou dos nossos recursos habilitados para voz. Saiba mais sobre o que coletamos desses recursos e como usamos as informações da câmera em máscaras, filtros, avatares e efeitos.
> - As mensagens enviadas e recebidas, incluindo o conteúdo, sujeitas às leis aplicáveis. Não podemos ver o conteúdo de mensagens criptografadas de ponta a ponta a menos que os usuários as denunciem para análise.
> - Os metadados sobre conteúdo e mensagens, sujeitos às leis aplicáveis
> - Os tipos de conteúdo visto ou com o qual você interage e o modo como faz isso.
> - Os aplicativos e recursos usados e quais ações você realiza neles.
> - As compras ou outras transações efetuadas, incluindo informações de cartão de crédito.
> - As hashtags usadas.
> - O horário, a frequência e a duração das suas atividades nos nossos Produtos
> - Informações com proteções especiais
> - Talvez você forneça informações sobre a sua religião, preferência política, pessoas em quem você tem interesse (o que pode revelar sua orientação sexual) ou saúde nos acontecimentos ou campos de perfil do Facebook. Essas e outras informações (como origem racial ou étnica, crenças filosóficas ou filiações sindicais) podem ter proteções especiais de acordo com as leis do seu país (g.n) (META, 2022).

Adequando-se e aludindo diretamente a LGPD, a Meta também sinaliza nas suas políticas de privacidade que, de acordo com esse ordenamento, você tem o direito de acessar, retificar e apagar seus dados, além de autorizar o seu tratamento e solicitar a sua portabilidade.

Assim, uma das grandes contribuições advindas da Lei 13.709 determina que todas as empresas ou órgãos públicos só poderão guardar ou usar dados pessoais com o consentimento

expresso dos usuários. Sendo expressa em determinar que, se uma rede social ou até mesmo uma empresa de telemarketing utilizar ou divulgar seu nome, endereço ou qualquer tipo de dado pessoal fornecido, sem permissão ou qualquer base legal, é passível de processo do disseminador desse dado.

A legitimidade do tratamento de dados é atribuída a uma hipótese legal, o legislador pautando-se nos princípios do Art. 1º da Lei 13.709 (proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural), elaborou em seus Arts. 7º e 11º as hipóteses para o tratamento dos dados pessoais não sensíveis e sensíveis, respectivamente:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os

> direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (g.n.) (BRASIL, 2018).

É nítido que a repetição e fixação pelo substantivo ‘’consentimento’’ não é vã, a autonomia e o livre – arbítrio que é disponibilizado ao usuário, assegurando-o de sofrer qualquer medida abusiva e coercitiva das plataformas sociais, na medida que, sem o seu prévio consentimento, qualquer procedimento de tratamento de dados torna-se simplesmente inviável e ilegal nos moldes da LGPD.

Todo e qualquer tratamento deverá ser informado ao seu titular, a antiga prática empresarial e costumeira de angariar dados, reforçando e criando uma base de informações, com propósito comercial, seja para a venda ou benefício próprio, sem consentimento dos titulares, é completamente inimaginável nos dias de hoje. A Lei Geral de Proteção de Dados vem nitidamente preencher a lacuna legal do tratamento de dados e regulamentar a forma controversa como as empresas costumavam tratar e gozar dos dados pessoais de seus usuários indiscriminadamente.

Ao vigorar da LGPD em 2020, qualquer pessoa jurídica de direito público ou privado, órgão ou entidade e até mesmo, pessoas naturais, que pretendessem tratar dados pessoais com uma finalidade econômica, deveriam adequar-se as hipóteses de tratamento supramencionadas (Art. 7º e 11º – Lei 13.709/2018), caso pretendessem manter a continuidade de suas atividades sem sofrerem as sanções cabíveis, é claro.

Lembrando somente que, conforme já observamos no tópico 3.2, ao classificarmos os dados pessoais, verificamos a existência dos dados pessoais tornados manifestamente públicos pelo seu titular, o titular do dado ao realizar a publicação deste, expondo para a sua rede de amigos, conhecidos e terceiros, dispensa também o seu consentimento para que este dado seja tratado (Art. 7º, § 4º - LGPD). Obviamente, a falta de consentimento do usuário não inibe a incidência dos princípios e às garantias dos direitos do titular. Quando pensamos no contexto das redes sociais, os dados manifestamente públicos são a base da coleta de dados.

Existe uma diferença entre os dados pessoais de acesso público (Art. 7º, § 3º) e entre os dados tornados manifestamente públicos pelos seus usuários, devendo o tratamento destes considerar a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização. Não é possível simplesmente coletarmos deliberadamente de uma base de dados pública, nome, telefone, e-mails para fins comerciais sem nenhuma relação, vínculo ou questão pública relacionada ao titular.

O ônus da comprovação e validação do consentimento do usuário é da empresa, do controlador daqueles dados, sendo ele inequívoco, informado e expressamente manifesto pelo titular, considerando a possibilidade, inclusive, da revogação deste consentimento a qualquer momento, mediante manifestação do seu detentor e sem nenhum tipo de onerosidade, nos moldes do Art. 8º, § 5º da LGPD:

> 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.
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei (BRASIL, 2018).

Sem prejuízos quanto às terminologias técnicas, a definição do controlador e operador de dados é disposta pela Lei Geral de Proteção de Dados, em específico em seu Art. 5º, VI e VII:

> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (BRASIL, 2018).

A seguir, observaremos alguns aspectos sobre adequação e governança, primordiais e basilares para a consolidação de diversas empresas e corporações no mercado concorrencial principalmente após a implementação da LGPD, sem uma boa gestão, instrução e falta de conhecimento, os riscos aos tratamentos de dados dos usuários são diretamente proporcionais aos riscos e responsabilidades empresariais.

3.1 APONTAMENTOS SOBRE ADEQUAÇÃO E GOVERNANÇA

Dada a vastidão na variedade das redes sociais (TikTok, Instagram, Snapchat, Twitter, Messenger e outras), estabelecer uma identidade de marca é fundamental em um mercado tão competitivo e voraz, preservando a garantia dos conceitos criativos, uma vez que a luta pela atenção e tempo do usuário em suas plataformas é cada vez mais intensa e, em contrapartida, a atenção do usuário é nitidamente diluída entre as extensas opções. Essa guerra pelo tempo do usuário no mercado digital não limita-se somente às redes sociais, de maneira alguma, ela é uma cobiça das multinacionais que estende-se por todos os ramos do mercado.

A lógica é simples, tudo aquilo que o usuário, consumidor, cliente, usufrui além do meu serviço, que demande o tempo e a atenção dele, e faça com que ele migre do meu serviço para outro, é considerado concorrência. Nesse caso podemos sim considerar que empresas como Facebook, Twitter, TikTok, Amazon Prime Video, Netflix, Youtube, Twitch a até mesmo a PlayStation estão concorrendo diretamente entre si pelo preciosíssimo tempo do usuário, na medida que, ao jogar vídeo game, assistir séries e filmes, realizar ou acompanhar uma live, você involuntariamente deixa de consumir, por exemplo, as redes sociais.

Dito isto, a consolidação e estruturação da marca em um mercado tão competitivo é fundamental para a vida útil de uma empresa, para isso a governança de marca ou *brand governance*, como é conhecida nos Estados Unidos, vêm para alcançar propostas de melhor experiência ao cliente.

A ambição pelo engajamento impulsiona ainda mais a complexidade dos canais de marketing das empresas. A governança propicia que os profissionais atentem-se a aderência aos elementos obrigatórios da marca e às práticas recomendadas por cada plataforma de mídia.

As tecnologias atuais propiciam o emprego de inteligência artificial e análise de dados o gerenciamento automático dos ativos de marca e fornecer percepções para a sua otimização. Elas removem a tensão entre os valores da marca e as metas de desempenho de marketing, provendo não apenas as melhores práticas, mas também dados e insights em tempo real. Isso torna o processo criativo mais mensurável e transparente.

Tais ferramentas dispõem uma visão clara e intuitiva de todos os ativos criativos em reprodução e podem ser filtrados por região e plataforma para sinalizar anúncios que não seguem as práticas recomendadas. Algumas das soluções mais avançadas podem ser analisadas antecipadamente.

Disserta Alex Collmer (2021), a respeito do papel da governança em funçção da adequação das empresas a LGPD:

> A governança da marca também facilita a adesão às regulamentações como a LGPD, garantindo que as campanhas não violem a privacidade do consumidor. Além disso, reduz a dependência de segmentação comportamental de rastreamento cruzado, que pode prejudicar a reputação da marca, ajudando a otimizar o envolvimento dos consumidores

Para Alex Collmer (2021), são quatro os passos para a implementação da governança de uma marca nas redes sociais: definição de critérios; apontamento dos ativos criativos; monitoramento de desempenho e; percepções de melhoria.

Além disso, é imprescindível que sejam elaboradas políticas e procedimentos internos de governança que auxiliem e estabeleçam parâmetros e diretrizes para o tratamento dos dados, principalmente nos departamentos de marketing e comerciais (geralmente responsáveis pelo tratamento).

Alinhado a essa documentação acima listada, apresentam-se em caráter suplementar os treinamentos e as ações de conscientização, afinal um polo profissional despreparado e negligente não é de nenhuma valia, independente de políticas e procedimentos internos. Nesse sentido, a qualificação do profissional é um quesito básico, sendo a conscientização uma ferramenta de blindagem, contribuindo, invariavelmente, com a sua especialização.

Um dos pilares mais importantes para a manutenção da governança, sem dúvida, são os avisos de privacidade ou políticas de privacidade, já exemplificados no tópico 4. Através dessa ferramenta é possível apresentar ao titular dos dados informações referentes a transparência do tratamento, a sua finalidade, quais os direitos que ele possui e por qual canal ele pode contactar a empresa para exercício desse direito. Esses avisos poderão ser disponibilizados em sites, plataformas e, preferencialmente, na própria rede social, facilitando o acesso do usuário.

Finalmente, o último quesito relevante à governança é a possibilidade de avaliação de terceiros, a contratação de assessorias de marketing, de imprensa, para a realização desse tratamento. Possibilitando um ecossistema integrado de proteção e não somente uma área exclusiva e singular da empresa.

3.2 *WEB SCRAPING* NAS REDES SOCIAIS

Certamente, em algum momento de nossas vidas, já fomos abordados por empresas, das quais temos ou não vínculos, mediante e-mails ou ligações telefônicas, oferecendo incessantemente seus produtos e serviços, ocasionando desconforto e aborrecimento. A identificação de um sujeito para aquela oferta, ou meramente a oferta massiva e indiscriminada de um ‘’presente’’, travestindo a venda, incorpora o termo em inglês *fishing*, traduzido para pescaria, fisgando o cliente e intrometendo-se em ambientes privativos.

Ao desenvolver da Inteligência Artificial, a sua dinamização e eficiência expressivamente maiores em relação aos esforços humanos massivos fez com que a prática de *fishing* mediante serviços de *telemarketing* fosse substituída gradativamente. A necessidade de centenas, e até milhares, de funcionários de debruçarem-se sobre guias telefônicas contendo o nome de pessoas, seus números de telefone e endereço chegou ao fim.

Atualmente, mecanismos tecnológicos conseguem captar automaticamente, desde a simples raspagem indiscriminada de dados até aquelas que são parametrizadas, chegou-se até a raspagem de dados automatizada (*Data Scraping*), quando é possível extrair da web e redes sociais, quaisquer tipos de dados, sejam pessoais ou não. O uso de rastreadores para a coleta (e outras atividades de tratamento) de dados pessoais deve levar em conta as normas legais sobre tratamento e de proteção de dados pessoais.

Para as empresas, o *data scraping* pode servir como ferramenta, por exemplo, para direcionar melhor as campanhas publicitárias. A partir de informações em sites, respostas a pesquisas digitais, os interesses ou empregos de muitas pessoas podem ser descobertos, propiciando um marketing mais eficaz.

Além disso, esses mecanismos de *Scraping* permitem a definição de uma persona, um sujeito, os dados pessoais específicos que se deseja, e o seu uso, por exemplo o envio de um e-mail padrão. Há a definição de uma persona e o programa busca esse perfil coletando os dados pessoais como por exemplo nome e e-mail.

A facilidade na realização dessa raspagem de dados preocupa a pesquisadora da ESET Amércia Latina, Cecilia Pastorino, em entrevista:

> Raspagem de dados é uma técnica para extrair informações de sites em massa e por meio de scripts automatizados. Essa técnica é utilizada para indexação de sites ou análise de dados de diferentes páginas e se tornou muito popular em algumas ações de marketing digital, como melhorar o posicionamento na web ou obter métricas. Isso torna muitas das ferramentas de raspagem disponíveis na Internet e muito fáceis de usar (BRANCO, 2021).

O *Web Scraping*, teoricamente, orienta-se pelas normas da LGPD, quando os dados forem coletados em território nacional, quando o site estiver sediado aqui, ou até mesmo quando a coleta tiver entre as suas finalidades o tratamento de dados localizados no Brasil ou a oferta ou o fornecimento de bens ou serviços para pessoas localizadas no território nacional, conforme disposições do Art. 3º da Lei 13.709/2018:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional (BRASIL, 2018).

A prática de *Web Scraping* não caracteriza nenhuma ilegalidade, nas palavras de Oscar Valente Cardoso (2020):

> Apesar de o *web scraping* não ser uma atividade ilícita, deve-se ter atenção especialmente com a coleta genérica e indiscriminada de dados pessoais na internet, o que pode violar o princípio da necessidade (art. 6º, III, da LGPD). Ainda, os dados pessoais de acesso público não dispensam o cumprimento das normas de proteção de dados e, nessa hipótese, a coleta deve considerar a mesma finalidade que levou à divulgação (art. 7º, § 3º, da LGPD).

Portanto, o *Data Scraping* ou *Web Scraping* não é ilegal, mas a forma de obtenção e utilização dos dados pode caracterizar ilegalidade, seja pela venda dos dados coletados, na forma de uma base de dados estruturada, ou pela coleta massiva sem propósito legítimo.

Em suma, a coleta indiscriminada deve restringir-se a não violação do princípio da necessidade, haja vista que, os dados considerados manifestamente públicos são totalmente passíveis dessa prática, devendo considerar somente a finalidade que levou essa divulgação.

De acordo com um artigo publicado pela MFO – Advogados em outubro de 2021, o Facebook e o Linked In, já foram alvo de Data Scraping, este último com a exposição, por uma única pessoa, dos dados de 92% de todos os seus usuários. o que o levou a incorporar ao seu contrato de usuário a proibição do uso desta técnica (ESCOBAR, 2022).

Além dos direitos e liberdades fundamentais dos titulares, também devem ser consideradas suas legítimas expectativas em relação à coleta e tratamento de dados sobre ofertas de produtos/serviços, um teste de equilíbrio entre as intenções e expectativas do controlador em seu benefício. Essa é a maior dificuldade em estabelecer essa proporcionalidade, por todos os motivos citados acima, sem contar o descumprimento dos princípios gerais da LGPD como transparência, necessidade, adequação e segurança (artigo 6º).

Em contrapartida, o Regulamento Geral Europeu de Proteção de Dados (GDPR) estabelece que quando os dados pessoais não foram obtidos diretamente do titular dos dados, o controlador de dados deve fornecer-lhe algumas informações, incluindo: a finalidade do tratamento e a base legal para justificá-lo (Artigo 14).

Assim, dando um passo adiante, não basta apenas dar ao titular a opção de cancelar o mailing, já que a coleta está ocorrendo sem o seu conhecimento.

Além disso, empresas coletarem dados de titulares que tomam decisões sobre novos usos e finalidades no processamento de ofertas de produtos/serviços (fins econômicos),

tornando-os controladores e, portanto, obrigando-os a cumprir e cooperar com a LGPD, consequentemente comprovando o uso justo e lícito dos dados pessoais, frente aos titulares e à Autoridade Nacional de Proteção de Dados.

Conclui Luciano Escobar (2022) que:

> A prática de *data scraping*, no contexto de tratamento aqui discutido, não está em conformidade com a LGPD, sujeitando a Empresa que o pratica às sanções da própria Lei e a possibilidade de o titular de dados pessoais postular alguma reparação indenizatória pela ofensa aos seus direitos.

É necessário que encare essa prática como algo em desacordo com e legislação, embora lícita, sempre arriscará garantias e direitos fundamentais do titular dos dados pessoais.

A melhor forma do usuário resguardar a sua privacidade em meio a essa prática é não deixar os seus perfis nas redes sociais, seja Facebook, Instagram ou Twitter, totalmente públicos, caso deseje, pode liberar o acesso as suas postagens somente a seus amigos próximos nas configurações das próprias plataformas.

Ademais, conforme já ocorre na grande maioria das redes sociais atualmente, as próprias plataformas, em suas políticas de privacidade podem vedar a prática de *Scraping*, assegurando ainda mais a privacidade, e segurança de seus usuários.

3.3 PRINCÍPIOS DO TRATAMENTO DE DADOS

De acordo com Julia Ramos (PRIVACIDADE..., 2022), os princípios mais emblemáticos e basilares do tratamento de dados nas redes sociais são: Finalidade; Adequação; Necessidade e Transparência. Não que os demais princípios instaurados pelo legislador no Art. 6º não tenham sua relevância, de maneira alguma, estes quatro princípios sintetizam muito bem a segurança do usuário perante as relações de serviço e tratamento de dados nas plataformas sociais e garantem seus direitos fundamentais com primazia.

A seguir, transitaremos pelos conceitos dos princípios acima citados e vislumbraremos, ainda, alguns outros que a legislação nos apresenta, dos quais unificados compreendem as mais diversas esferas da Internet, sendo eles: Livre Acesso; Qualidade de Dados; Segurança; Prevenção; Não discriminação e Responsabilização e prestação de constas.

3.3.1 Princípio da Finalidade

Com o advento da LGPD todas as empresas que lidam com dados pessoais precisam mudar seus termos de uso. As principais mudanças advindas da legislação para o tratamento de dados nas empresas baseiam-se nos princípios expressamente definidos e categorizados no Art. 6º da Lei 13.709/2018:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (g.n.) (BRASIL, 2018).

O Princípio da Finalidade demanda um destaque especial, em razão da sua tamanha importância no cenário das redes, uma vez que as empresas precisam explicitar a razão pela qual coletam e tratam os dados, qual o objetivo para isso, qual a necessidade disso, e deixar claro ao usuário que essa coleta ocorrerá estritamente para uma finalidade desejada, assim como percebemos nas recentes políticas de privacidade listadas pela Meta acima.

Doneda (2014) também destaca o princípio da finalidade como um dos pilares norteadores da boa-fé consumerista nas redes sociais, eliminando também a possibilidade de disseminação de dados a terceiros:

> Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade).

Todo e qualquer tratamento deverá ser informado ao titular, isso implica na proibição de algumas práticas costumeiras, tais como a aglutinação de dados para o enriquecimento de uma base robusta de dados para fins de venda, sem conhecimento de seus titulares. Essa prática é condenável e afronta diversos entendimentos da LGPD, sendo passível de inúmeros processos em diversas áreas da justiça.

3.3.2 Princípio da Adequação

O princípio da Adequação (Art. 6º, II – LGPD), estabelece basicamente que os dados pessoais tratados devem ser compatíveis a finalidade informada pelo agente, adequando-se a circunstância do tratamento, portanto, a justificativa e a garantia que os dados coletados tenham relação com o serviço prestado são essenciais.

Do contrário, caso o tratamento de dados não seja compatível com o negócio ou serviço prestado, vindo a ser injustificado, o infrator torna-se passível de multa.

Um simples exemplo dessa incompatibilidade na finalidade do tratamento de dados é a necessidade de um cliente, ao realizar compras on-line em um mercado de sua região, ser instruído pela plataforma digital a inserir informações de caráter religioso e político, Veja que não coexiste nexo na solicitação da informação para a obtenção do resultado final proposto (compra da mercadoria), logo não existe a menor necessidade da disponibilização do dado e, consequentemente, a adequação prevalece.

3.3.3 Princípio da Necessidade

O princípio da Necessidade (Art. 6º, III – LGPD), consubstancia-se na limitação da realização do tratamento ao mínimo necessário para a efetivação de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Tal princípio observa a responsabilidade das empresas no tratamento dos dados na medida que, a responsabilidade é diretamente proporcional a quantidade de dados tratados,

ampliando, assim, os riscos jurídicos em caso de falha no tratamento destes, podendo gerar um desgaste oneroso ao faturamento da empresa.

É conclusivo que somente os dados estritamente necessários deverão ser coletados e tratados para o desenvolvimento empresarial, podendo, os excessos, prejudicar ao invés de ajudar.

3.3.4 Princípio do Livre Acesso

O princípio do Livre Acesso (Art. 6º, IV - LGPD), é um dos pilares da Lei 13.709/2018, em especial tratando-se das mudanças referentes às políticas de privacidade nas redes sociais implementadas quando esta entrou em vigor.

O livre acesso nada mais é que a garantia ao titular do dado, de que a consulta a este será facilitada e gratuita, além de instruí-lo acerca da forma e duração do tratamento realizado, bem como sobre a integralidade de seus dados pessoais. Vale lembrar que esse princípio é assegurado após as pessoas naturais titulares sofrerem o tratamento correspondente.

A legislação ao oferecer esse princípio, exalta a sua indignação com a maneira obscura com que eram tratados os dados e trilha uma nova jornada na luta pela transparência. Conversando diretamente com esse princípio e citando-o, o Art. 9º da LGPD deixa claro ao prestador de serviço responsável pelo tratamento às medidas a serem seguidas:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei (BRASIL, 2018).

Como pudemos notar mais atentamente quando tratamos das políticas de privacidade do Facebook (Meta), inúmeras empresas implementaram mecanismos para que o usuário consiga usufruir do princípio do livre acesso em toda a sua plenitude, evidenciando (muitas vezes de maneira oculta, causando dificuldade para o usuário localizar-se) os seus objetivos e o período de tempo que os dados serão utilizados.

3.3.5 Princípio da Qualidade dos Dados

O princípio da Qualidade dos Dados (Art. 6º, V – LGPD), garante aos seus titulares a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Maldonado e Blum (2019) dispõe sua visão referente aos impactos que as imprecisões nos dados podem ocasionar:

> Qualquer imprecisão, seja um dado pessoal equivocado, seja desatualizado, pode ser catastrófico ao titular, como ocasionar um erro de tratamento médico, recusa de crédito, vedação de participação em concursos públicos, eliminação em processo seletivo, ou, até mesmo, uma prisão injusta. (MALDONADO; BLUM, 2019, p. 149).

Esse princípio é impactante pois, com base nas informações coletadas, uma série de decisões serão tomadas a respeito de seu titular, cabe ao controlador garantir a sua segurança e seu reflexo na sociedade.

3.3.6 Princípio da Transparência

O princípio da Transparência (Art. 6º, VI – LGPD) complementa o princípio ao Livre Acesso, garantindo que os titulares dos dados tenham informações claras, precisas e com o seu acesso facilitado acerca do tratamento e sobre os agentes de tratamento (basicamente outras empresas envolvidas no processo de tratamento dos dados), assegurados os segredos industriais e comerciais.

Em outras palavras, as informações transmitidas pelas empresas deverão ser claras, precisas e, acima de tudo, verdadeiras.

A importância expressa da informação ‘’clara’’ deseja destacar o desejo da legislação em indicar que o uso de terminologias ou conteúdos excessivamente técnicos, ora hermenêuticos, não condizem com a proposta deste princípio, dado que este procura a que as pessoas naturais garantam de imediato, compreender do que trata-se a informação correspondente.

3.3.7 Princípio da Segurança

O princípio da Segurança (Art. 6º, VII – LGPD), como o próprio nome sugere, envolve a adoção, pelos protagonistas do tratamento, de medidas técnicas e administrativas aptas a protegerem os dados pessoais de acessos indevidos, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

O fundamento principal é de preservação de um ambiente seguro ao indivíduo, aprimorando técnicas e minando ao máximo às brechas de segurança, visando mitigar e prevenir eventuais incidentes, tais como, um ataque hacker.

Para fins de caracterização de culpa (*lato sensu*), é irrelevante se a perda, acesso, difusão ou alteração resulte de conduta voluntária do agente (ilícita) ou decorra de conduta acidental, seja ela resultado de negligência, imprudência ou imperícia.

Contudo, na concepção de Oliveira (2019, p. 22), a culpa não é presumida, e sim oriunda de verificação técnica de determinada violação.

3.3.8 Princípio da Prevenção

O princípio da Prevenção (Art. 6º, VIII – LGPD) é compreendido também pelo princípio da Segurança, de qualquer forma, coube a ele um lugar de destaque na legislação, determinando, no processo de tratamento, que sejam adotadas as medidas necessárias para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Destaca-se, portanto, a importância do responsável pelo tratamento, do qual encarrega-se de comunicar o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados.

3.3.9 Princípio da Não Discriminação

O princípio da Não Discriminação (Art. 6º, IX – LGPD) assegura que o tratamento de dados jamais realizar-se-á com objetivos ou propósitos discriminatórios ilícitos ou abusivos contra os seus titulares, geralmente os dados mais suscetíveis a aplicação desse princípio são os sensíveis, pois englobam origem racial ou étnica, convicção religiosa, opinião política e outras intimidades.

É consensual que a impossibilidade da comissão do ato ilícito é, por óbvio, intrínseca ao direito, sendo a sua prática expressamente vedada pelo Código Civil (Lei 10.406/2002), tendo as suas definições e resultantes dispostas nos Arts. 186, 187 e 927:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
>
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.
>
> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem (BRASIL, 2002).

Não resta dúvida quanto ao entendimento do ilícito, contudo, a maleabilidade do substantivo ‘’abusivos’’ não é bem definido e pode trazer algumas margens para elucubrações.

Na interpretação de Pestana (2020) acerca da abrangência de possibilidades trazidas pela palavra ‘’ abusivos’’:

> Aqui o legislador pecou ao não deixar claramente assentado de que abuso se referia, especialmente porque o alojou numa hipótese de finalidade imprópria. E, como se sabe, tal vocábulo (abuso), admite diversas acepções.
> Entendemos, particularmente, que pretendeu se referir ao manuseio excessivo ou imoderado dos dados das pessoas naturais, com isso transbordando, inclusive, o nexo lógico e jurídico estabelecido pelo trinômio dado-tratamentofinalidade, afrontando toda a orientação introduzida pela LGPD.
> Isso porque, se pretendesse assentá-lo na finalidade propriamente dita, teria enfatizado tal valor (vedação à abusividade) ao delimitar o conteúdo do princípio da finalidade, antes já examinado, não o destacando, apartadamente, como o fez, para o princípio da não discriminação (g.n.).

Contudo, a tentativa do legislador em garantir ainda mais a proteção da privacidade e intimidade do usuário, ainda que de forma subjetiva, através desse princípio, é totalmente válida, reforçando os pilares, por exemplo, na consolidação de políticas de privacidade.

3.3.10 Princípio da Responsabilização e Prestação de Contas

Por último, o princípio da Responsabilização e Prestação de Contas (Art. 6º, X – LGPD) dispõe sobre a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Os responsáveis pelo tratamento têm o ônus de responderem pelos seus atos, tanto em suas omissões quanto em suas ações. Na esfera da responsabilização e falta de cumprimento de alguma das medidas acima listadas, propiciando e caracterizando qualquer tipo de dano ao titular do dado, Maldonado e Blum (2019) ilustram o objetivo o legislador em garantir a defesa do indivíduo:

> Prever a responsabilização e a prestação de contas como princípio demonstra a intenção da Lei em alertar os controladores e os operadores de que são eles os responsáveis pelo fiel cumprimento de todas as exigências legais para garantir todos os objetivos, fundamentos e demais princípios nela estabelecidos. E não basta somente pretender cumprir a Lei, é necessário que as medidas adotadas para tal finalidade sejam comprovadamente eficazes. Ou seja, os agentes deverão, durante todo ciclo de vida de tratamento de dados sob sua responsabilidade, analisar a conformidade legal e implementar os procedimentos de proteção dos dados pessoais de acordo com a sua própria ponderação de riscos.

De todo modo, esse princípio alinha-se com a rastreabilidade, uma vez que é exigida a comprovação de procedimentos e atos praticados. O referido rastreio deverá ocorrer com seriedade e respeito em relação ao tratamento dos dados, refletindo em seus usuários.

3.4 CONSIDERAÇÕES ACERCA DOS PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

Os princípios acima listados e conceituados demonstram eloquentemente e inquestionavelmente a importância da aplicação específica do comando incluído a LGPD e, como ocorre em qualquer instrumento legislativo de base principiológica, esses não conduzem ações disciplinares detalhadas para todos os incidentes, ações e circunstâncias, componentes da realidade fática. Logo, é fundamental para aqueles que pretendam transitar pelo ambiente das redes, ou até mesmo tenham interesse em tratar dados, que conheçam e dominem esses princípios.

Cumpre um apontamento ao caráter regulador que os princípios do Art. 6ª imprimem na esfera das redes sociais, embora a Lei Geral de Proteção de Dados não as tratem em seus artigos com exclusividade, dedicando disposições específicas para elas, o reflexo em suas políticas de privacidade são completamente visíveis, adequando-se às padronizações exigidas por lei, visando atender cada aspecto de cada um dos princípios listados, demonstrando um estrondoso avanço na proteção e tratamento de dados das pessoais naturais e minando a banalização com a finalidade destes.

4 RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS

Conforme refletimos acima, a importância fundamental da gestão e preservação dos princípios garantidos pela LGPD são o escopo de toda a sua estruturação, buscando, em caráter preventivo, garantir sempre o benefício do detentor dos dados e que o seu tratamento ocorra da melhor maneira possível.

Tratando de um cenário de redes sociais, onde os dados são a principal matéria prima, tanto para os usuários, quanto para os prestadores de serviço (controladores ou operadores), a proteção e gerenciamento desses dados é fundamentalmente prioritária, sendo intrínseca à regularidade daquela plataforma.

O direcionamento equivocado no tratamento de dados em redes sociais pode causar consequências irreversíveis aos usuários, desde uma violação à intimidade, em sentido amplo, até o desvio de senhas bancárias, o ambiente virtual propicia uma gama de possibilidades, dentre elas, não são em todas que o usuário sairá beneficiado, com certeza.

Além disso, um dos malefícios e benefícios que a internet nos trouxe foi a "eternalização" da informação, uma vez que um dado ou notícia relevantes alcançam os meios digitais, redes sociais, plataformas de notícias, é quase impossível que ele passe despercebido, antes que consiga ser excluído em anonimato sem que haja replicação.

Isso é positivo por um lado pois permite que diversos escândalos sejam expostos sem que passem pelo crivo tendencioso de grandes mídias, que, por motivos ou interesses maiores, talvez deixassem de noticiar o acontecido caso o descobrissem com exclusividade. Essa prática propiciou o surgimento de diversas mídias independentes ao redor do mundo, gerando um grande debate a respeito da democratização da informação, o próprio WikiLeaks, citado anteriormente quando tratamos do caso Snowden, talvez seja o exemplo mais conhecido.

Agora, infelizmente, os malefícios falam mais alto, tomando somente como exemplo, a Carolina Dieckman, teve a sua carreira e vida pessoal extremamente abalada pelo vazamento de uma foto íntima, da qual percorreu por milhares de celulares no Brasil, sem qualquer tipo de rastreio, gerando uma movimentação expressiva no legislativo brasileiro, do qual entendeu por alterar o código penal para delitos informáticos.

Observamos então que o tratamento indevido dos dados pessoais, sejam quais forem, podem gerar consequências das mais variadas possíveis, dependendo somente da imaginação do seu malfeitor.

Para isso, o legislador criou algumas ferramentas inibitórias, visando a minimização de qualquer lesão na coleta e tratamento de dados/informações, propondo um sistema coercitivo capaz de propiciar a reparação integral do dano distribuído (FRAZÃO, 2019, p. 35).

Antes de mais nada, precisamos ter em mente que no âmbito das relações consumeristas, a regra para a responsabilização dos agentes infratores é a responsabilidade objetiva, a qual estabelece que, independentemente da existência de culpa, o autor da conduta responde pela reparação do dano. Para isso, porém, é preciso atestar o nexo de causalidade, o vínculo lógico entre a ação e o dano sofrido.

Em contrapartida, o Código Civil nos apresenta uma responsabilidade subjetiva, considerando também a demonstração do dano e nexo de causalidade, contudo, leva em consideração além desses fatores o dolo e a violação de um dever pela culpa lato sensu (negligência, imprudência ou imperícia).

Desde a sua produção até a sua eliminação, passando pelos mais diversos tipos de processos e operações: coleta, modificação, reprodução, transferência internacional e arquivamento. Na resultante final, os dados pessoais embarcam na LGPD sob o amplo conceito de ‘’tratamento’’, sendo denominados agentes de tratamento, àqueles que exercem as operações com esses dados.

Tais agentes podem ser divididos em duas classificações, a primeira é a do controlador, sendo ele uma pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões referentes ao tratamento de dados. Determinando ele a sua atuação, regras de acordo com seu modelo de negócios e seu legítimo interesse, em conformidade com a lei.

Em contrapartida, o operador é uma pessoa natural ou jurídica, de direito público ou privado, realizando o tratamento de dados pessoais em nome do controlador. A sua função é processar e gerenciar as informações de acordo com as regras estabelecidas pelo controlador.

A Lei Geral de Proteção de Dados é categórica em assegurar um espaço em seu ordenamento ao tema ‘’ Da Responsabilidade e do Ressarcimento de Danos’’, relacionado aos agentes de tratamento de dados, por óbvio, especificamente em seus artigos 42 a 45:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver

> seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.
> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.
> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.
> Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente (BRASIL, 2018).

O Art. 42, em sua inteligência, resguarda a reparação civil nos âmbitos, moral, patrimonial, coletivo ou individual, imposto aos controladores e operadores, em ocasião das operações de tratamento de dados em que haja violação expressa à LGPD. Em suma, uma cláusula generalista de reparação, a obrigação de reparar sobrecai ao controlador ou operador, causador do dano patrimonial ou extrapatrimonial dos dados atingidos.

Em consonância com o Código de Defesa do Consumidor CDC (Lei 8.078/90), a LGPD estabeleceu uma responsabilidade solidária dos agentes de tratamento que vierem a cometer qualquer tipo de dano (art. 42, § 1º, I e II), possibilitando, também inspirada no CDC, a inversão do ônus probatório por critério judicial (art. 42, § 2º), mitigando a desproporcionalidade nas relações entre os controladores, operadores e titulares.

Tece Vieira (2018, p. 29), algumas considerações sobre o artigo 42:

> A LGPD traz, ainda, previsão expressa de responsabilidade solidária dos operadores e controladores. Nesse sentido, conforme disposição do inciso I do §1º do art. 42. o operador responde solidariamente pelos danos causados pelo tratamento quando

> descumprir as obrigações da LGPD ou quando não tiver seguido as instruções lícitas do controlador. Já os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados, conforme inciso II do §1º do art. 42 da LGPD, respondem solidariamente. O direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso, é assegurado àquele que reparar o dano ao titular dos dados consoante §4º do art. 42 da LGPD. Nos termos do art. 44 da LGPD, será considerado irregular o tratamento de dados pessoais quando for inobservada a legislação ou quando não for fornecida ao titular a segurança que ele poderia esperar, levando-se em conta as seguintes circunstâncias: o modo pelo qual o tratamento é realizado; o resultado e os riscos que razoavelmente dele se esperam; as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Por sua vez, o artigo 43, elenca hipóteses de exclusão da responsabilidade civil dos agentes de tratamento, comprovando eles os seguintes requisitos i) não realizaram o tratamento dos dados pessoais, ii) se o realizaram, não violaram as normas de proteção de dados pessoais ou iii) que o dano foi causado por terceiro ou pelo próprio titular (art. 43, I a III).

Ademais, embora o art. 43, II, da referida norma preveja que os agentes de tratamento não serão responsabilizados caso não tenham violado a legislação de proteção de dados, por outro lado, a violação do princípio da segurança (art. 6º, VII, da LGPD), por si só, já enseja a responsabilização, desde que haja o nexo causal do dano:

> Em relação aos danos causados em relação ao tratamento indevido de dados pessoais, é necessário que se compreenda a existência de um dever de segurança imputável aos agentes de tratamento (controladores e operadores de dados), que é segurança legitimamente esperada daqueles que exercem a atividade em caráter profissional, e por esta razão presume-se que tenham a expertise suficiente para assegurar a integridade dos dados e a preservação da privacidade de seus titulares. Daí porque a responsabilidade dos agentes de tratamento decorre do tratamento indevido ou irregular dos dados pessoais do qual resulte o dano. Exige-se a falha do controlador ou do operador, que caracteriza o nexo causal do dano. Contudo, não se deve perquirir se a falha se dá por dolo ou culpa, senão que apenas sua constatação é suficiente para atribuição da responsabilidade, inclusive com a possibilidade de inversão do ônus da prova em favor do titular dos dados, nas mesmas hipóteses de hipossuficiência e verossimilhança que a autorizam no âmbito das relações de consumo (art. 42, § 2º, da LGPD) (MIRAGEM, 2019, p. 26).

Essa inversão tão extremada do ônus probatório é justificada pela decadência recursal do titular dos dados. Observam Teixeira e Armelin (2020) que essa hipossuficiência faz-se "facilmente constatável quando se tem uma sociedade permeada pela cultura do Big Data, em que há uma coleta massiva de dados, muitas vezes até desnecessária". Concluindo ainda sobre o desbalanceamento entre controladores e titulares, "o titular de dados se encontra em uma posição claramente desfavorável, em que beira [a]o impossível saber quais de seus dados estão sendo tratados, de que forma isso tem sido feito e quem seriam os agentes de tratamento".

A redação do Art. 44, por sua vez, define o conceito do tratamento irregular de dados, mais uma vez à luz do CDC, estabeleceu que a irregularidade se dará quando contrariar a disciplina legal (art. 44, caput) ou, também, quando não fornecer a segurança legitimamente esperada pelo respectivo titular (art. 44, I a III). Ainda, o § único desse dispositivo estabelece o dever de indenizar derivado da violação de normas técnicas provenientes da Autoridade Nacional de Proteção de Dados (ANPD), diferenciando-se dos outros dispositivos, que tratam a responsabilidade como a violação de normas jurídicas do microssistema de dados pessoais.

A doutrina, no ano de vigor da LGPD, entendia pela responsabilidade objetiva em decorrência dos danos causados pelo tratamento irregular de dados:

> Conclui-se, portanto, que apesar do uso de expressões diversas em sua redação, tanto o artigo 42, quanto o artigo 44, da LGPD, adotam o fundamento da responsabilidade civil objetiva, impondo aos agentes de tratamento a obrigação de indenizar os danos causados aos titulares de dados, afastando destes o dever de comprovar a existência de conduta culposa por parte do controlador ou operador. Fundamenta esta conclusão o fato de que a atividade desenvolvida pelo agente de tratamento é evidentemente uma atividade que impõe riscos aos direitos dos titulares de dados, que, por sua vez, são intrínsecos, inerentes à própria atividade e resultam em danos a direito fundamental. Ademais, tais danos se caracterizam por serem quantitativamente elevados e qualitativamente graves, ao atingirem direitos difusos, o que, por si só, já justificaria a adoção da responsabilidade civil objetiva, tal como no caso dos danos ambientais e dos danos causados por acidentes de consumo (MULHOLLAND, 2020).

A visão acima sobre a responsabilização objetiva está interligada a Teoria do Risco, prevista no Código de Defesa do Consumidor e no Código Civil, especificamente no Art. 927 (já mencionado anteriormente quando tratamos do princípio da não discriminação), nela, o grau de perigo da atividade justifica a responsabilização independente da culpa:

> A teoria do risco aparece na história do Direito, portanto, com base no exercício de uma atividade, dentro da ideia de que quem exerce determinada atividade e tira proveito direto ou indireto dela responde pelos danos que ela causar, independentemente de culpa sua ou de prepostos. O princípio da responsabilidade sem culpa ancora-se em um princípio de equidade: quem aufere os cômodos de uma situação deve também suportar os incômodos (VENOSA, 2017, p. 399).

A LGPD muitas vezes é interpretada na perspectiva de ser alicerçada no risco. Em, outras palavras, podemos dizer que devemos esperar mais daqueles agentes de tratamento de dados pessoais cujas atividades têm um risco maior. A legislação é muitas vezes é contundente com aqueles que, via de regra, tendem a tratar dos dados pessoais sensíveis em uma escala considerável. De tal forma que, os princípios da prestação de contas e da responsabilidade não podem faltar no vocabulário dos controladores de dados, além disso, as medidas preventivas,

de segurança e proteção têm de ser substanciais, reduzir o material a uma papelada empobrece os mecanismos citados.

Entendia-se que a responsabilidade dos agentes de tratamento era objetiva, uma vez que a atividade do tratamento implicaria diretamente nos riscos aos direitos dos titulares, de tal forma, que as hipóteses de exclusão de responsabilidade objetiva do artigo 43 da LGPD, subsidiariamente, espelhavam-se às excludentes do artigo 14 do Código de Defesa Do Consumidor, possibilitando, ambas, a inversão do ônus probatório (MIRAGEM, 2019, p. 27):

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.
> § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:
> I - o modo de seu fornecimento;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - a época em que foi fornecido.
> § 2º O serviço não é considerado defeituoso pela adoção de novas técnicas.
> § 3° O fornecedor de serviços só não será responsabilizado quando provar:
> I - que, tendo prestado o serviço, o defeito inexiste;
> II - a culpa exclusiva do consumidor ou de terceiro.
> § 4° A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa (BRASIL, 1990).

Finalizando a Seção II da responsabilidade, o artigo 45 ressalta que em caso de lesão ao direito do consumidor, ou pessoa a ele equiparada, continuam sujeitas à disciplina do microssistema de relações de consumo instituído pelo CDC (Lei 8.078/90). Em outras palavras, sob a tutela do artigo 14 do CDC, da qual a responsabilidade civil será objetiva, conforme ilustra o entendimento de Moraes e Queiroz (2019, p. 131):

> Uma leitura desavisada do dispositivo e contrária à unidade do ordenamento poderia levar à conclusão incorreta de que a LGPD não se aplica às relações de consumo, sendo acertado concluir que o art. 45 quer, em verdade, apontar para que o regime de responsabilidade civil do controlador ou operador de dados pessoais no âmbito das relações de consumo será objetivo quando violada qualquer disposição da própria LGPD ou de quaisquer garantias de proteção de dados pessoais nas relações de consumo contidas nos arts. 43 a 44 do CDC. Em outras palavras, estando o intérprete diante da violação dos princípios e garantias do titular de dados pessoais no âmbito de relações de consumo, aplicar-seá o regime de responsabilidade civil objetiva contida no art. 14 do CDC, com fulcro no art. 45 da LGPD e, no que diz respeito ao rol de garantias e direitos do titular de dados pessoais e dos deveres dos tratadores e coletores de dados pessoais, aplica-se a LGPD em sua inteireza.

Embora existam tantos indicativos direcionando a responsabilidade objetiva como uma verdade absoluta, quando o assunto é responsabilização na LGPD, a volatilidade desse tema nunca foi tão contundente.

De acordo com a matéria publicada no portal Jota (GUIMARÃES, 2022) em junho de 2022, Antonio Freitas, conselheiro da Associação dos Advogados de São Paulo (AASP) é adepto da teoria da responsabilidade subjetiva na LGPD, para ele a aplicação da responsabilidade objetiva é contraditória, sendo que há uma série de dispositivos na LGPD regulando boas práticas e medidas de adequação, tais como os princípios do artigo 6º, entre outros.

Segundo a lógica de Antonio se a responsabilização independe da existência de culpa, não há sentido para cumpri-la. Ressalta ainda que o art. 45 da lei, conforme vimos, já deixa claro que, tratando-se de relações de consumo, as hipóteses permanecem sujeitas à incidência do Código de Defesa do Consumidor, o qual norteia-se pela responsabilização objetiva em seu artigo 14, logo, o restante da Lei Geral de Proteção de Dados deveria seguir a lógica subjetiva.

Diante dessa discussão entre responsabilidade objetiva e subjetiva, surge uma questão fundamental, uma vez que o Art. 42 é superficial ao especificar a configuração do dano, dos quais os controladores e operadores devem reparar, quais seriam as situações que ensejariam o dever de reparação do dano?

Partindo do pressuposto da conduta, nexo de causalidade e de que o dano é um pré-requisito para a reparação civil e sem ele não há efetivamente nada a ser reparado, Paulo Renná (2022) faz algumas considerações acerca das características que constituem o dano no ambiente de tratamento de dados:

> Entendo que qualquer vazamento de dados pessoais gere o direito à indenização por dano moral. Da mesma forma, qualquer falha nos deveres de transparência ativa e comunicação de incidentes. Essa conclusão, no entanto, depende da compreensão de que o dano corresponde a qualquer violação de direito, e não depende de um prejuízo financeiro.

Dessa forma Paulo Renná (2022), entende que a LGPD segue essa perspectiva, ao afirmar a obrigação do controlador e do operador em reparar tanto o dano patrimonial quanto o moral. Contudo, é evidente para ele que ela não apresenta uma configuração específica de dano moral em termos de dados pessoais, abrindo algumas margens para discussões sobre o tema.

O portal Jota ainda expõe o surgimento de uma terceira via de responsabilização, proposta por Maria Celina Moraes e João Quinelato de Queiroz, desvencilhando o regime de

responsabilidade da LGPD da aplicação de uma teoria clássica, surgindo assim uma ‘’responsabilidade ativa’’, nele os agentes devem comprovar a sua conformidade com o cumprimento normativo e que suas medidas são eficazes, não sendo mais suficiente apenas o cumprimento dos artigos da lei.

Indo mais além, a matéria aponta o posicionamento da professora de Direito Civil do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), Laura Schertel Mendes, da qual apresenta um posicionamento a aplicabilidade de mais de um tipo de responsabilidade, contudo, a sua aplicabilidade na legislação seria independente de debates doutrinários entre subjetivistas e objetivistas. Uma vez que não caberia à vítima comprovar a ilicitude do tratamento de dados, com base no texto dos artigos 42 e 43, antes, competiria aos agentes a comprovação da inocorrência da atividade ou de sua licitude.

Em entrevista concedida ao portal, Laura ressalta seu posicionamento:

> A responsabilidade civil na LGPD pressupõe o reconhecimento do risco no tratamento de dados pessoais. Dessa forma, pouco importa na prática se qualificarmos a responsabilidade da LGPD como objetiva ou como subjetiva com culpa presumida," explica Mendes.
> "Fato é que o dever de indenizar surge quando houver o dano, a violação à norma e o nexo causal, podendo os agentes de tratamento provarem que não houve violação à norma, que a atividade não se realizou ou que o dano decorre de culpa exclusiva de titular ou de terceiro" (GUIMARÃES, 2022).

Dessa forma, o posicionamento apresentado por ela demonstra uma visão menos protecionista ao indivíduo detentor dos dados violados, mas, em contrapartida, possibilita ao controlador ou operador dos dados a oportunidade de contestar e apresentar defesa às alegações de dano, seja pela comprovação da ausência de dano, que a atividade não ocorreu, ou que decorreu por culpa exclusiva da vítima ou de terceiro, fator esse que rompe com o nexo de causalidade e, consequentemente, com o dever de indenizar.

Bruno Bioni, figura notória na proteção de dados, já citado anteriormente, compartilha de um pensamento similar ao da Dra. Laura, em um artigo publicado juntamente com Daniel Dias na revista eletrônica de direito "civilistica.com", denominado "Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor " (BIONI; DIAS, 2020).

Nesse artigo eles concluem que, basicamente, a nossa visão de responsabilização civil atual é binária e limitada no regime jurídico da LGPD, carecendo de avanços quanto à discussão de “objetivo” ou “subjetivo”. Já que, não há espaço para dúvidas que a política legislativa

adotada exige a investigação em torno de um juízo de culpa dos agentes de tratamento de dados, mas, simultaneamente, prescreve diversos elementos com potencial instabilidade dos filtros para que os agentes de tratamento de dados sejam responsabilizados.

Em uma conclusão final, Bioni e Dias entendem por uma resultante peculiar, no sentido de uma legislação de regime jurídico de responsabilidade civil subjetiva, com um alto grau de objetividade.

Por fim, em meio a tantos impasses e contreversas, existe alguma saída ou perspectiva de mudança? Uma das percepções de Paulo Rená (2022) é que muitas das discussões mais contemporâneas sobre responsabilidade civil, são reflexos de uma série de controvérsias oriundas da própria disciplina jurídica da responsabilidade civil, para ele, tanto o Marco Civil da Internet quanto a LGPD carecem de um amadurecimento no regime jurídico de responsabilidade civil.

A solução para Rená (2022), logo, vem mediante o auxílio do Poder Judiciário, especialmente ao desempenhar o seu papel institucional, de afirmar a garantia constitucional de proteção de dados pessoais, assegurando o seu cumprimento, seja de imediato aplicando-os a casos concretos ou até mesmo em exame de teses em abstrato. Nesse sentido, para ele, toda e qualquer violação de direitos previstos na LGPD impõe um dever de compensação ao titular dos dados pessoais afetados, ainda que a indenização tenha um valor reduzido ou limite-se a uma obrigação de fazer e, segundo, a prevalência do regime objetivo de responsabilização dos agentes de tratamento, deixando bem claro o seu posicionamento.

Compartilho do pensamento de Paulo, acima de tudo pela garantia à proteção de dados, à inviolabilidade dos direitos previstos da LGPD, e pelo dever de indenizar referente a ocorrência do dano, todos esses fatores somam aos pensamentos dos autores supracitados que zelam pela aplicabilidade de um regime de responsabilidade objetiva na Lei Geral de Proteção de Dados. Resta unânime somente um fator nessa discussão, enquanto não houver um posicionamento do judiciário, o debate manter-se-á acirrado.

5 SANÇÕES ADMINISTRATIVAS

Antes de tratarmos das sanções administrativas precisamos primeiramente compreender qual é o papel da Autoridade Nacional de Proteção de Dados (ANPD) nesse processo.

O principal objetivo desse órgão é garantir, com excelência, às medidas da LGPD no Brasil e, deste modo, garantir a devida proteção aos direitos fundamentais de liberdade, privacidade, livre desenvolvimento da personalidade dos indivíduos, dentre outros princípios vigentes na legislação.

Quanto às suas competências, o Art. 55-J da lei 13.709/2018 elenca mais de 24 incisos, dentre elas destacam-se: i) Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; ii) Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; iii) Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; iv) Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; v) Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; vi) Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD; vii) Ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; viii) Editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se à Lei; ix) Deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da LGPD, as suas competências e os casos omissos; x) Articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e xi) Implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a LGPD.

Compreendendo melhor os encargos desse órgão, podemos retornar às sanções administrativas. O art. 52 da LGPD nos diz que os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas, ficam sujeitos às seguintes sanções administrativas aplicáveis pela Autoridade Nacional de Proteção de Dados (ANPD):

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;''
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)
> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano;
> VII - a cooperação do infrator;
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção (BRASIL, 2018).

A Resolução CD/ANPD nº 1, de 28 de outubro de 2021, foi aprovada nesta data pela Autoridade Nacional de Proteção de Dados estabelecendo, mediante o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, os procedimentos de fiscalização e as regras a serem observadas no âmbito do processo administrativo sancionador pela ANPD.

A Lei 13.709/2018 determina, ainda, que a Autoridade Nacional de Proteção de Dados edite o seu próprio regulamento sobre sanções administrativas, sendo objeto de consulta pública, contendo as metodologias que orientarão o cálculo do valor-base das sanções de multa. Esses métodos devem ser divulgados antecipadamente, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, dos quais conterão fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos na legislação.

De acordo com as disposições da lei, a aplicação de sanções também exige uma avaliação cuidadosa e consideração de uma variedade de circunstâncias, incluindo a gravidade e a natureza da infração e os direitos pessoais afetados, a situação econômica do infrator, a extensão do dano, o infrator cooperante, adoção de políticas de governança, conforme ilustrado no tópico 4.1 e a adoção de medidas corretivas.

À primeira vista os critérios e parâmetros trazidos pelo parágrafo 1º do art. 52 são, em sua maioria, objetivos e taxativos, não existindo margem para grandes contestações. A subjetividade é determinada nesse caso pela aplicabilidade de cada critério ao caso concreto.

Na visão de Aline Pelet, a adequação das empresas à LGPD ainda é tímida no mercado, carecendo de uma atuação mais robusta da agência reguladora:

> A edição do relatório que estabelece a dosimetria com certeza irá contribuir para uma maior efetividade e cumprimento das normas pelas empresas e profissionais liberais. Mas os efeitos apenas poderão ser sentidos após a realização da consulta pública, pois apesar de ter sido estabelecida uma série de critérios para aplicação de sanções, ainda é importante que a norma estabeleça prazos razoáveis para cumprimento e aplicação de cada questão levantada (REDAÇÃO, 2022).

As consequências decorrentes do descumprimento da lei são graves, mas, num primeiro momento, o que não pode cair em normalidade, é o recebimento por parte das empresas de recomendações e advertências com caráter educativo e orientativo, e não coercitivo, banalizar a má gestão de dados é ser conivente com práticas que afrontam o alicerce da LGPD.

Por hora, mesmo sem a base de cálculo de multas formulada, as companhias, especialmente as redes sociais, precisam atentar-se como nunca aos possíveis prejuízos financeiros que estão passíveis de sofrer, decorrendo da suspensão do direito de tratar dados pessoais. Podendo significar a impossibilidade de uma empresa acessar e usufruir de seu banco de dados, no qual tenha armazenado diversas informações relacionadas a seus cliente e parceiros.

As redes sociais, por fornecerem um serviço gratuito, em sua maioria, tem como principal fonte de renda a utilização de dados dos usuários para direcionamento de vendas com empresas parceiras, caso o direito de tratar esses dados fosse minimizado, apenas em percentuais, o dano financeiro seria catastrófico, tratando de parcerias comerciais ou até mesmo no ramo do mercado financeiro, caso essa empresa tenha capital aberto na bolsa de valores.

A lei prevê que a Agência Nacional de Proteção de Dados (ANPD) crie um regulamento próprio sobre as sanções administrativas, que inclua as metodologias que devem orientar o cálculo do valor-base das sanções e multas. Por ora, no entanto, a ANPD ainda não estabeleceu essa metodologia.

CONSIDERAÇÕES FINAIS

Vivemos em uma sociedade centrada na informação, fruto de diversas novas formas de organização socioeconômica. O fluxo de dados não apenas altera o relacionamento social, mas redefine o conceito espacial e comercial. A ordem econômica vigente usa informações, ou seja, dados sobre a experiência humana, os recursos humanos, como matéria-prima para fins comerciais, subdividem as atividades e segmentam os consumidores, criam produtos cada vez mais personalizados e, finalmente, tendenciam a escolha do usuário. Essa lógica de acumulação funciona, e se retroalimenta, para que isso ocorra cada vez mais dados são coletados.

A cultura orientada a dados é calcada fortemente na tecnologia e em ferramentas digitais inteligentes, ganhando ainda mais amplificação com o advento das redes sociais, ambiente esse em que os dados dos usuários são o bem mais valioso, objeto de proteção, segurança, cuidado, cautela e acima de tudo, de desejo, desejo esse responsável por todo o esmero do operador no tratamento dos dados.

A LGPD (Lei nº 13.709/2018) surge em 2018 com a proposta de regular a coleta, o armazenamento e o tratamento de dados pessoais, com o objetivo de garantir os direitos de liberdade e privacidade das pessoas, além de fornecer mais controle e autonomia aos usuários sobre seus próprios dados. O processo de consolidação da LGPD no ordenamento jurídico brasileiro, como vimos, passou por medidas progressivas legislativas e diversos acontecimentos históricos que propiciaram uma mobilização do Legislativo, tais como o vazamento de dados da *Cambridge Analytica*, coletando dados de milhões de usuários do Facebook para fins políticos e no caso Snowden, relacionado diretamente com uma violação da segurança interna brasileira, mediante espionagem de dados da ex-presidente Dilma Rousseff.

Diante desse cenário, a esmagadora maioria dos requisitos de adequação que foram incorporados pelas plataformas através da imposição da LGPD e também pelas empresas em estratégias de vendas dizem respeito aos princípios da própria legislação (Art. 6º), listados categoricamente nessa monografia, buscando ser um espelho das orientações e medidas neles embutidas, por falta de dispositivos objetivos.

A aplicabilidade maior desses princípios para o contexto das redes sociais pode se dar pela: i) obtenção de um consentimento expresso do titular dos dados,; ii) através da transparência , seja pela comunicação com o usuário , ou na informação sobre como e quais dados serão coletados; iii) a imprescindível demonstração da finalidade, específica e legítima de uso desses dados, devendo o agente deixar claro para qual destinação corresponde o

tratamento e a coleta daquele determinado dado, não podendo ele ser utilizado para fins que não sejam a sua destinação de origem; iv) informações sobre o compartilhamento de dados com outras empresas e; v) garantir a orientação dos usuários quanto as medidas adotadas para o tratamento de dados, além de reforçar medidas de segurança e prevenção.

Tais elementos podem ser instituídos, não somente nas redes sociais, mas em qualquer empresa que trate de dados pessoais, através de políticas de privacidade, adequação estrutural e governança.

A utilização dos dados pessoais de seus usuários, por parte das redes sociais está diretamente relacionada ao direcionamento e segmentação de anúncios, ocasionando, portanto, um impacto mais significativo da nova legislação em razão do risco de gerenciamento. Em suma, o princípio da transparência impossibilita com que a obscuridade e omissão das políticas de privacidade se façam presentes, além disso a LGPD garante a proteção aos dados pessoais sensíveis na medida que o seu compartilhamento é regulamentado, o ordenamento abrange até mesmo os menores de idade em ambiente digital.

Dentre outras diversas percepções e apontamentos acerca da LGPD, podemos concluir que essa legislação tem trazido grandes frutos ao ambiente digital, em especial às redes sociais, das quais tornaram-se e tornam-se a cada dia mais seguras a seus usuários, respeitando a soberania da intimidade e privacidade.

Conforme já expressei-me anteriormente, o caráter coercitivo da punibilidade de grandes empresas, acima de tudo, no que diz respeito aos impactos comerciais, gera um senso de responsabilização coletivo e uma conduta de obediência, possibilitar a impunidade, nesses casos, é possibilitar uma prática abusiva que coloca milhões de usuários em risco. A manutenção da LGPD exige um pulso firme do Judiciário, perpetuando os princípios emanados pela legislação.

REFERÊNCIAS

BIONI, Bruno Ricardo. **Regulação de dados é uma janela de oportunidade**. Data Privacy. 2019. Disponível em: https://dataprivacy.com.br/regulacao-de-dados-e-uma-janela-deoportunidade/. Acesso em: 8 nov. 2022.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica**, v. 9, n. 3, 2020. Disponível em: https://images.jota.info/wp-content/uploads/2022/05/662-texto-integral-1387-1-10-20201222.pdf. Acesso em: 8 nov. 2022.

BIONI, Ricardo B. **De 2010 a 2018**: a discussão brasileira sobre uma lei geral de proteção de dados. 2018. Disponível em: https://brunobioni.com.br/blog/2018/07/02/de-2010-a-2018-a-discussao-brasileirasobre-uma-lei-geral-de-protecao-de-dados/. Acesso em: 8 nov. 2022.

BIONI, Ricardo B. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2018. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530983291/. Acesso em: 2 nov. 2022.

BRANCO, Dácio Castelo. **O que é web scraping e como ocorre?**. Canal Tech. 2021. Disponível em: https://canaltech.com.br/seguranca/o-que-e-web-scraping/. Acesso em: 6 nov. 2022.

BRASIL. Congresso Nacional. Lei n. 12.965, de 22 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, 24 de abril de 2014, ano 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 8 nov. 2022.

BRASIL. Congresso Nacional. Lei n. 13.709, de 13 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, 15 de agosto de 2018, ano 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 6 nov. 2022.

BRASIL. Congresso Nacional. Lei n. 8.078, de 10 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências.. **Diário Oficial da União**, Brasília, 12 de setembro de 1990, ano 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 6 mar. 2022.

BRASIL. Congresso Nacional. Lei n. 9.507, de 11 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. **Diário Oficial da União**, Brasília, 13 de novembro de 1997, ano 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9507.htm#:~:text=LEI%20N%C2%BA%209.507%2C%20DE%2012%20DE%20NOVEMBRO%20DE%201997.&text=Regula%20o%20direito%20de%20acesso,rito%20processual%20do%20habeas%20data. Acesso em: 6 nov. 2022.

BRASIL. Constituição Federal, de 04 de outubro de 1988. **Diário Oficial da União**, Brasília, 05 de outubro de 1988, ano 1988. Disponível em: https://bit.ly/3f9s7JG. Acesso em: 26 out. 2022.

BRASIL. Lei n. 10.406, de 09 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília, 11 de janeiro de 2002, ano 2002. Disponível em: https://bit.ly/33zFpJY. Acesso em: 4 mar. 2021.

CARDOSO, Oscar Valente. **O Web Scraping Viola a Proteção de Dados Pessoais?**. Jusbrasil. 2020. Disponível em: https://ovcardoso.jusbrasil.com.br/artigos/1152362639/o-web-scraping-viola-a-protecao-de-dados-pessoais. Acesso em: 3 nov. 2022.

CETAX. **Big Data**: o que é, conceito e definição. Cetax. 2022. Disponível em: https://cetax.com.br/big-data/. Acesso em: 6 nov. 2022.

COLLMER, Alex. **Como Implementar a Governança de uma Marca nas Redes Sociais na Era da LGPD**. E-commerce Brasil. 2021. Disponível em: https://www.ecommercebrasil.com.br/artigos/como-implementar-a-governanca-de-uma-marca-nas-redes-sociais-na-era-da-lgpd. Acesso em: 2 nov. 2022.

CRUZ, Bruno Sousa. **Facebook traça perfil até de quem não usa a rede social**. TILT. 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/04/12/zuckerberg-confirma-que-facebook-traca-perfil-de-quem-nao-usa-a-rede-social.htm. Acesso em: 2 nov. 2022.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. *In:* MARTINS, Guilherme Magalhães (Coord.). **Direito Privado e Internet**. São Paulo: Atlas, 2014.

ESCOBAR, Luciano. **A LGPD e o Data Scraping A Coleta de Dados Massiva na Web e Redes Sociais**. MFO Advogados. Porto Alegre, 2022. Disponível em: https://mfoadvogados.com.br/a-lgpd-e-o-data-scraping-a-coleta-de-dados-massiva-na-web-e-redes-sociais/. Acesso em: 1 nov. 2022.

FORTES, V.B. **Os direitos de privacidade e a proteção de dados pessoais na internet**. Rio de Janeiro: Lumens Juris, 2016.

FRAZÃO, Ana. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D.. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thompson Reuters Brasil, 2019, p. 23-52.

G1. **Entenda o caso de Edward Snowden, que revelou espionagem dos EUA**: Procurado pelos Estados Unidos, ex-técnico da CIA obteve asilo da Rússia. Caso gerou crise para o governo Obama e debate sobre privacidade online. G1. 2013. Disponível em: https://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em: 3 nov. 2022.

GOGANI, Ronaldo. **O maior roubo de dados da história do Facebook que ajudou a eleger Donald Trump**: Investigação revela o grande esquema que envolveu o maior roubo de dados da história do Facebook, que pode ter ajudado Donal Trump a ser eleito presidente dos Estados Unidos e aprovado o Brexit no Reino Unido. Meio Bit. 2018. Disponível em: https://meiobit.com/381701/facebook-cambridge-analytica-roubo-dados-ajudou-campanha-donald-trump-e-brexit/. Acesso em: 8 nov. 2022.

GUIMARÃES, Arthur. **Jota DIscute**: Lei Geral de Proteção de Dados Pessoais. JOTA. 2022. Disponível em: https://www.jota.info/coberturas-especiais/protecao-de-dados/responsabilidade-civil-na-lgpd-e-bola-dividida-e-nao-ha-consenso-entre-especialistas-24062022. Acesso em: 3 nov. 2022.

INTERSOFT CONSULTING. **GDPR**. 2016. Disponível em: https://gdpr-info.eu/. Acesso em: 8 nov. 2022.

KOKOLAKIS, S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. **Computers & Security**, p. 122-134, 2017.

KRIEGER, Maria Victoria Antunes. **A análise do instituto do consentimento frente à lei geral de proteção de dados do Brasil**: lei nº 13.709/18. Florianópolis, f. 83, 2019 Trabalho de Conclusão de Curso (Curso de DIreito) - Universidade Federal de Santa Catarina. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/203290/TCC.pdf?sequence=1&isAllowed=y. Acesso em: 6 nov. 2022.

LEMOS, Ronaldo; PACETE, Luiz Gustavo. **A GDPR terá um efeito viral**. Meio e Mensagem. 2018. Disponível em: https://www.meioemensagem.com.br/home/midia/2018/05/21/a-gdpr-tera-um-efeito-viral.html. Acesso em: 8 nov. 2022.

LOEWENSTEIN, George. Privacy and human behavior in the age of information. **Science**, v. 347, n. 6221, p. 509-514, 2015.

MACIEL, Rafael Fernandez. **Manual prático sobre a lei geral de proteção de dados pessoais**: atualizado com a MP 869/18. 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019.

MATZNER, Ryan. **Veja o que as redes sociais e buscadores fazem com os dados dos usuários**: Do Facebook ao Google, recolhimento de dados, venda de informação e compartilhamentos variam de empresa para empresa. Exame. 2018. Disponível em: https://exame.com/tecnologia/veja-o-que-as-redes-sociais-e-buscadores-fazem-com-os-dados-dos-usuarios/. Acesso em: 6 nov. 2022.

MENDES, Gilmar Ferreira; BRANCO, Paulo G. **Curso de direito constitucional**. 10 ed. São Paulo: Saraiva, 2015.

META. **Políticas de Privacidade do Facebook**. 2022. Disponível em: https://www.facebook.com/privacy/policy/entry_point=data_policy_redirect&entry=0. Acesso em: 2 nov. 2022.

MINISTÉRIO DA CIDADANIA. **Classificação dos Dados**. Gov.br. Brasília, 2021. Disponível em: . Acesso em: 2 nov. 2022.

MIRAGEM, Bruno. A lei geral de proteção de dados (lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, São Paulo, v. 1009, p. 173-224, nov. 2019.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP. **Cadernos Adenauer**, Rio de Janeiro, n. 3, p. 113-136, out. 2019.

MULHOLLAND, Caitlin. **A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais**: culpa ou risco?. Migalhas. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco. Acesso em: 8 out. 2022.

OLIVEIRA, José Eduardo da Silva. **Responsabilidade civil dos agentes de proteção de dados no Brasil**. João Pessoa, 2019 Monografia (Curso de Direito do Centro de Ciências Jurídicas) - Universidade Federal da Paraíba.

PESTANA, Marcio. **Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais)**. Consultor Jurídico. 2020. Disponível em: https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf. Acesso em: 8 nov. 2022.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais comentários à lei n. 13.709/2018**. São Paulo: Saraiva, 2018. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553608324/cfi/0!/4/2@100:0.00. Acesso em: 8 nov. 2022.

PRIVACIDADE acima de tudo: LGPD e Redes Sociais. Privacy Tools. YouTube, 2022. Disponível em: https://www.youtube.com/watch?v=D3LOMb8yvzM. Acesso em: 8 nov. 2022.

REDAÇÃO. **Sanções ao descumprimento da LGPD deverão surgir em breve**: Minuta de norma em audiência pública estabelece como punir infrações à lei de proteção de dados. Legislação & Mercado. 2022. Disponível em: https://legislacaoemercados.capitalaberto.com.br/sancoes-ao-descumprimento-da-lgpd-deverao-surgir-em-breve/. Acesso em: 8 nov. 2022.

RENÁ, Paulo. **Responsabilidade civil no tratamento de dados pessoais**: controvérsias sobre regime e ressarcimentos. Instituto de Referência em Internet e Sociedade. 2022. Disponível em: https://irisbh.com.br/responsabilidade-civil-no-tratamento-de-dados-pessoais-controversias-sobre-regime-e-ressarcimentos/. Acesso em: 7 nov. 2022.

RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

TADDICKEN, Monika. The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. **Journal of Computer-Mediated Communication**, v. 19, n. 2014. 248–273 p, 2013. Disponível em: https://academic.oup.com/jcmc/article/19/2/248/4067550. Acesso em: 6 nov. 2022.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Responsabilidade e ressarcimento de danos por violação às regras previstas na LGPD: um cotejamento com o CDC. *In:* LIMA, Cintia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 6 nov. 2022.

VENOSA, Silvio de Salvo. **Direito Civil**: obrigações e responsabilidade civil. 17 ed. São Paulo: Atlas, v. 2, 2017.

VIEIRA, Ronaldo. **LGPD**: o Brasil também entra no mapa. Security Report. 2018. Disponível em: https://www.securityreport.com.br/overview/lgpd-o-brasil-tambem-entra-no-mapa/#.Y2o-bHbMLrc. Acesso em: 8 nov. 2022.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Brasília, f. 297, 2007 Dissertação (Mestrado em Direito, Estado e Sociedade) - Universidade de Brasília.

WARREN, Samuel D.; BRANDEIS, Louis D.. The Right to Privacy. **Harvard Law Review**, v. IV, n. 5, 15 dez. 1890.

TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, Fernando Oliveria Melo, discente regularmente matriculado(a) na disciplina TCC II, da 10ª etapa do curso de Direito, matrícula nº 3187553-1, período - 10º, turma 10S, tendo realizado o TCC com o título: LEI GERAL DE PROTEÇÃO DE DADOS: Impactos e Imposições às Redes Sociais sob a orientação do Professor Luiz Gustavo Friggi Rodrigues, declaro para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 09 de novembro de 2022. .

Assinatura do discente