DIREITO
ISSN 2763-7999
SEÇÃO I: DIREITO, CULTURA E SOCIEDADE

DIREITO A PRIVACIDADE NA INTERNET: A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

THE RIGHT TO PRIVACY ON THE INTERNET: THE GENERAL LAW FOR THE PROTECTION OF PERSONAL DATA

Gustavo Costa Severiano[1] **Leonardo Barreto Ferraz Gominho**[2]

RESUMO: Esse estudo procurou analisar as novas conjecturas em relação à privacidade na internet, tendo em vista que a Lei Federal n.º 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados, entrou em vigor em 2020 no intuito de proteger as informações pessoais de seus usuários e consumidores. Busca-se avaliar se tal medida é eficaz, pois são diversas informações armazenadas em sites de grandes corporações sem qualquer segurança aos proprietários dos dados. O trabalho terá quatro divisões, primeiramente um breve relato sobre o uso da internet, posteriormente, um relato sobre a proteção da privacidade. A segunda parte mostrará as consequências da Lei e as reflexões sobre os vazamentos de dados recentes em grandes corporações A terceira parte do trabalho estudará os principais aspectos acerca da legislação em tela, com a análise acerca do consentimento do usuário para processar as informações e a última parte trará as conclusões obtidas através do estudo. O presente artigo é classificado como um estudo de natureza descritiva sob meio de uma pesquisa bibliográfica que apresentará a síntese de estudos disponibilizados no meio acadêmico. O estudo revelou que a Lei é ineficaz, pois não impediu que houvesse novos vazamentos de dados.
Palavras-chave: Privacidade. Responsabilidade Civil. Lei Federal n.º 13.709/2018.

ABSTRACT: This study sought to analyze new conjectures regarding internet privacy, considering that Federal Law No. 13.709/2018, better known as the General Data Protection Law, entered into force in 2020 in order to protect personal information of its users and consumers. It seeks to assess whether such a measure is effective, as there are several information stored on websites of large corporations without any security for data owners. The work will have four divisions, first a brief report on internet usage, later a report on the protection of privacy. The second part will show the consequences of the Law and reflections on recent data leaks in large corporations. The third part of the work will study the main aspects of the legislation on screen, with an analysis of the user's consent to process the information and the last part will bring the conclusions obtained through the study. This article is classified as a study of a descriptive nature through a bibliographical research that will present the synthesis of studies available in the academic environment. The study revealed that the Law is ineffective, as it did not prevent new data leaks.
Keywords: Privacy. Civil responsability. Federal Law No. 13,709/2018.

1 INTRODUÇÃO

A invasão da intimidade é um assunto de grande importância para o mundo jurídico em razão das consequências que esse fenômeno ocasiona. A internet, assim como outros meios de comunicação, invade a privacidade de terceiros de diversas formas, a exemplo de noticiários onde são divulgadas informações pessoais acerca de indivíduos sob a justificativa de proteger o interesse público.

Sabe-se que a internet surgiu com o departamento de defesa dos Estados Unidos em 1969, com a primeira conexão entre os computadores da Stanford e da UCLA, durante a Guerra Fria, e que na década de 90, Tim Berners-Lee desenvolveu o navegador: a *World Wide Web (www)*. Atualmente a internet se tornou um meio de comunicação

muito lucrativo, com armazenamento de todos os tipos de informações e de alto impulsionamento de notícias muitas vezes inverídicas (as chamadas fakes news) sendo também instrumento para a prática de diversos crimes, tanto no âmbito penal como na esfera civil.

Em todas as sociedades sempre existiram redes de convivência, a diferença é que hoje, com a internet, elas ultrapassaram as barreiras geográficas e proporcionaram a aproximação síncrona entre várias pessoas. Para adaptar-se a esses acontecimentos a legislação também evoluiu, para resguardar direitos dos indivíduos, a exemplo da Lei Carolina Dieckmann, que, passou a criminalizar a conduta de invasão de aparelhos eletrônicos para obtenção de dados particulares.

Hoje, as redes sociais são fontes para o consumo de informações, gerando novas discussões sobre a privacidade na internet no tocante ao tratamento de dados fornecidos pelos usuários, disseminados sem seu conhecimento. São inúmeras informações cruzadas com destreza e de forma economicamente acessíveis sobre perfis de qualquer indivíduo.

Esses dados também são utilizados para fins comerciais, onde empresas coletam e interligam atividades usuais nas redes. O resultado dessa prática é visível: assim que o internauta faz a busca de algum produto em algum site (a exemplo do Google), se depara com uma infinidade de ofertas referentes à sua pesquisa nas suas redes sociais. Em razão disso, o legislador editou a Lei Federal n.º 13.709/2018 conhecida como a Lei Geral de Proteção de Dados Pessoais.

O trabalho é classificado como um estudo de natureza descritiva sob meio de uma pesquisa documental e bibliográfica que apresentará a síntese de estudos disponibilizados no meio acadêmico. Trata-se de uma técnica de documentação indireta, com análise qualitativa e quantitativa das informações. A abordagem qualitativa é "um meio para explorar e para entender o significado que os indivíduos ou os grupos atribuem a um problema social ou humano". (CRESWELL; CRESWELL, 2007, p. 43).

Diante do exposto, o objetivo do trabalho é analisar a eficácia da referida Lei. Também se pretende verificar conceitos acerca de privacidade na internet e analisar a responsabilidade civil nos casos de violação da intimidade nas redes sociais, portanto, será estudado a Lei, jurisprudência, doutrina, e outros trabalhos acerca do tema.

Assim, começaremos a tratar sobre o direito à privacidade na vida digital.

2 O DIREITO À PRIVACIDADE NA VIDA DIGITAL

A internet não é apenas uma fonte de entretenimento, ela é um instrumento imprescindível para o trabalho e estudos. As próprias redes sociais se tornaram uma extensão do trabalho, sobretudo durante a pandemia decorrente do Covid19 em que os profissionais de diversos ramos divulgam seu trabalho através delas.

Existem empresas que aproveitam as informações postadas pelos usuários nessas ferramentas digitais, ou até mesmo "repassadas" por lojas em geral, para venda de seus produtos. Nesse contexto, a privacidade na internet tornou-se um campo de discussão jurídica.

O direito a intimidade é tutelado no artigo 5º, inciso X, da Constituição Federal de 1988, o qual determina que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas". (BRASIL, 1988, s.p.).

Estamos na Era da Informação, assim definido por Manuel Castells:

> Assim, computadores, sistemas de comunicação, decodificação e programação genética são todos amplificadores e extensões da mente humana. O que pensamos e como pensamos é expresso em bens, serviços, produção material e intelectual, sejam alimentos, moradia, sistemas de transporte e comunicação, mísseis, saúde, educação ou imagens. A integração crescente entre mentes e máquinas, inclusive a máquina de DNA, está anulando o que Bruce Mazlish chama de a "a quarta descontinuidade" (aquela entre seres humanos e máquinas), alterando fundamentalmente o modo pelo qual nascemos, vivemos, aprendemos, trabalhamos, produzimos, consumimos, sonhamos, lutamos ou morremos. (CASTELLS, 1999, p. 69).

Porém há um grau elevado de exposição na internet, e o controle da própria apresentação individual se torna difícil, com consequências jurídicas (difamação, calúnia, invasão de computadores, compartilhamento não consentido de imagens), sendo importante que o Direito acompanhe as inovações da sociedade.

No tocante as relações contratuais na internet, essas são firmadas na confiança dos usuários para com os sites que exigem a concordância expressa de suas condições: "li e aceito os termos do contrato". Esses compromissos necessitam de uma proteção jurídica, tal quais os demais contratos formais.

Não obstante, as informações prestadas pelos internautas estão frequentemente alimentando bancos de dados, e esses, usados para anúncios, como uma espécie de análise de comportamento do consumidor. Nesse sentido, tem-se que há um ciclo de vida da informação, onde empresas coletam, armazenam e transferem dados da rede. Nas palavras de Ana Frazão:

> Ao se referir expressamente ao livre desenvolvimento da personalidade, à cidadania e à dignidade, a lei certamente procura evitar muitas das destinações atuais que vêm sendo conferidas aos dados pessoais, os quais, processados por algoritmos, são capazes de fazer diagnósticos e classificações dos usuários que, por sua vez, podem ser utilizados para limitar suas possibilidades de vida. Mais do que isso, a partir de tais dados, as empresas podem discriminar usuários ou mesmo tentar manipular suas opiniões, crenças ou valores em vários âmbitos, inclusive o político. (FRAZÃO, 2018, s.p.).

Por conseguinte, cumpre analisar a privacidade em relação à proteção dos dados disponibilizados via digital, através de aspectos jurídicos, sobretudo na Lei de Proteção de Dados.

3 A LEI DE PROTEÇÃO DE DADOS

A Lei de Proteção de Dados é descendente direta do Regulamento Geral da Proteção de Dados que surgiu na Europa após os escândalos de vazamento de dados sem consentimento por parte de gigantes como o Facebook. Pioneira no ramo, o Regulamento Geral da Proteção de Dados atualizou a lei de privacidade europeia de 1995, com o objetivo de garantir transparência aos cidadãos no que diz respeito ao uso dos seus dados. (GUNTHER; COMAR; RODRIGUES, 2020, s.p.).

No caso do Brasil, a Lei de Proteção de Dados especifica alguns pontos do abrangente Marco Civil da Internet, sancionado em 2014, e vem para colocar o país no mesmo patamar das nações europeias e norte-americanas no combate ao tratamento indevido de dados na internet. A lei tem enorme alcance e ampla abrangência, pois praticamente qualquer pessoa ou empresa que armazena algum dado de seus clientes e fornecedores, sofrerá o impacto e deverá se enquadrar aos ditamos legais da legislação. (PESTANA, 2021, s. p.).

A Lei Geral de Proteção de Dados Pessoais é a lei brasileira que impõe regulamentação acerca da coleta e tratamento a ser dado aos dados dos usuários, determinando ainda sanções para quem infringi-la. Embora já houvesse legislação que tratassem do assunto, essas não traziam a segurança jurídica necessária para tratar de conflitos concretos. A mencionada lei veio legislar sobre os usos de dados pessoais no Brasil, seja na esfera pública quanto privada regulamentando a privacidade de dados. A motivação para a criação dela adveio da utilização cada

vez mais frequente de dados pessoais, tendo esses se tornado um recurso valioso, a sociedade usar as redes sociais causando grande impacto no comportamento das pessoas. (GUNTHER; COMAR; RODRIGUES, 2020, s.p.).

Publicada em agosto de 2018, a Lei Geral de Proteção de Dados, trouxe à tona maiores obstáculos nos setores públicos e privados, que utilizam diretamente essas informações. Assim, o setor empresarial deverá se adequar aos princípios norteadores da referida lei, sobretudo a boa-fé, finalidade, transparência e segurança, entre outros. (PESTANA, 2021, s. p.).

O princípio da finalidade institui como condição necessária para a coleta de dados uma ligação entre o uso deles e o fim pretendido, sendo necessário o esclarecimento dessa coleta ao seu titular. O princípio da transparência impõe que as empresas divulguem em registros públicos, o nome sede e conteúdo, deixando explícito de que possuem bancos de dados de conhecimento público. No tocante ao princípio da segurança, as empresas devem se assegurar que haja a proteção dos dados pessoais contra extravios, desvios e alterações desautorizados por seus donos. (ASSIS E MENDES, 2021, s.p.).

Desse modo, podemos compreender que o objetivo da Lei é preservar "os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". (FRAZÃO, 2018, s.p.). Isto é, dar mais custódia ao tratamento de dados pessoais na internet. Nesse sentido, importante compreender o conceito de tratamento de dados.

Patrícia Peck Pinheiro entende que é possível conceituar o tratamento de dados da seguinte forma:

> Toda operação realizada com algum tipo de manuseio de dados pessoais: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (PINHEIRO, 2018, p. 25).

O Decreto Regulamentador do Marco Civil da Internet assim dispõe:

> Art. 14. Para os fins do disposto neste Decreto, considera-se:
> I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e
> II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (BRASIL, 2016, s.p.).

O objetivo da Lei Geral de Proteção de Dados Pessoais é preservar os direitos previstos na Constituição Federal de 1988 e assegurar a privacidade e determinar como deve ser realizado o tratamento dos dados pessoais, pelas organizações públicas e privadas. Além disso, coloca o Brasil numa mesma posição jurídica em relação a outros países que já possuíam uma legislação específica acerca do tema. Trata-se de uma lei com parâmetros técnicos para assegurar a supracitada proteção de dados sendo indiscutivelmente importante para assegurar melhorias aos usuários da internet tendo em vista que essas informações pessoais são, na verdade, parte da personalidade individual, merecendo ser resguardadas com uma legislação específica e para isso, é importante compreender alguns termos técnicos trazidos pela legislação que começa estabelecendo nomenclaturas e criando algumas figuras no processo de tratamento dos dados, definições que são imprescindíveis para operar com a Lei. (GUNTHER; COMAR; RODRIGUES, 2020, s.p.).

Dado Pessoal é qualquer informação relativa a pessoa "identificada ou identificável"; Dado Pessoal Sensível é informação relativa à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização, saúde, vida sexual ou dado genético ou biométrico; Dado Anonimizado é relativo a um titular que

não possa ser identificado; Banco de Dados é o conjunto estruturado de informações pessoais; Titular é a pessoa a quem se referem os dados; Controlador é a pessoa responsável por tomar as decisões referentes a tratamento de dados; Operador é quem executa o tratamento em nome do controlador; Encarregado é a pessoa responsável pela comunicação entre as três partes: o controlador e o operador (empresa), o titular e a Autoridade Nacional de Proteção de Dados; Consentimento é a manifestação livre pela qual o titular permite o uso dos dados (o ônus da prova cabe ao controlador); Relatório de impacto à proteção de dados pessoais é a documentação do controlador descrevendo o processo de tratamento dos dados que podem gerar risco às liberdades civis. (GUNTHER; COMAR; RODRIGUES, 2020, s.p.).

Cumpre salientar que o rol de dados pessoais elencados no Decreto n.º 8.771/2016 não é taxativo, cabendo interpretação extensiva. Além disso, a Lei Geral de Proteção de Dados Pessoais possui validade extraterritorial, sendo irrelevante se os titulares são brasileiros ou estrangeiros. (GUNTHER; COMAR; RODRIGUES, 2020, s.p.).

A Lei Geral de Proteção de Dados Pessoais não se trata de um simples software, pois os órgãos públicos e privados deverão possuir relatórios com as informações que possui de cada indivíduo. Também precisarão contratar/possuir um funcionário incumbido pelo manuseio dessas informações, sendo também criminalizado, caso a empresa infrinja a norma. A organização também necessitará instituir uma espécie de Serviço de Atendimento ao Consumidor (SAC).

> Assim que a lei entrar em vigor, todas as empresas brasileiras e todos os órgãos públicos terão de estar preparados para responder às seguintes perguntas feitas por qualquer cidadão: que dados possui de cada pessoa? Para que usou os dados? Qual a justificativa para ter cada um dos dados? Transferiu essas informações para outras pessoas ou empresas? Transferiu de graça ou teve lucro com isso? Os dados estão seguros? Já vazaram alguma vez? Se vazou, fez alguma coisa para evitar um novo vazamento? (...), qualquer pessoa poderá exigir essas informações de qualquer empresa (...). Sabe aquele corretor de imóveis que fica te ligando e você nem sabe de como ele tem o seu número de telefone? Ele vai ter de explicar onde e como conseguiu isso. (...). Qualquer vazamento de dados precisará ser informado imediatamente. E as empresas poderão pagar multas milionárias caso não obedeçam a lei. (PAULA, 2021, s.p.).

Qualquer pessoa que possua um negócio de qualquer porte e lida com informações do público, sejam elas específicas ou tão simples quanto apenas um nome, é muito importante estar por dentro da legislação, pois a partir do corrente ano de 2021, todas as empresas do Brasil precisarão estar em concordância com essas regras. (ASSIS E MENDES, 2021, s.p.).

O ponto central da Lei Geral de Proteção de Dados Pessoais é a necessidade de consentimento expresso do titular para armazenamento dos seus dados. Fica proibido ceder ou vender informações de contato de potenciais clientes para divulgação de produtos e serviços por telemarketing, por exemplo. Está proibido até mesmo o uso dos dados por parte da própria empresa para uma finalidade diferente daquela que foi combinada com o cliente. É preciso obter o consentimento específico e ser capaz de provar isso a qualquer momento (é o caso dos pop-ups nos sites, por exemplo, que perguntam se o usuário está de acordo em fornecer informações pessoais). (ASSIS E MENDES, 2021, s.p.).

Para os dados considerados sensíveis, o processo é ainda mais rigoroso. No caso de dados de crianças e adolescentes, é preciso o consentimento de ao menos um dos pais ou responsável legal. O que está proibido, segundo a lei: “Acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”. (BRASIL, 2021, s.p.).

Entre as sanções previstas para descumprimento das medidas de proteção de dados está uma multa de 2% (dois por cento) do faturamento total da empresa ou do conglomerado, limitada a R$ 50.000.000,00 (cinquenta milhões de reais). Os agentes de tratamento: Controlador e Operador devem adotar medidas de segurança para proteger os dados, mantendo o registro de todos os processos realizados. (ASSIS E MENDES, 2021, s.p.).

Embora exista ainda muita discussão sobre a abrangência da lei, tendo em vista que não fora determinado o nível de rigor na fiscalização e punição para organizações multimilionárias e para negócios locais ou Organizações Não Governamentais, por exemplo. Todavia, sabe-se que toda empresa com algum tipo de cadastro de clientes ficará sujeita à Lei Geral de Proteção de Dados Pessoais. Para isso é necessário seguir alguns passos: Elaborar um plano de ação, discorrendo sobre quais as informações das pessoas percorrem na organização, sendo importante conhecer toda a vida útil desses dados, desde a coleta até o armazenamento, a finalidade de uso etc.. Dependendo do porte da organização e da complexidade dos serviços realizados, pode ser recomendável a contratação dos serviços de uma consultoria. (GUNTHER; COMAR; RODRIGUES, 2020, s.p.).

Com o levantamento dessas informações específicas, é preciso ir mais a fundo na lei, é a hora da empresa acionar o departamento jurídico e consultar assessoria especializada, desenvolvendo um planejamento. Também deve ser definido os agentes de tratamento de dados: o controlador e o(s) operador(es), o encarregado, responsável por fazer o contato com os clientes, com o público interno (funcionários) e com a recém-criada agência reguladora. Independentemente dessas quais medidas, é importante lembrar que o grande objetivo de toda essa mudança é aumentar a segurança dos cidadãos e a transparência das empresas. Os clientes poderão questionar a qualquer momento a situação dos seus dados ou até mesmo pedir a exclusão de tudo. (ASSIS E MENDES, 2021, s.p.).

A ideia da Lei Geral de Proteção de Dados Pessoais é criar uma cultura de respeito à privacidade dos dados e como consequência para quem não se adaptar, estará sujeito ao pagamento de multas. Assim, toda empresa que registre qualquer informação sobre clientes deverá estar atenta a essa norma, que, entre outras disposições, proíbe qualquer empresa de transmitir esses dados sem consentimento expresso dos titulares. (GUNTHER; COMAR; RODRIGUES, 2020, s.p.).

Transcorrida esta etapa seguiremos para abordar casos de alerta que justificam a criação da Lei Geral de Proteção de Dados Pessoais.

4 OS CASOS QUE JUSTIFICAM A CRIAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

O vazamento de informações pessoais é um acontecimento fortemente danoso, tendo em vista que algum hacker pode utilizar para praticar diversas condutas ilícitas (falsidade ideológica, desvio de dinheiro, phishing...) ocasionando também prejuízos financeiros. O Brasil possui vários casos de vazamentos de dados, conforme demonstrado por Ivan Ventura: “Segundo um estudo anual da IBM em parceria com o Instituto Ponemon ‘Cost of a Data Breach’, o Brasil é o quarto País em volume de informação vazada a partir de um incidente de segurança, atrás apenas de países do Oriente Médio, da Índia e dos EUA. Os dados são de 2019”. (VENTURA, 2021, s.p.).

Dentro deste contexto, podemos citar como exemplos: o Instituto Nacional de Colonização e Reforma Agrária (INCRA) que em outubro de 2019 deixou exposto o nome completo, telefone e C.P.F. de beneficiários do referido instituto. (CARNEIRO, 2021, s.p.); o Plataforma de Gestão Inteligente da Nota Fiscal de Serviço Eletrônica (GINFES) que vazou o nome completo, endereço, e-mail, C.P.F./C.N.P.J., descrição e valor do serviço de todos os

brasileiros que utilizavam a plataforma de emissão de notas fiscais. (OLHAR DIGITAL, 2021, s.p.); o Departamento Estadual de Trânsito do Estado do Rio Grande do Norte (DETRAN-RN) que deixou exposta ficha cadastral de todos os brasileiros portadores de Carteira de Habilitação ou proprietários de veículos. (OLHAR DIGITAL, 2021, s.p.); o Facebook que vazou dados de 87.000.000 (oitenta e sete milhões) de pessoas, destes, mais de 443.000 (quatrocentas e quarenta e três mil) são brasileiros. (ASSIS E MENDES,2021, s.p.); o Uber que vazou 57.000.000 (cinquenta e sete milhões) de dados em 2016, sendo 196.000 (cento e noventa e seis mil) clientes brasileiros. (ASSIS E MENDES, 2021, s.p.); o Adobe que vazou 38.000.000 (trinta e oito milhões) de dados em 2013, com estimativa de que 152.000.000 (cento e cinquenta e dois milhões) de nomes e senhas expostos e 2.800.000 (dois milhões e oitocentos mil) números de cartões de crédito. (ASSIS E MENDES, 2021, s.p.); e ainda o Netshoes que expos 2.000.000 (dois milhões) de dados, de números de C.P.F., e-mail e data de nascimento. (ASSIS E MENDES, 2021, s.p.).

Mesmo com a promulgação da Lei Federal n.º 13.709/2018, ainda houve casos de vazamento de dados, o que demonstra a fragilidade da rede. No corrente ano de 2021, infringindo a própria Lei em vigência, dados de usuários foram mais uma vez expostos, na qual ainda estão sob investigação pela Autoridade Nacional de Proteção de Dados (ANPD), consoante se observa a seguir:

> A empresa de cibersegurança PSafe detectou, logo nos primeiros dias de 2021, um vazamento de dados sensíveis de 223 milhões de brasileiros – praticamente, a totalidade da população. Entre as informações potencialmente expostas estavam CPF, nome completo, data de nascimento e até score de crédito dos cidadãos. No mês seguinte, o mesmo laboratório relatou que foram expostos indevidamente RG, CPF, data de nascimento, e-mail, endereço, número do celular e informações sobre a fatura de 102,8 milhões de contas de celulares das operadoras Claro, Vivo, Oi e Tim. (DALLABRIDA, 2021, s.p.).

Entretanto, cumpre salientar que, na comprovação do responsável pelo armazenamento dos dados, e, pelo consequente dever de armazenamento das informações, a Autoridade Nacional de Proteção de Dados tem como função aplicar as multas previstas na Lei Geral de Proteção de Dados Pessoais.

Após estes dados alarmantes, traremos questionamentos sobre a ineficácia da Lei Geral de Proteção de Dados Pessoais.

5 A ANALOGIA DA LEGISLAÇÃO ESTRANGEIRA

Outros países também já legislaram acerca da proteção de dados. Inicialmente vale ressaltar que essa preocupação advém desde a década de 1970, em que foram criadas leis europeias que tratavam do assunto, em Hessen, na Alemanha. Essa preocupação em legislar sobre os dados adveio do avanço no uso do computador pela população e veio a ser concretizada em 1978, com o objetivo de verificar como os dados de seus cidadãos eram utilizados. Posteriormente, outros países seguiram com a mesma proposta, a exemplo da França e Suécia. (GLOGOVCHAN, 2021, s.p.).

Já “em 1981, uma convenção elaborada pelos países membros do então Conselho da Europa ajudou a unificar e desenvolver melhor as normas para o tratamento automatizado de dados pessoais”. (ASSIS E MENDES, 2021. s.p.).

Em 1995 a Europa regulamentou um conjunto de normas a serem obedecidas pelos países da União Europeia, nas quais aperfeiçoaram a concepção acerca da custódia de informações pessoais até então existentes e que resultaram no conceito de proteção de dados análogos as Leis atuais. Os “princípios como recolhimento de

dados de acordo com uma finalidade específica, direito ao acesso dos dados por parte do consumidor e responsabilidade das empresas sobre a segurança das informações armazenadas, já são abordados na lei". (ASSIS E MENDES, 2021, s.p.).

Dando prosseguimento na preocupação legislativa, em 2018, a Europa criou o Regulamento Geral sobre a Proteção de Dados europeu (GDPR), decorrente da necessidade de proteger dados pessoais que estavam constantemente sendo vazados na internet, além do uso constante do comércio dessas informações. Este regulamento forçou empresas como Facebook e Google a adotarem uma série de medidas para evitar novos vazamentos de dados, e foi motivador para que outros países, como o Brasil, legislassem sobre o tema. (COMPUGRAF, 2021, s.p.). Acerca disso, cabem algumas observações sobre o funcionamento do Regulamento Geral sobre a Proteção de Dados Europeu (GDPR):

> Alega que a transferência internacional dos dados pode ser realizada independente de autorização específica caso a comissão europeia reconheça que o país terceiro assegure um nível de proteção adequado. Caso não, a transferência internacional estará condicionada a garantias adequadas, que devem ser asseguradas pelo Agente. Todos os procedimentos e elementos que são levados em consideração pela Comissão para a autorização da transferência estão descritos na GDPR. (COMPUGRAF, 2021, s.p.).

O Regulamento Geral sobre a Proteção de Dados Europeu (GDPR) objetiva proteger dados e identidade dos cidadãos da União Europeia, pois embora já houvesse leis sobre a temática desde 1995, elas não se adequavam ao cenário tecnológico atual. Aprovado em 2016 essas diretrizes obrigam as empresas a se adequarem a regras para coleta, processamento, compartilhamento e guarda de dados pessoais. (ALECRIM, 2021, s.p.).

As principais obrigações são as seguintes:

> O serviço deverá permitir que o usuário escolha como os seus dados serão tratados e autorize ou não o seu uso; O usuário tem direito de saber quais dados estão sendo coletados e para quais finalidades; Deve haver meios para que o usuário solicite a exclusão de informações pessoais ou interrompa a coleta de dados, com a decisão devendo ser respeitada; O usuário também pode acessar, solicitar cópia ou migrar dados coletados para outros serviços (quando cabível); Uso de linguagem clara, concisa e transparente para que qualquer pessoa possa compreender comunicações sobre seus dados, inclusive termos de privacidade; Em caso de incidentes que resultem em vazamento ou violação de dados que podem ferir direitos e a liberdade das pessoas, a organização deverá notificar autoridades em até 72 horas; Aplicação da privacidade por design: a proteção dos dados deve ser considerada desde o início do projeto de um sistema, como parte imprescindível deste; (ALECRIM, 2021, s.p.).

Esse regulamento afeta outros países, inclusive o Brasil, primeiro porque, como mencionado, incentivou a regulamentação sobre o uso dos dados e segundo porque para que lojistas de outros países possam vender seus produtos à União Europeia deverão se adequar a Lei. Todavia nem todos os países se adequaram a essa nova realidade:

> Venezuela, Equador, Bolívia, Egito, Somália, Israel, Paquistão e outros, por exemplo, não contam com nenhuma lei específica sobre o tema. Já países como Índia, Chile, Paraguai, Rússia e China contam com algumas leis de proteção a dados pessoais, mas nada oficializado. Por outro lado, o Brasil, a Austrália, África do Sul, Turquia e México são exemplos de países que possuem autoridade nacional e leis de proteção de dados pessoais, com a LGPD. A Argentina, o Japão e a Nova Zelândia estão adequados quanto a lei mundial GDPR. Já os países da Europa, obviamente, como Alemanha, Polônia, Itália, Espanha, França, Inglaterra e outros estão fortemente adequados à GDPR. (GLOGOVCHAN, 2021, s.p.).

Nos Estados Unidos, "apesar de não existir uma lei federal que determine regras para a preservação de dados pessoais (...) a exemplo da GDPR europeia ou da LGPD brasileira, existem várias legislações locais, de âmbito estadual, com esse objetivo". (CONECTAJÁ, 2021, s.p.).

Nota-se que a Lei Geral de Proteção de Dados é um avanço na legislação brasileira, que busca se adequar as novas realidades tecnológicas e a necessidade de cooperação com outros países, na busca pelo uso consciente de dados pessoais pelas empresas.

6 A INEFICÁCIA DA LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD) possui algumas lacunas, e por ser uma nova Lei, também é cercada por dúvidas na sua execução. Uma dessas incertezas está relacionada a forma de responsabilização dos agentes de dados, quando houver as condutas danosas previstas na Lei, pois não é possível identificar se ela é subjetiva ou objetiva.

Maria Helena Diniz nos traz apontamentos relevantes a respeito:

> A responsabilidade civil é a aplicação de medidas que obriguem alguém a reparar dano moral ou patrimonial causado a terceiros em razão de ato do próprio imputado, de pessoa por quem ele responde, ou de fato de coisa ou animal sob sua guarda (responsabilidade subjetiva), ou, ainda, de simples imposição legal (responsabilidade objetiva). (DINIZ, 2003, p. 34).

E complementa: "A responsabilidade civil é a aplicação de medidas que obriguem uma pessoa a reparar dano moral ou patrimonial causado a terceiros, em razão de ato por ela mesmo praticado, por pessoa por quem ela responde, por alguma coisa a ela pertencente ou de simples imposição legal". (DINIZ, 2003, p. 36).

Com efeito, diz-se que são elementos subjetivos da responsabilidade civil o "dano", "nexo causal" e "culpa ou dolo". Para que a reparação civil ocorra, é necessário, portanto, esses três elementos só se podem falar em direito à reparação quando presentes os três elementos. (MAIA, 2016, s.p.).

Entretanto, em decorrência da interpretação de que o tratamento de dados seja uma atividade de risco, adequar-se ia ao parágrafo único do artigo 927, do Código Civil, além disso, a Lei apresenta apenas um rol exemplificativo de condutas. (BRASIL, 2002, s.p.).

Por outro lado, nas circunstâncias da Lei Geral de Proteção de Dados deve ser considerado, um terceiro elemento: o hacker. É ele quem usa suas aprendizagens para o acesso ilegal de sites de terceiros, possuindo também ingresso aos dados pessoais armazenados.

Nesse caso, quando há vazamentos mesmo com a devida aplicação de normas de segurança pelos agentes de dados, caberia à interpretação de uma responsabilidade subjetiva, sendo imprescindível avaliação da existência de culpa, dolo, erro de conduta por imprudência, negligência e/ou imperícia.

A imprudência ocorre na realização de um ato sem o cuidado necessário, é saber fazer um ato, mas fazendo-o, não toma a devida cautela; a negligência ocorre com uma omissão no cuidado, quando o agente dá causa a um resultado, por deixar de praticar uma ação que sabe que deveria fazer; a imperícia é o não saber fazer, a realização de uma ação sem o conhecimento necessário. Ex.: Dirigir sem ser habilitado e provocar um acidente. (MAIA, 2016, s.p.).

Outra questão que precisa ser considerada são as hipóteses de excludente por caso fortuito ou força maior, que são excludentes de responsabilidades, isentando o agente da conduta delituosa de ser responsabilizado pelos danos causados em situações excepcionais. É excludente de responsabilidade, "que impedem que o nexo causal, a culpa da vítima, o fato de terceiro, o caso fortuito e a força maior e, no campo contratual, a cláusula de não indenizar". (VENOSA, 2007, p. 40).

Álvaro Villaça Azevedo ensina que "caso fortuito é o acontecimento provindo da natureza, sem qualquer intervenção da vontade humana" (AZEVEDO, 2001, p. 270), enquanto a força maior, nos dizeres de Maria Helena Diniz:

> Na força maior conhece-se o motivo ou a causa que dá origem ao acontecimento, pois se trata de um fato da natureza, como, p. ex., um raio que provoca um incêndio, inundação que danifica produtos ou intercepta as vias de comunicação, impedindo a entrega da mercadoria prometida, ou um terremoto que ocasiona grandes prejuízos etc. Já no caso fortuito, o acidente que acarreta o dano advém de causa desconhecida, como o cabo elétrico aéreo que se rompe e cão sobre fios elétricos, causando incêndio, explosão de caldeira de usina, e provocando morte. (DINIZ, 2013, p. 356).

Assim, para ocorrer à punição, deve ser avaliada uma série de fatores, o mero vazamento de dados não tem o condão de responsabilizar o agente de dados visto que outros elementos devem ser considerados, a saber: as condutas preventivas para o não vazamento, e as repreensivas (para a identificação/punição do responsável pelo vazamento).

Outro fator que merece ser considerado para fins de responsabilização quanto a Lei Geral de Proteção de Dados está relacionado aos casos concretos de vazamentos de dados esporádicos de consumidores/usuários. Como identificar qual empresa seria a responsável pelo vazamento de um determinado dado pessoal, tendo em vista, o armazenamento deste, por várias outras empresas? Num primeiro momento, só seria possível a identificação desse vazamento em casos extravagantes como os já mencionados no presente trabalho.

Pelo que fora exposto, estamos diante da primeira condição de ineficácia da Lei em análise: a responsabilização do agente causador do dano.

A segunda condição de ineficácia da Lei está relacionada à fiscalização do armazenamento desses dados, que ficou na incumbência da Autoridade Nacional de Proteção de Dados (ANPD).

Como visto o texto legal já está em vigor (tendo sido alterado por duas vezes), mas a fiscalização administrativa e respectivas punições começaram a valer em 2021, com a finalmente instituída Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por fiscalizar todo o processo.

> O que dará eficácia à Lei Geral de Proteção de Dados é a autoridade, um órgão que tem um papel supervisor, garantidor e regulatório da lei (...). Em uma lei assim, é fundamental ter um órgão regulador para normatizar os vários temas inspirados na lei, as formas infralegais que serão fundamentais para que a LGPD tenha eficácia. Por isso a necessidade de um órgão regulatório forte, supervisor e que tenha autonomia. (CONECTAJÁ, 2021, s.p.).

Inicialmente a criação da Autoridade Nacional de Proteção de Dados (ANPD) fora vetada pelo então presidente da República Michel Temer sob a justificativa de vício de iniciativa. Inicialmente esse órgão deveria ter autonomia administrativa e financeira, com equipe técnica multidisciplinar, ligado ao Ministério da Justiça, com competência normativa. Porém a Autoridade Nacional de Proteção de Dados (ANPD) foi constituída como órgão ligado à Presidência da República, dependente, e sem aumento de despesa, conforme Lei Federal n.º 13.853/2019: "Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República". (BRASIL, 2021, s.p.).

Assim, a Autoridade Nacional de Proteção de Dados (ANPD) perde o poder de fiscalização quanto ao tratamento de dados pelo Estado, uma vez que a própria Administração Pública irá "se fiscalizar".

A Lei também se torna ineficaz, nesse sentido em virtude de não se esperar as mesmas exigências para o setor público e privado.

Transcorrida mais uma etapa, o estudo prosseguirá para analogia da legislação estrangeira.

7 CONCLUSÃO

Este artigo inquiriu acerca da Lei Geral de Proteção de Dados (LGPD) que é uma importante ferramenta no combate ao vazamento de dados e fez com que o Brasil alcançasse o patamar de outros países. Porém há lacunas no tocante a responsabilização objetiva ou subjetiva e deixa margens para que não haja o mesmo rigor na punição de órgãos privados e públicos tendo em vista que o órgão fiscalizador não é autônomo.

A consequência que se pode obter é que o legislador buscou normatizar o tratamento de dados pessoais, na tentativa de evitar vazamentos ou comercialização abusiva de informações pessoais.

Observa-se que as empresas de maior porte têm buscado se adequar tanto a Lei Geral de Proteção de Dados (Brasil), quanto ao Regulamento Geral de Proteção de Dados (União Europeia), esse fenômeno é visível, tendo em vista que os usuários da internet têm recebido constantes e-mails e notificações sobre atualizações em termos de privacidade. Porém a simples autorização de pop ups pelos usuários de internet não é medida suficiente para assegurar que as empresas possam armazenar os dados dos usuários sem quaisquer cautelas.

A globalização e os avanços na tecnologia proporcionam uma série de avanços na forma como as pessoas se relacionam, como se comportam no comércio de produtos e na exposição da vida cotidiana, mas trouxeram consigo um conjunto de consequências que precisavam ser positivadas no ordenamento jurídico internacional. Muito embora a Constituição da República Federativa do Brasil de 1988, em seu artigo 5º, menciona o direito à privacidade, essa prerrogativa necessitava de uma regulamentação específica e nesse sentido a Lei fora benéfica.

Sob o ponto de vista dos autores, é importante o desenvolvimento de ferramentas que tornem possível que o usuário saiba de forma mais detalhada quais informações estão sendo colhidas, qual o objetivo de armazená-las e como excluí-las, pois embora essas informações possam ser exigidas pelo usuário, o procedimento para adquiri-las é burocrático.

A Lei Federal n.º 13.709/2018, que está em vigência, aponta uma série de nomenclaturas, tratamento diferenciado para os dados considerados "sensíveis", condutas, punições, e desse modo simboliza ainda que tardiamente (em relação a União Europeia) a efetivação de prognósticos mencionados na Lei do Marco Civil da Internet, regulamentando efetivamente o tratamento dessas informações pessoais.

O dever de indenizar, quando positivado, traz certa sensação de segurança jurídica, e desse modo, havia uma lacuna quanto essa determinação a ser cumprida no mundo cibernético. Além disso, a divulgação desses direitos previstos na supracitada lei permite ao cidadão o conhecimento de garantias que não tinha conhecimento, embora certas condutas, hoje vedadas, fossem comuns (Quem nunca se perguntou como de vez em quando apareciam empresas munidas de informações pessoais oferecendo produtos e serviços?).

A criação da Autoridade Nacional de Proteção de Dados foi um ponto polêmico, tendo em vista que ele estava previsto inicialmente na Lei como um órgão independente, posteriormente ele vetado pelo então presidente Michel Temer, sob alegação de vício de iniciativa, já que gerava custos pelo poder executivo, essa Autoridade deveria ser criada por esse poder. A Autoridade Nacional de Proteção de Dados, finalmente criada pelo poder executivo através de uma medida provisória, mas sem autonomia financeira e vinculado a Presidência da República. Esse órgão é importante para a efetividade da Lei, embora se questione no presente estudo, como seria feito a fiscalização nos órgãos públicos.

A soma desses dois fatores: lacuna na legislação quanto ao tipo de responsabilidade e órgão fiscalizador não autônomo, torna a lei ineficaz. Não obstante, essa ineficácia aponta para um risco na segurança da informação digital no Brasil, e na prática de comércio internacional, considerando que deve haver uma adequação das normas brasileiras com o Regulamento Geral sobre a Proteção de Dados Europeu (GDPR).

A Lei em questão afeta a todos e é necessária uma adequação a essas normas de modo efetivo, e nesse sentido, todos devem cooperar: o Estado através da correta e imparcial fiscalização, as empresas na execução de todas as medidas previstas na legislação, e os cidadãos na supervisão de seus diretos e deveres.

Assim, uma das contribuições desse estudo foi o resumo de sanções disciplinares e a definição de algumas terminologias importantes na Lei, que definem a responsabilização de cada agente dentro das empresas que permitirem de algum modo o vazamento de dados, incluindo ainda a discussão acerca da responsabilidade civil.

O trabalho demonstrou ainda exemplos de vazamento de dados pessoais sensíveis, fato que torna incontroverso a necessidade da criação da mencionada Lei Geral de Proteção de Dados. Porém, indica que mesmo com a vigência das Leis referentes à proteção de Dados os vazamentos podem ocorrer, o que comprova que a Lei precisa de melhorias, porquanto no momento ainda é ineficaz.

Por fim, o artigo verificou que a responsabilização dos agentes depende de uma interpretação acerca da subjetividade da conduta, pois caso a empresa tenha adotado todos os procedimentos de segurança exigidos e mesmo assim tenha sido alvo de hacker, por exemplo, ou algum fenômeno de força maior, haverá uma série de interpretações divergentes quanto a punição a ser aplicada, tendo em vista a lacuna na legislação. O estudo revelou que são necessárias maiores adequações.

Como sugestão de pesquisa para um trabalho posterior, é a pesquisa em loco para obter informações acerca da fiscalização da Autoridade Nacional de Proteção de Dados (ANDP) nos órgãos públicos.

REFERÊNCIAS

ASSIS E MENDES. 5 casos de vazamento de dados nas grandes empresas. Assis e Mendes, 2021. Disponível em: https://assisemendes.com.br/vazamento-de-dados-nas-empresas/. Acesso em: 09 abr. 2021.

ALECRIM, Emerson. O que é GDPR e que diferença isso faz para quem é brasileiro. Disponível em: https://tecnoblog.net/245101/gdpr-privacidade-protecao-dados/. Tecnoblog, 2019. Acesso em: 25 mai. 2021.

AZEVEDO, Álvaro Villaça. Teoria Geral das obrigações e responsabilidade civil. São Paulo: Atlas, 2001.

BRASIL. Constituição da República Federativa do Brasil de 1988. Planalto, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 mar. 2021.

BRASIL. Decreto 8.771 de 2016. Regulamenta a Lei n. 12.965, de 23 de abril de 2014. Planalto, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm#:~:text=Regulamenta%20a%20Lei%20n%C2%BA%2012.965,transpar%C3%AAncia%20na%20requisi%C3%A7%C3%A3o%20de%20dados. Acesso em: 21 mar. 2021.

BRASIL. Lei n.º 13.709/2018. Lei Geral de Proteção de Dados. Planalto, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 21 mar. 2021.

CARNEIRO. Eduardo. Brasil registra onda de vazamentos (e até leilão) de dados na internet. Konduto blog, 2019. Disponível em: https://blog.konduto.com/pt/2019/10/onda-de-vazamento-de-dados-no-brasil/. Acesso em: 09 abri. 2021.

CASTELLS, Manuel. A sociedade em rede. Trad. Roneide Venâncio Majer. 14 ed. Paz e Terra, 2000.

CONECTAJÁ. Eficácia da lei. Conectajá, 2019. Disponível em: https://conectaja.proteste.org.br/anpd-funcionamento-da-autoridade-dara-eficacia-a-lgpd/#:~:text=Efic%C3%A1cia%20da%20lei,regulat%C3%B3rio%20da%20lei%20(%E2%80%A6).&text=Por%20isso%20a%20necessidade%20de,supervisor%20e%20que%20tenha%20autonomia.%E2%80%9D. Acesso em: 13 mai. 2021.

CONECTAJÁ. Veja como são as leis de proteção de dados nos Estados Unidos. Conectajá, 2020. Disponível em: https://conectaja.proteste.org.br/veja-como-sao-as-leis-de-protecao-de-dados-nos-estados-unidos/. Acesso em: 25 mai. 2021.

COMPUGRAF. LGPD em vigor e a transferência internacional de dados. Compugraf, 2020. Disponível em: https://www.compugraf.com.br/transferencia-internacional-de-dados-lgpd/#:~:text=Transfer%C3%AAncia%20Internacional%20de%20Dados%20na%20LGPD,-LGPD%20(Brasil)%20%E2%80%93&text=Permite%20a%20transfer%C3%AAncia%20de%20dados,a%20serem%20considerados%20como%20adequados. Acesso em: 25 mai. 2021.

CRESWELL, John W.; CRESWELL, J. David. Projeto de pesquisa: Métodos qualitativo, quantitativo e misto. 2. ed. Porto Alegre. 2007.

DALLABRIDA, Poliana. Vazamento de dados: Brasil "vê a banda passar" e não garante direito dos consumidores. Brasil de fato, 2021. Disponível em: https://www.brasildefato. com.br/2021/03/02/vazamento-de-dados-brasil-ve-a-banda-passar-e-nao-garante-direito-dos-consumidores#:~:text=A%20empresa%20de%20ciberseguran%C3% A7a%20PSafe,score% 20de%20cr%C3%A9dito%20dos%20cidad%C3%A3os. Acesso em: 09 abr. 2021.

DINIZ, Maria Helena. Curso de direito civil brasileiro: responsabilidade civil. Vol. 7. 17 ed. São Paulo: Saraiva, 2003.

FRAZÃO, Ana. Nova lgpd: as demais hipóteses de tratamento de dados pessoais. Jotainfo, 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018. Acesso em: 21 mar. 2021.

GUNTHER, Luiz Eduardo; COMAR, Rodrigo Thomazinho; RODRIGUES, Luciano Ehlke. A proteção e o tratamento dos dados pessoais sensíveis na era digital e o direito à privacidade: os limites da intervenção do Estado. Relações Internacionais no Mundo Atual, [S.l.], v. 2, n. 27, p. 25-41, nov. 2020. ISSN 2316-2880. Disponível em: http://revista.unicuritiba.edu.br/index.php/RIMA/article/view/3972/371372300. Acesso em: 23 mai. 2021.

GLOGOVCHAN, Carolina. Como é a Lei de Proteção de Dados Pessoais no Mundo? Sebrairespostas, 2020. Disponível em: https://respostas.sebrae.com.br/como-e-a-lei-de-protecao-de-dados-pessoais-no-mundo/. Acesso em: 25 mai. 2021.

MACHADO, Joana de Moraes Souza. A tutela da privacidade no controle de dados pessoais no direito brasileiro. In: Arquivo Jurídico, Teresina, v. 2, n. 2, jul./dez. 2015.

OLHAR DIGITAL. [EXCLUSIVO] Site da Nota Fiscal de Serviço Eletrônica vaza dados de mais de 60 municípios brasileiros. Olhar digital, 2019. Disponível em: https://olhardigital.com.br/2019/10/15/noticias/exclusivo-site-da-nota-fiscal-de-servico-eletronica-vaza-dados-de-mais-de-60-municipios-brasileiros/. Acesso em: 09 abr. 2021.

MAIA, Juliana de Souza Garcia Alves. Responsabilidade civil: pressupostos e excludentes. Âmbito jurídico, 2016. Disponível em: https://ambitojuridico.com.br/cadernos/direito-civil/responsabilidade-civil-pressupostos-e-excludentes/. Acesso em: 21 mai. 2021.

PAULA, Igor dos Santos de. LGPD não é um software e empresas precisarão correr para se adaptar. LGPD.com.br, 2020. Disponível em: https://www.lgpdbrasil.com.br/lgpd-nao-e-um-software-e-empresas-precisarao-correr-para-se-adaptar/. Acesso em: 09 abr. 2021.

PESTANA, Marcio. Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). Conjur, 2018. Disponível em: https://www.conjur.com.br/dl/ artigo-marcio-pestana-lgpd.pdf. Acesso em: 21 mai. 2021.

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

VENOSA, Sílvio de Salvo. Direito civil: responsabilidade civil. 7 ed. São Paulo: Atlas, 2007.

VENTURA, Ivan. A agenda de 2021 da LGPD. Revista Consumidor moderno, 2021. Disponível em: https://digital.consumidormoderno.com.br/a-agenda-de-2021-da-lgpd-ed261/#:~:text=O%20estudo%20%E2%80%9CCost%20of%20a,registrou%2026.523%20casos%20em%202019. Acesso em: 09 abr. 2021.

Recebido em: 12 de agosto de 2020
Avaliado em: 24 de agosto de 2020
Aceito em: 11 de dezembro de 2021

1 Bacharelando em Direito pela Faculdade de Ciências Humanas Exatas do Sertão do São Francisco (FACESF). E-mail: gustavoc.severiano@gmail.com

2 Graduado em Direito pela Faculdade de Alagoas; Pós-graduado em Direito Processual Civil pela Universidade do Sul de Santa Catarina; Especialista e Mestre em Psicanálise Aplicada a Educação e a Saúde pela UNIDERC/ANCHIETA; Mestre em Ciências da Educação pela Universidad de Desarrollo Sustentable; Advogado; Professor de Direito. E-mail: ferrazbar@hotmail.com