A RESPONSABILIDADE CIVIL EM DECORRÊNCIA DA VIOLAÇÃO AOS DADOS PESSOAIS NO AMBIENTE VIRTUAL

Lucas Haviner Costa Silva[1]
Pedro Henrique Batista França[2]
Tamires Sousa Oliveira[3]
Rafael Freire Ferreira[4]

RESUMO

O avanço da tecnologia no presente século é um fator revolucionário que dinamizou o ambiente social, sendo marcado pelo acesso instantâneo às informações e o tratamento automatizado dos dados, alterando a maneira de pensar dos indivíduos e também a sua forma de se relacionar. Nesse sentido, surgiu a problemática acerca de como assegurar os dados pessoais nos meios digitais. Em razão desta situação foi que se tornou necessário o estudo acerca da adoção de medidas de proteção e garantia de direitos no ambito digital. Com isso, o objetivo principal foi pautado na análise de como está ocorrendo o tratamento e a proteção das informações pessoais na web. Para isso, foi importante a realização de um substancial e ativo trabalho buscando informações acerca do cadastro dos dados junto as plataformas, analisando como estava acontecendo o compartilhamento destas informações, trazendo assim um demonstrativo de como a ausência de tratamento de dados pessoais trouxe impactos significativos nas liberdade civis e na violação dos direitos fundamentais. Com efeito, a realização deste artigo se valeu de uma metodologia pautada na pesquisa bibliográfica, tendo sido enriquecida com a doutrina, a legislação e o conhecimento de renomados autores que contribuiram acerca da temática.

Palavras-chave: Proteção de Dados, LGPD, Responsabilidade Civil

---

[1]Discente do curso de Direito da Faculdade UNEX de Itabuna/BA, e-mail: lucashaviner@gmail.com
[2]Discente do curso de Direito da Faculdade UNEX de Itabuna/BA, e-mail: pedrofranca1320@gmail.com
[3]Discente do curso de Direito da Faculdade UNEX de Itabuna/BA, e-mail: tamoliver708@gmail.com
[4]Docente Orientador da Faculdade UNEX de Itabuna/BA. Professor, Escritor e Advogado. Doutorando em Ciências jurídicas e Especialista em Direito Público material, e-mail: rafael.freire@ftc.edu.br

CIVIL LIABILITY RESULTING FROM VIOLATION OF PERSONAL DATA IN THE VIRTUAL ENVIRONMENT

ABSTRACT

The advancement of technology in this century is a revolutionary factor that has boosted the social environment, marked by instant access to information and automated data processing, changing the way individuals think and also their way of relating. In this sense, the problem arose regarding how to secure personal data in digital media. Due to this situation, it became necessary to study the adoption of measures to protect and guarantee rights in the digital environment. Therefore, the main objective was based on the analysis of how personal information is being processed and protected on the web. For this, it was important to carry out substantial and active work seeking information about the registration of data on the platforms, analyzing how this information was being shared, thus providing a demonstration of how the lack of processing of personal data brought significant impacts on civil liberties and the violation of fundamental rights. In fact, the creation of this article used a methodology based on bibliographical research, having been enriched with doctrine, legislation and the knowledge of renowned authors who contributed to the topic.

Keywords: Data Protection, LGPD, Civil Liability.

1 INTRODUÇÃO

O avanço da tecnologia vivenciado pela sociedade em escala mundial trouxe consigo uma nova forma de compreender a realidade, podendo-se afirmar que reduziu a distância entre as pessoas e permitiu que estes pudessem ter acesso a qualquer informação em tempo real e simultaneamente, sendo que, tudo isso só foi possível em razão da internet, que possibilitou uma gama de troca de informações entre os indivíduos de diferentes partes e locais do mundo. Com essa nova realidade e sua infinidade de possibilidades dentro do ambiente de navegação, foi necessária uma adaptação do sistema jurídico no sentido de garantir a proteção e a segurança no ambiente virtual em analogia com a vida real.

Com efeito, essa inovação tecnológica permitiu que diversas empresas de mercado de capital pudessem expandir seus produtos e serviços por meio de plataformas digitais seja de maneira gratuita ou condicionado através de um pagamento de determinado montante. Nesse sentido, muitos indivíduos se valiam da internet para comunicação e também para o comércio, insta salientar que a compra e venda é fator marcante e primordial de movimentação econômica na atualidade, sendo que, estas circunstâncias se davam por intermédio de plataformas digitais.

Com o imensurável aumento do uso da internet muitas pessoas deixavam passar despercebidos minuciosos detalhes, uma vez que, para se valer do uso destas plataformas era necessário proceder com a realização de um cadastro que se vale do fornecimento de informações particulares de cada indivíduo, como nome completo, RG, CPF, Data de Nascimento, sem contar o cruzamento de dados que era realizado entre as plataformas o que permitia a estas oferecer o produto adequado ao indivíduo com base em seu histórico de pesquisa.

Esse problema de compartilhamento de dados foi fator limitante para a implementação da Lei Geral de Proteção de Dados (13.709/2018) que tem como intuito justamente impor limites e condições acerca do tratamento dos dados pessoais no meio digital visando assim trazer segurança e proteção as pessoas que utilizam estas plataformas. Entretanto, mesmo com previsões legislativas vigentes muitos ainda insistem de forma errônea em se valer das informações pessoais dos indivíduos, chegando a utilizar delas até como moeda de valor, com o comércio ilegal de dados.

Por conseguinte, o problema identificado foi justamente a ausência de segurança no tratamento dos dados pessoais junto ao ambiente digital, circunstância esta que levou a análise de quais os meios que estão sendo utilizados para evitar esta situação. Com isso, a pesquisa junto às plataformas e o próprio ordenamento jurídico se mostram essenciais para que se possa ter uma noção de como é realizado o cadastro dos dados pessoais e se as plataformas estão de fato se valendo da observância a LGPD e os direitos fundamentais e assim buscar identificar as circunstâncias que estão permitindo o compartilhamento dos dados pessoais, visando assim trazer a tona quais os impactos que esta situação pode trazer para a liberdade civil e como pode implicar nos direitos fundamentais resguardados na Constituição Federal e na LGPD.

A delimitação desse tema tem por base os seguintes objetivos: o aumento da interação no mundo digital, a transmissão de informações e a ausência de segurança

dos dados pessoais no ambiente virtual. Com isso, observando estas situações foi que se despertou o interesse por este conteúdo, mais especificamente como ocorre o tratamento dos dados pessoais nas plataformas digitais e por que muitas dessas informações são compartilhadas ou até vazadas a terceiros. Cumpre ressaltar que, sendo a internet um meio de expansão e comunicação entre os diversos indivíduos em várias partes do mundo, este também tem por obrigação proporcionar melhores condições de proteção e qualidade de funcionalidade para seus usuários, levando em consideração a segurança e o bem-estar de cada um deles.

A metodologia a ser utilizada está pautada na pesquisa bibliográfica, com ênfase na leitura de livros, artigos científicos, legislação e demais conteúdos que tratem acerca da relação do indivíduo com as plataformas digitais e como está sendo realizada a segurança desses dados e quais as possíveis soluções para o compartilhamento e a evasão dessas informações.

2 RESPONSABILIDADE CIVIL E A PROTEÇÃO DE DADOS PESSOAIS

2.1 Histórico da LGPD

Embora a proteção de dados e privacidade seja agasalhada em diversos diplomas de ordenamento jurídico pátrio, como a Constituição Federal (art. 5º, X e LXXII), o Código Civil, o Código de Defesa do Consumidor, a Lei n. 12.527/2011 (Lei de A cesso à Informação) ou a Lei nº 12.965/2014 (Marco Civil da Internet), era imprescindível a regulação transversal, através de lei própria, do tratamento de dados pessoais.

Segundo Ferreira (2023, p. 193) [1] “Após a exposição dos dispositivos legais percebe-se que a autodeterminação informativa, no Brasil, carece de regulamentação, a privacidade está atrofiada na sociedade da informação e na intimidade comprometida [...]”

A Lei Geral de Proteção de Dados, Lei nº13.709/2018, é a legislação brasileira que regula as atividades de tratamento de dados pessoais, sancionada em agosto de 2018 passou a entrar em vigor a partir de 18 de setembro de 2020, visando tratar e proteger os dados pessoais.

Possuindo uma função dupla a LGPD tem como proposito fomentar o

[1] FERREIRA, Rafael Freire. **Autodeterminação informativa e a privacidade na sociedade da informação**. Rio de Janeiro: Lumen Juris, 2023.

desenvolvimento econômico e tecnológico; e, proteger direitos e liberdades fundamentais. A Lei se aplica a qualquer operação de tratamento de dados pessoais realizada tanto por pessoa natural quanto por pessoa jurídica (independente do porte da empresa); seja realizada em território brasileiro, ou com dados coletados no território nacional, mas também àquelas que oferecem serviços ao mercado consumidor brasileiro ou coletam e tratam dados de pessoas localizadas no país.

A implementação da LGPD e a proteção de dados já compõem realidades locais e globais, proteção e oportunidades únicas para que construam relações de confiança ainda mais fortes com clientes, fornecedores, terceiros e a sociedade em geral.

A transparência, como um princípio básico do Direito, tornou-se ainda mais crucial para as organizações que lidam com os dados pessoais dos seus clientes, fornecedores e colaboradores. Nesta nova era tecnológica, o que parecia ser trivial deve ser encarado com cuidado, igualmente por todos os setores.

Em última análise, a percepção dos dados pessoais como um ativo de valor intangível ganhou dimensão e forma.

2.2 Responsabilidade civil na LGPD

A revolução digital do século XXI trouxe consigo inúmeras oportunidades e desafios, com a proteção de dados pessoais emergindo como uma questão de extrema importância em um mundo cada vez mais interconectado. Nesse cenário, a Lei Geral de Proteção de Dados (LGPD), entrou em vigor no Brasil em setembro de 2020, representa um marco regulatório fundamental na proteção da privacidade e dos direitos dos indivíduos no ambiente digital.

A LGPD estabelece diretrizes claras para a coleta, processamento e armazenamento de dados pessoais, visando garantir que as informações sensíveis dos cidadãos sejam tratadas com o devido respeito e segurança. No entanto, a complexidade do ambiente digital e a constante evolução tecnológica trazem desafios significativos quando se trata de cumprir com os requisitos da LGPD.

Um dos aspectos mais cruciais da LGPD é a questão da responsabilidade civil. A lei prevê a responsabilidade das organizações que lidam com dados pessoais, estabelecendo que elas devem tomar medidas adequadas para proteger a

privacidade e segurança desses dados. Isso significa que, em caso de violação da LGPD, as organizações podem ser responsabilizadas e sujeitas a sanções.

Este Artigo tem como objetivo a responsabilidade civil estabelecida pela LGPD, abordando acerca dos desafios e implicações legais enfrentados por organizações que lidam com dados pessoais, bem como os direitos e recursos disponíveis para os indivíduos afetados. Além disso, buscou identificar as melhores práticas para garantir a conformidade com a LGPD e minimizar o risco de violações, contribuindo para um ambiente digital mais seguro e confiável.

A responsabilidade civil está regulamentada na Seção III do Capítulo VI da LGPD, intitulada de “Da Responsabilidade e do Ressarcimento de Danos”.

É importante salientar que a LGPD representou um marco significativo na proteção de dados pessoais, sendo que, a sua compreensão em termos de aplicabilidade é de suma importância para empresas, instituições e indivíduos no Brasil para que possam prosseguir em inteira harmonia. Neste contexto, este trabalho visa contribuir para uma compreensão mais aprofundada da responsabilidade civil na LGPD, promovendo assim a conscientização sobre a importância da proteção de dados pessoais no ambiente digital em constante evolução.

2.3 Confidencialidade dos dados do ser humano

A proteção de dados pessoais e a Lei Geral de Proteção de Dados (“LGPD”) são assuntos que afetam a população de maneira geral.

No cotidiano, por vezes, é normal a inserção de informações em diversos sites sem no entanto, haver por parte do usuário uma preocupação no que diz respeito ao destino final de seus dados. Nesse sentido, é preciso considerar que algumas farmácias utilizam esses para desenvolver um mapeamento das doenças e vender para planos de saúde, por sua vez algumas empresas se valem destas informações para exercer a precificação dinâmica, ou seja, ofertando o produto que mais condiz com as caracterísitcas do usuário. Para além disso, foi criada indústrias de venda de *mailing* de clientes, em que, vários dados podem constar nessas listas, nesse tipo de situação até mesmo o wi-fi público grátis não tem nada de grátis, o que ocorre é a troca de internet por dados pessoais utilizados para finalidades bem diversas à de entregar acesso à internet.

Chega a ser um fato cômico a perseguição da publicidade, há que considerar que posterior a uma rápida pesquisa de um determinado item, logo em seguida ao entrar em qualquer plataforma é enviada várias publicidades e propagandas simultaneamente, seduzindo e perseguindo até ceder e realizar a compra de determinado produto.

Os dados pessoais é um reflexo da individualidade, ajuda a identificar e tem o poder de influenciar as nossas decisões e até minar a democracia, são extremamente importantes e essenciais, porque refletem o conhecimento da empresa sobre aquele determinado cliente. Assim, pode-se interpretar quanto mais conhecimento uma empresa possui, maior ela cresce, mais vendas ela realiza e mais lucrativa ela se torna.

A LGPD visa estabelecer as normas para que os controladores possam manter os dados como sua matéria prima principal, sendo essencial a proteção dos direitos dos proprietários. Isso promove confiança, eficiência e transparência no tratamento dos dados.

2.4 As redes sociais e a evasão dos dados pessoais em decorrência de uma segurança precária

Nas redes sociais, é normal compartilharmos todo os tipos de informações, porém devemos manter as informações sensíveis o mais longe de estranhos. Antes de se registrar nas redes sociais, devemos considerar que tipo de conteúdo vamos compartilhar dentro delas e relevar se elas não vão conter dados importantes do usuário.

É mais que notório que mais da metade da população do planeta tem acesso a rede de internet, dentre estes se considera que 98% façam o uso de redes sociais e afins, seja para se comunicar com os amigos ou parentes ou simplesmente para fazer a postagens de conteúdos e compartilhar vídeos e fotos de seu interesse. As redes sociais se tornou o meio de comunicação mais bem cotado no mundo, haja vista que, tem como funcionalidade específica aproxima aqueles que se encontram distantes e facilitar a divulgação de diversos tipos de conteúdos.

Não obstante a realidade das redes sociais há aqueles que se valem desta para a prática de atos ilegais, que seja a venda de dados, a invasão de privacidade, o compartilhamento de dados sigilosos e a prática de crimes contra a honra. Em que

pese estas práticas ilícitas, a mais freqüente é a evasão e venda de dados, a qual é sabido que viola totalmente a privacidade do indivíduo. Apesar de todos esses dados serem comercializados legalmente, uma vez que o usuário “aceita” a política de utilização do site ou da rede social, existe outro mercado que comercializa estes dados ilicitamente. No mesmo sentido Marcelino (2011) discorre que:

> As práticas de venda desses dados são ilegais, pois viola a privacidade do consumidor, o Artigo 5º da Constituição assegura a inviolabilidade da vida privada e da intimidade do cidadão, permitindo ao indivíduo que foi vítima desse abuso, o direto à indenização. Apesar dessa segurança garantida em lei, a privacidade é exposta de qualquer maneira, seja por livre e espontânea vontade ou não (MARCELINO, 2011) [2].

Um caso muito interessante sobre a questão da evasão dos dados pessoais aconteceu em 2014, haja vista que, foi um fato que naquele momento teve grande repercussão, tendo em vista que, foi praticado por uma grande corporação. Naquela ocasião a empresa de telefonia Oi, teve uma multa no percentual de R$ 3,5 milhões de reais por conta de uma constatação de violação ao direito à privacidade.

A situação que acarretou para com esta penalidade teve origem em investigações por parte do Departamento de Proteção e Defesa do Consumidor (DPDC), sobre a parceria entre a Oi e a empresa britânica Phorm, restou constatado o desenvolvimento do Software Navegador Oi Velox feria o princípio básico da privacidade, na medida que, tinha por função mapear o tráfego de dados do consumidor, com o objetivo de compor um perfil de navegação do usuário.

O vazamento de dados é uma realidade tão cotidiana que no ano de 2021 aconteceu mais uma cena que deixou o mundo digital estagnado, frente à notícia do vazamento de dados de e-mail e números de telefone de cerca de 533 milhões de contas vinculadas ao facebook em um fórum de hackers. A reportagem foi trazida a conhecimento por intermédio da revista “Business Insider”. Com efeito, este não foi o único escândalo envolvendo a empresa. No ano de 2018, uma situação semelhante ocorreu, sendo que, na época a empresa britânica Cambridge Analytica, capturou os dados pessoais de milhões de usuários do Facebook para propagandas políticas.

A precariedade e a ineficiência são nítidas sendo por tanto necessária a adoção de medidas que visem reparar estes danos. Com isso, é Importante salientar que nas redes sociais já existem mecanismos que dificultam que invasores possam ter acessos a informações pessoais dos usuários.

---

[2] MARCELINO, Caroline. **Empresas vendem dados do consumidor na internet.** São Paulo: AASP, 2011.

Um destes métodos é o controle de acesso a informações pessoais, em que, conforme estabelce Marteleto (2018):

> Apenas pessoas que estão conectadas podem tem acesso às informações que compartilhamos no perfil, porém, a rede social permite separar em grupos tais como: família e colegas de trabalho e delimitar o acesso a determinado tipo de informação para cada um deles, dando mais controle ao dono do perfil (MARTELETO, 2018)[3].

Outra forma é a privacidade do perfil que se manifesta atráves de HAMADA (2019) no seguinte entendimento:

> As rede sociais possuem "configurações de privacidade", onde podemos definir quem pode acessar determinado tipo de conteúdo tais como: fotos, posts, vídeos e etc. Assim podemos evitar que pessoas indesejadas tenham acesso a esse conteúdo (HAMADA; NASSIF, 2019)[4].

Com efeito, existem diversos outros métodos que podem ser utilizados para evitar ou dificultar que os dados do indivíduo sejam vazados, como por exemplo: Evitar compartilhar informações sigilosas nos chats de bate papo, Não clicar em links suspeitos e desativar redes sociais que não utilizar cotidianamente. Sobre esta circunstância MARTELETO (2018) afirma que:

> Com a grande quantidade de ataques as redes sociais, o seu uso pode parecer perigoso. Porém se algumas dicas e boas práticas forem empregadas, é possível se proteger e evitar esse tipo de incidente ocorra durante o usos dessas plataformas (MARTELETO, 2018)[4].

Pelo que foi analisado resta claro que os dados pessoais não se encontram seguros juntos as redes sociais, haja vista que, a todo o momento milhares de pessoais podem está sendo vítimas da evasão de seus dados particulares. Entretanto, conforme se observou existem maneiras de dificultar ou evitar que indivíduos de caráter malicioso tenham acesso a estes dados, sendo que, podendo-se seguir estes métodos é possível tentar esquivar-se de uma possível evasão de dados.

2.5 Proteção e segurança: Como o ambiente virtual pode trabalhar gerando confiança e garantindo direitos aos seus usuários

O advento da tecnologia trouxe consigo diversos avanços significativos, contudo, em meio a este progresso novos desafios surgiram em relação à segurança da

---

[3] MARTELETO, Regina Maria. **REDES SOCIAIS, MEDIAÇÃO E APROPRIAÇÃO DE 20 INFORMAÇÕES: situando campos, objetos e conceitos na pesquisa em Ciência da Informação.** São Paulo: BRAPCI, 2010.

[4] HAMADA, Hélio Hiroshi; , Lilian Noronha Nassif. **PERSPECTIVAS DA SEGURANÇA PÚBLICA NO CONTEXTO DE SMART CITIES: desafios e oportunidades para as organizações policiais**. Minas Gerais: Revista UEMG, 2018.

informação. Importante pontuar que o aumento da conectividade e a dependência cada vez maior das pessoas aos dispositivos e sistemas digitais, fez com que a proteção de dados e informações se tornasse um assunto essencial.

Com essa nova realidade se fez necessário o desenvolvimento de um pensamento estratégico voltado à área da segurança da informação, sendo que, se fez essencial neste momento desenvolver práticas, políticas e tecnologias que tivessem como intuito a proteção dos dados dos usuários contra ameaças de hackers, malware e violações de privacidade, buscando também ceifar qualquer tipo de evasão de informações por parte dos provedores de dados.

Com esta intenção e visando proteger as informações daqueles que se valem da utilização da rede de internet, foram desenvolvidos os seguintes mecanismos:

A **Criptografia** que se refere ao processo matemático de tornar uma mensagem impossível de ser lida, é um conjunto de regras que visa fazer a codificação da informação onde apenas o emissor e o receptor consigam ter acesso a elas (Surveillance Self-Defense, 2018)[5];

A **Autenticação** diz respeito à confirmação da identidade dos usuários, sendo por tanto um processo que emprega a utilização de senhas seguras e uso de biometria, ou seja, utiliza-se do método de autenticação de dois fatores (2FA), objetivando assim que apenas usuários legítimos acessem suas contas e informações pessoais.

As **Políticas de Privacidade** são exigências que empresas e organizações têm de adotar no desenvolvimento de suas atividades, sendo utilizadas como uma forma de anuência pela qual o usuário concorda para com a utilização dos seus dados baseado na ideia de coleta, utilização, transparência e proteção.

A **Legislação e suas Regulamentações** são mecanismos criados por meio de legisladores com força de lei que tem como intuito coibir atitudes que violem a segurança dos dados pessoais dos usuários que utilizam de sites ou aplicativos, visando assim garantir a segurança e a privacidade no ambiente digital.

---

[5] SURVEILLANCE SELF-DEFENSE. **O que eu deveria saber sobre criptografia?.** São Paulo: SSD.EFF.ORG, 2019.

Considerando estes mecanismos adotados e a dinamicidade do direito, é essencial sempre prezar pela proteção a dignidade da pessoa humana, a sua privacidade e principalmente a sua intimidade, há que pontuar que a Carta Magna preconiza no art. 5º, inciso X, acerca desta temática e estampa o seguinte: "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;" (BRASIL, 1988)

Neste entendimento lapidado pela Constituição Federal há que se levar em consideração a privacidade do indivíduo a qual segundo Marques (2008)[6] é dívida em três níveis, com decrescente intensidade de proteção, sendo que, o direito à privacidade em suas palavras é tido como aquilo que preserva o indivíduo do conhecimento alheio, reservando este a sua própria realidade e vivência.

Em suma, pode-se considerar que a proteção dos dados pessoais dentro do âmbito virtual vem a cada dia evoluindo e garantido de maneira incisiva a segurança do usuário. Com efeito, contrário a isso, a evasão de dados ainda é muito frequente e o desenvolvimento de mecanismos maliciosos só vem aumentado, fato este que acaba por gerar nos indivíduos receio quanto ao compartilhamento de seus dados. Com isso, conclui-se que é a manipulação de dados é um complexo desafio e precisa por tanto de investimentos mais eficazes que permitam combater o vazamento de dados em massa, os cybers crimes e os hackers, fortalecendo assim a tecnologia e gerando um ambiente virtual ordeiro e de boa qualidade, que permita o acesso mútuo a seus usuários sem preocupações ou qualquer tipo de risco a sua privacidade.

2.6 Critérios para a definição do *quantum* indenizatório

A Lei Geral de Proteção de Dados (LGPD) não especifica critérios detalhados para a definição do quantum indenizatório em casos de violação de dados pessoais. No entanto, a LGPD estabelece princípios gerais que podem ser usados como referência para determinar a extensão das indenizações em casos de violação de dados pessoais. Aqui estão alguns critérios e princípios que podem ser relevantes:

Dano Moral: O quantum indenizatório deve levar em consideração o dano

[6] MARQUES, E., Scalon, C., Oliveira, M. **Comparando estruturas sociais no Rio de Janeiro e São Paulo**. Rio de Janeiro: Revista Dados, 2008.

moral sofrido pela vítima da violação de dados pessoais. Isso inclui aspectos como a gravidade da violação, a sensibilidade dos dados vazados e o impacto sobre a vida do titular dos dados.

Natureza da Violação: A gravidade da violação desempenha um papel importante na determinação da indenização. Violações mais sérias, que resultem em danos substanciais, geralmente resultarão em indenizações mais altas.

Negligência ou Intencionalidade: Se a violação de dados pessoais resultar de negligência grave ou de ações intencionais por parte da empresa ou organização responsável, isso pode aumentar o valor da indenização.

Perdas Financeiras: Caso a violação de dados pessoais tenha causado perdas financeiras diretas para o titular dos dados, essas perdas também devem ser consideradas no cálculo da indenização.

Gravidade da Violação: A LGPD prevê que a Autoridade Nacional de Proteção de Dados (ANPD) pode aplicar sanções administrativas às empresas que violarem a lei. Essas sanções podem incluir multas significativas, que também podem ser consideradas ao determinar o quantum indenizatório.

Consentimento: A LGPD exige que as empresas obtenham o consentimento dos titulares de dados para o processamento de suas informações pessoais. Se a violação ocorreu sem o consentimento adequado, isso pode ser um fator relevante na determinação da indenização.

Vale-se se ressaltar que o art. 944 da Código civil também discorre que “a indenização se mede pela extensão do dano”, neste sentido CAPANEMA[7], 2020, p. 163 discorre que:

a) a quantidade de dados pessoais afetados;

b) a natureza dos dados pessoais afetados: o vazamento de dados pessoais sensíveis, por exemplo, determinará uma indenização maior, especialmente se se tratar de dados biométricos, que não podem ser substituídos;

c) a reincidência da conduta;

d) a omissão em tomar medidas de segurança e técnicas para minorar o dano ou em colaborar com a Autoridade Nacional de Proteção de Dados;

e) a ausência de notificação dos usuários da ocorrência do incidente;

f) a comprovada utilização dos dados vazados de titulares por terceiros;

---

[7] CAPANEMA, Walter Aranha. **A responsabilidade civil na Lei Geral de Proteção de Dados**. São Paulo: Cadernos Jurídicos, 2020.

Outro ponto a ser discorrido, é no tocante a responsabilização solidária pelo operador e pelo controlador dos dados pessoais, o art. 42 da LGPD prevê que:

§ 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. Logo é possível se verificar tanto ambos têm responsabilidade mútua para realizar a gestão destas informações, de modo a garantir a total privacidade destes dados

É importante lembrar que, em muitos casos, a LGPD prevê que o titular dos dados pode buscar uma ação judicial para buscar indenização por danos materiais e morais em caso de violação. Os tribunais brasileiros têm a autoridade para considerar todos esses critérios ao determinar a indenização em um caso específico.

3 CONSIDERAÇÕES FINAIS

Em decorrência dos fatos ora mencionados, o presente trabalho teve por finalidade tratar sobre o estudo da responsabilidade civil das plataformas digitais em razão do grande número de evasão de dados de seus usuários, objetivando assim, fazer uma análise em concorrência com os direitos e garantias já conquistados pela sociedade frente a era digital, trazendo à tona dispositivos da Constituição Federal, da Lei Geral de Proteção de Dados, dentre outras doutrinas e fundamentação de teóricos que abordaram acerca do tema, considerando as ameaças existentes no ambiente virtual e os sérios riscos que estas podem trazer ao indivíduo quando invadem os seus dados pessoais.

Nesse contexto, foi possível observar a importância da responsabilidade civil no tocante há como pode ser assegurado a proteção e responsabilização dos dados sensíveis dos usuários na internet. Neste enredo, constatou-se que a LGPD trouxe consigo uma proteção e regulamentação acerca do tratamento dos dados sensíveis. Em que pese esta regulamentação, há que salientar a inobservância de muitos sites

e aplicativos, sem contar que alguns agentes maliciosos desenvolvem sistemas já na intenção de captar os dados das pessoas. Com isso, a partir da aplicação da Lei foi possível ter uma maior facilidade na identificação destes indivíduos e assim então foi ´possível responsabilizá-los pelas práticas dos atos.

Há que ponderar que a Responsabilidade Civil é tratada na LGPD e vem cumulada justamente com a responsabilização e o ressarcimento de danos. Sendo que, em termos gerais esta Lei é tida como um marco de muita relevância para o ambiente digital. Não obstante a esta circunstância é necessário frisar que o referido dispositivo vem sendo empregado no ambiente digital de maneira geral, sendo que, muitos casos de evasão de dados e crimes cibernéticos, só foram possíveis de punir graças a esta lei, contudo, assim como a legislação vem se aperfeiçoado, os criminosos e hackers também estão buscando cada dia mais criar mecanismos que fujam da visão do fiscal ou que apenas passem despercebidos. Com isso, é notório a necessidade de investimento nessa área, para que mais pessoas possam ser responsabilizadas pelas suas atitudes errôneas.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Constituição da República Federativa do Brasil**, de 05 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 28 out. de 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 27 out. 2023.

BRASIL. **Lei nº 12.965, de 23 abril de 2014. Marco Civil da Internet**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 25 out. 2023.

CAPANEMA, Walter Aranha. **A responsabilidade civil na Lei Geral de Proteção de Dados**. Cadernos Jurídicos: Direito Digital e proteção de dados pessoais, ano, v. 21, p. 163-170, 2020.

DE PAULA MAIMONE, Flávio Henrique Caetano. **Responsabilidade Civil na LGPD**. Editora Foco, 2021.

DUQUE, Waleska Estrada Vieira. **A privacidade no ambiente cibernético: Direito fundamental do usuário**. Revista da Esmec, Santa Catarina, v.24, n.30, p. 197-217 , 2017. DOI: https://doi.org/10.14295/revistadaesmesc.v24i30.p197. Disponível em: https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Rev-ESMESC_30.09.pdf. Acesso em: 30

out. 2023.

FERREIRA, Rafael Freire. **Autodeterminação informativa e a privacidade na sociedade da informação**: atualizado com a Lei no 14.460, de 2022 e a Lei no 13.853, de 2019/ Rafael Freire Ferreira. - 5. ed. - Rio de Janeiro : Lumen Juris, 2023.

GODINHO, Adriano Marteleto; NETO, Genésio Rodrigues Queiroga; TOLÊDO, Rita Cássia Morais. **A responsabilidade civil pela violação a dados pessoais**. Revista IBERC, v. 3, n. 1, 2020.

HAMADA, Hélio Hiroshi; , Lilian Noronha Nassif. **PERSPECTIVAS DA SEGURANÇA PÚBLICA NO CONTEXTO DE SMART CITIES: desafios e oportunidades para as organizações policiais**. Perspectiva em Políticas Públicas, Belo Horizonte, v. 11, n. 22, p. 189-213, jul./dez. 2018. Disponível em: . Acesso em: 25 out.. 2023.

MARCELINO, Carolina. **Empresas vendem dados do consumidor na internet**: Basta o cliente preencher um cadastro em uma loja para que suas informações sejam repassadas para outras empresas sem autorização. A prática viola a privacidade e abre espaço para indenização caso a pessoa se sinta lesada. 2011. Disponível em: <http://www.estadao.com.br/blogs/jt-seu-bolso/2011/02/05/empresas-vendem-dados-do-consumidor-na-internet/>. Acesso em: 25 out. 2023

MARTELETO, Regina Maria. **REDES SOCIAIS, MEDIAÇÃO E APROPRIAÇÃO DE 20 INFORMAÇÕES: situando campos, objetos e conceitos na pesquisa em Ciência da Informação.** BRAPCI - Base de Dados em Ciência da Informação, Rio de Janeiro, v. 3, n. 1, p. 27-46, jan./dez. 2010. Disponível em: . Acesso em: 22 out. 2023.

MULTHOLLAND, Caitlin. **Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018)**. 2021. 19 f. Tese (Doutorado em Direito Civil) - Departamento de Direito da PUC Rio de Janeiro, 2021. Disponível em: https://www.jur.puc-rio.br/wp content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em: 29 out. 2023.

SURVEILLANCE SELF-DEFENSE. **O que eu deveria saber sobre criptografia?**. Disponível em: https://ssd.eff.org/pt-br/module/o-que-%C3%A9-criptografia. Acesso em: 15 mai. 2019.