doi.org/10.51891/rease.v8i5.6048

A RESPONSABILIDADE CIVIL PELO VAZAMENTO DIGITAL DE DADOS SOB A ÓTICA DO DIREITO BRASILEIRO

CIVIL RESPONSIBILITY FOR DIGITAL DATA LEAKAGE UNDER BRAZILIAN LAW

Kenny Maiana Silva Novais de Souza[1]
Gabriel Octacílio Bohn Edler[2]

RESUMO: A proteção de dados é um direito fundamental previsto na Emenda Constitucional nº 115, de 2022, assim o presente trabalho tem por objetivo analisar como a responsabilidade civil pode ser aplicada nos casos em que há sequestro de dados pessoais de usuários virtuais no ordenamento jurídico brasileiro. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) trata a atuação dos agentes no tratamento de dados para que seja possível enfrentar os problemas causados pela exploração das novas tecnologias. Foi utilizado para a exploração da temática, a legislação vigente, de modo a complementar o que está estabelecido na LGPD, além de fazer uso de doutrina que versa sobre a responsabilidade civil e a LGPD. Utilizou-se como fonte de pesquisa: doutrina, legislações, artigos científicos e revistas eletrônicas. Com a presente pesquisa, portanto, pode-se concluir que a LGPD é um avanço para a sociedade brasileira, no entanto para sua efetivação deverá ser desenvolvida uma cultura de proteção de dados por toda a população, pois todos deverão compreender seus direitos e preservar os seus dados.

Palavras-Chave: Proteção de Dados. LGPD. Responsabilidade Civil.

ABSTRACT: Data protection is a fundamental right provided by the Constitutional Amendment nº 115, of 2022. The present work aims to analyze how civil liability can be applied in cases where there is kidnapping of personal data of virtual users in the Brazilian legal system. The General Data Protection Law (Law No. 13,709/2018) deals with the performance of agents in data processing so that it is possible to face the problems caused by the exploitation of new technologies. The current legislation was used for the exploration of the theme, in order to complement what is established in the LGPD (Brazilian General Personal Data Protection Law), in addition to making use of doctrine that deals with civil liability and the LGPD. Doctrine, legislation, scientific articles and electronic journals were used as a source of research. With the present research, it can be concluded that the LGPD is an advance for Brazilian society, however, for its effectiveness, a culture of data protection must be developed by the entire population, as everyone must understand their rights and preserve their data.

Keywords: Data Protection. GDPL. Civil responsibility.

1 INTRODUÇÃO

A informação tecnológica integrou-se de maneira desenfreada na sociedade, e a característica mais marcante está sedimentada na possibilidade do registro de praticamente todos os atos da vida cotidiana, principalmente dos dados pessoais; porém esses dados e as interferências por eles geradas, ainda são "quase" desconhecidas. Como bem pontuou Frazão

[1] Discente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior de Ilhéus, Bahia. E-mail: novaiskenny@gmail.com.
[2]Docente do Curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior de Ilhéus, Bahia.E-mail: gabriel.edler@faculdadedeilheus.com.br.

(2019, s/p.), os dados ganharam uma importância transversal, tornando-se vetores das vias e das liberdades virtuais, assim como da sociedade e da própria democracia. Entende-se, deste modo, que a sociedade vive o que aponta-se por *data-driven economy,* ou seja, uma economia movida a dados.

A rede é alimentada através dos dados, que os próprios usuários fornecem; dados estes, que são propagados em fração de segundos, por meio da inteligência aplicada, tornando ainda mais vulneráveis as violações de dados pessoais dos indivíduos. A coleta de dados na internet, geralmente, acontece quando o indivíduo está na qualidade de consumidor, ou seja, quando o mesmo realiza algum cadastro, adquire e/ou utiliza dos serviços prestados pelas plataformas digitais.

Ressalte-se que, para aquisição ou acesso a páginas eletrônicas e produtos, é necessário o fornecimento de dados pessoais, que gera um elemento caracterizador do contrato firmado entre as partes. No entanto, todo esse avanço tecnológico e a propagação de dados já mostrou um lado negativo, o qual expõe a intimidade e a capacidade de escolha dos usuários aos interesses das grandes corporações.

Por tanto, essa vulnerabilidade de dados tornou-se pauta de discussão nos quesitos sobre a necessidade de proteção e regulamentação, assim como, a imposição de limites, pois tal fato infringe o direito à privacidade, que é um direito fundamental. Frisa-se que a legislação, até pouco tempo atrás, não delimitava de maneira clara quais os princípios e regras que deveriam ser aplicados, em casos de vazamento de dados, bem como, de qual maneira a proteção poderia ser materializada. Houve, portanto, a necessidade de regulamentação da proteção, e assim foi sancionada a Lei Geral de Proteção de Dados (Lei nº 13.709 de 2018).

A lei supramencionada fora sancionada com o objetivo de regulamentar as relações estabelecidas entre o titular dos dados e os controladores das páginas, de modo a instituir um órgão administrativo para regulamentar e fiscalizar a questão, além de uma positivação clara das atribuições, regras e punições cabíveis para o descumprimento do bom uso e sigilo das informações coletadas nas atividades com fins econômicos. Sendo assim, é de fundamental importância o mecanismo de reparação civil insculpido na lei, que estabelece os encargos que permitem identificar os responsáveis pela proteção das informações dos titulares.

Será, portanto, o objetivo geral deste estudo, analisar como a responsabilidade civil pode ser aplicada nos casos em que há sequestro de dados pessoais de usuários virtuais no ordenamento jurídico brasileiro, a fim de que o sistema sóciojurídico, e político não entrem em colapso. Sendo assim, é de suma importância que seja feita uma interpretação acerca da natureza jurídica e limites da responsabilidade civil na referida lei, a partir da confrontação entre a lei específica sobre proteção de dados e as normas gerais sobre responsabilidade civil presentes no Código Civil, Código de Defesa do Consumidor e na Constituição Federal.

Considerando que o descumprimento a direitos de outrem podem trazer danos que ensejam a reparação, é pacífico que a responsabilidade civil é um dos principais aspectos da lei objeto deste estudo. O tema ainda será explorado, a partir da identificação dos conceitos fundamentais, dos princípios, dos agentes e de suas atribuições contidos na Lei Geral de Proteção de Dados; além da verificação da legislação nacional acerca da responsabilidade civil e da proteção de dados; e da análise aos limites e especificidades para reparação dos danos gerados pelos agentes de proteção de dados.

Para discorrer o tema proposto será realizada uma pesquisa bibliográfica em livros, dissertações, artigos científicos, textos informativos veiculados na internet, leis e jurisprudências.

2 BREVE HISTÓRICO SOBRE O DIREITO À PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS

A Constituição Federal de 88 trata em seu artigo 5° dos direitos e garantias fundamentais, ou seja, garante a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade. Além disso, em seu inciso X, trata como sendo invioláveis: a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988). Portanto, a CF/88 tutela à pessoa natural, titular dos dados, o direito de usá-los e instrumentalizá-los como seus.

A CF/88 é clara ao elencar o direito à privacidade, como um direito fundamental, porém para compreender de forma coesa e objetiva como foi dado o surgimento ao direito de privacidade, deve-se analisá-lo dentro do contexto histórico conforme foram surgindo os avanços da tecnologia.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantidos aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X – São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XI – a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial; XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Brasil,1988)

Pode-se considerar que o direito à privacidade teve seu início em 1824, momento em que na Constituição daquele ano estava sendo proposto o "segredo da carta" e a "inviolabilidade da casa". Tratando-se em outras palavras, seria um direito de privacidade principiante, que se encontrava em construção. Já pela doutrina, considera-se que o direito à privacidade teve início em 1890 com a publicação do artigo The Right to Privacy, dos juristas norte-americanos, Brandeis e Warren (DONEDA, 2020). Contudo, o conceito de privacidade evoluiu de forma substancial.

Com a evolução social e, consequentemente tecnológica, as pessoas passaram a ter interesse em expor a própria vida, o que acabou provocando uma onda de fofocas sensacionalistas mundial. Em decorrência desses, entre outros fatos, houve a necessidade de se pensar sobre direitos da privacidade mais amplos. Entendeu-se, a partir de então, que o direito privado não envolvia apenas os meios físicos, como confidencialidade ou violação da carta residencial.

Warren, (1890, p.293) levantou o questionamento de quando começa e termina a lei para garantia aos indivíduos que desejam transmitir sua mensagem, seus pensamentos, sentimentos e emoções aos outros. Observamos que naquela época, o direito à privacidade era visto apenas como uma prerrogativa de ser deixado em paz ou ser "largado" só; longe da curiosidade alheia. Contudo, o direito à privacidade consagrou-se como um direito fundamental, através da Declaração Universal dos Direitos Humanos, no ano de 1948, conforme mencionado no Artigo 12, sendo válido até os dias atuais:

> Ninguém sofrerá intromissões arbitrários ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Toda a pessoa tem direitos à proteção da lei contra tais intromissões ou ataques. (DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, 1948, p.3).

Diante do exposto, constatou-se que a privacidade não seria mais passível de tolerância, assumindo um conceito mais amplo, e que estabeleceu limites, para quem poderia acessar dados sem devida autorização, tornando-se necessária, no ordenamento jurídico, a criação de modernas legislações que visariam dar maior proteção ao tema.

2.1 Proteção de Dados Pessoais

A proteção de dados é um meio de garantia, para que os dados sejam utilizados apenas quando aprovado previamente pelo titular. O termo propriamente dito está relacionado com a definição de processos que padronizem os tratamentos de dados pessoais, evitando falhas e violações durante todo o ciclo de vida dos dados e em sua organização.

A proteção destes dados pessoais significa fornecer um manual de instruções, a fim de estipular as regras de como nossos dados pessoais podem ser manipulados; afinal, estamos sujeitos à vigilância (estatal e/ou privada), à coleta arbitrária e ilegal dos dados pessoais, bem como, à interceptação de comunicações.

A proteção dos dados pessoais é um direito fundamental resguardado pela própria Constituição Federal, e está envolvido diretamente a outros direitos, destacando-se, nesse contexto, o direito à privacidade e o direito à autodeterminação informativa, os quais, embora autônomos entre si, apresentam zonas de contato importantes.

Nesse contexto, pela relevância hodierna que deve ser destacada ao desenvolvimento do direito à proteção de dados pessoais, é interessante trazer à baila uma breve pincelada do contexto histórico a seguir.

Pode-se ousar atribuir à Alemanha a promulgação da primeira lei mundial de proteção de dados pessoais. Em 1980, foi criada uma comissão: a Organization for Economic Cooperation and Development (OCDE), tradução livre "Organização para a Cooperação e Desenvolvimento Econômico", que publicou algumas diretrizes que estabeleceram princípios básicos em relação à proteção de dados e sobre o fluxo de informações entre países. Porém, essas diretrizes eram interpretadas de forma ampla, e não possuíam força para estabelecer um padrão, o que acabou gerando diversos dispositivos legais em vários países. (OCDE, 2002, pag.2)

No ano seguinte, a Europa, através de uma comissão, ratificou a "Data Protection Convention" traduzido como "Convenção de Proteção de Dados", através do Tratado nº 108, que se tornou instrumento legal primário internacional destinado a proteger os indivíduos contra o uso indevido e a coleta de dados pessoais de forma abusiva. Essa convenção consagrou o direito ao indivíduo de saber quais informações eram armazenadas sobre si e se fosse o caso, o próprio indivíduo poderia fazer a correção de seus dados. (COE,1981, p.18).

A importância sobre a proteção de dados no Brasil começou a surgir nos anos 90, a exemplo, o Código de Defesa do Consumidor, instituído com a promulgação da Lei nº 8.078/90, que regulou o uso de banco de dados de consumidores. A lei consumerista prevê regras sobre o acesso a "informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre o próprio consumidor", entretanto, não possui consentimento para o recolhimento desses dados, foi reivindicado que o consumidor seja comunicado sobre a abertura do registro de seus dados.

E outras leis foram surgindo, como: a Lei de Interceptação Telefônica e Telemática, que caracteriza o direito à privacidade ao limitar o uso de tal recurso, a Lei do Habeas Data regulando o direito constitucional e o rito de acesso e correção de informações pessoais.

O Código Civil de 2002 trouxe pontos sobre a vida privada, através do direito da personalidade, e dispôs instrumentos para que a violação dos direitos da personalidade fosse controlada. Anos após, foi publicada a Lei nº 12.527/11, conhecida como Lei de Acesso à

Informação, que instituiu em seu Art. 4°, inciso IV e 6°, inciso III, o acesso à informação pessoal, *in verbis*:

> Art. 4º Para os efeitos desta Lei, considera-se: IV - Informação pessoal: aquela relacionada à pessoa natural identificada ou identificável; Art. 6º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a: III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Vale salientar que a Lei Carolina Dieckman, Lei n. 12.737/12, também contribuiu neste contexto, ao reconhecer como delito a invasão de privacidade, através de dispositivos eletrônicos e cibernéticos, introduzindo no Código Penal o disposto no Art. 154- A, §3°. Mediante a celeridade de novas legislações, em vários países do mundo, viu-se a necessidade de proteção das informações pessoais, afirma Fernandes (2019, p. 10).

Os dados pessoais mostraram-se, ainda mais vulneráveis em 2013, quando a então Presidente Dilma Rousseff, teve seus e-mails, telefonemas e mensagens de celular monitorados por agentes do governo dos Estados Unidos, segundo documentos da Agência de Segurança Nacional Americana (NSA). (EXAME, 2013). Após o ocorrido, naquele mesmo ano, a Presidente e seus assessores foram alvos da agência de espionagem norte-americana, assim o governo brasileiro imprimiu urgência para colocar em tramitação o Projeto de Lei nº. 2126/11, conhecido como Marco Civil da Internet, assunto que será tratado com mais afinco no próximo tópico.

2.2 Marco Civil da Internet

Para tratar do Marco Civil, torna-se relevante trazer ao contexto, a Lei de Cadastro Positivo (Lei n° 12414/2011), que foi sancionada em 10 de junho de 2011, a qual permite a saída do consumidor do banco de dados em qualquer tempo, limitando a divulgação dos dados somente para a entidade em que o consumidor realizou a adesão de crédito ou produto. (BESSA, 2011). Contudo, cabe salientar, que no texto original da referida lei, mais precisamente no §3º do art. 5º da Lei 12.414/2011 determinava que a autorização concedida a uma fonte ou a um gestor, ainda que para fornecimento de informações a um banco de dados específico, era aproveitada a todos os bancos de dados.

A Lei do Cadastro Positivo ampliou um leque de possibilidades em relação às informações dos dados pessoais, como a formação de bancos de dados, regras de proteção à privacidade e métodos de controle e fiscalização dessa atividade. Assim, no caso de bancos de dados virtuais e informatizados, aplica-se a Lei nº 12.414/2011 em conjunto com a Lei nº 12.965/2014.

Conforme mencionado anteriormente, começou a tramitar no Brasil o Projeto de Lei n. 2126/11, conhecido como Marco Civil da Internet. Em seu bojo, elenca e estabelece princípios, garantias, direitos e deveres dos usuários da rede. Insta ressaltar, que se trata de um texto que sofreu forte evolução em sua tramitação, pois servia claramente aos interesses de um determinado setor da sociedade, para um texto que valoriza a liberdade de acesso à rede e, na maioria das vezes, a defesa do consumidor.

Então, em 23 de abril de 2014 a Lei nº 12.965, conhecida como o Marco Civil da Internet, veio para estabelecer os princípios, as garantias, os direitos e os deveres para o uso da Internet no Brasil. Em seu Art. 3º, inciso I, assegura a garantia da liberdade de expressão, de comunicação e de manifestação de pensamento que são direitos fundamentais previstos no Art. 5º da

Constituição Federal de 1988. Os incisos II e III trazem a proteção da privacidade e a proteção dos dados pessoais (BRASIL, 2014). Já no Art. 7º assegura sobre os direitos e garantias dos usuários.

Com a desenfreada utilização e evolução tecnológica, a Lei nº 12.965/2014 (Marco Civil da Internet) foi de suma importância, para a definição dos direitos e dos deveres dos internautas, usuários da rede mundial de computadores, sejam eles consumidores ou não. Contudo, deve-se interpretá-la de acordo com os mandamentos e valores constitucionais vigentes de proteção e defesa do consumidor, no tocante aos princípios da dignidade da pessoa humana, da igualdade, da privacidade, da liberdade de expressão, da autodeterminação informativa, da proteção de dados e de registros pessoais, entre outros.

2.3 Violações de Dados que Ensejaram a LGPD

O usuário diante da tela, raramente preocupa-se com as condições e riscos que podem estar por trás das páginas, e muitas vezes informam seus dados pessoais como, CPF, endereço, telefone, Registro Geral (RG), entre outros, para finalizar transações e realizar cadastros. Segundo DONEDA (2011) "os dados pessoais chegam a fazer às vezes da própria pessoa, em uma série de circunstâncias, nas quais a sua presença física seria outrora indispensável".

Souza (2018) afirma que os dados são coletados, sempre que se realiza um cadastro em determinado site, ou em redes sociais, ou simplesmente por meio de cookies de navegação, e as informações passadas ficam em um banco de dados onde é montado um verdadeiro quebra-cabeças com as informações pessoais, criando assim uma forma de dossiê virtual sobre o indivíduo.

Insta informar que, os cookies permitem que informações de navegação criem memórias de curto prazo dos dados fornecidos, e com isso os sites ofereçam ao indivíduo uma melhor experiência de navegação. Contudo, os cookies também são comumente relacionados a casos de violação de privacidade na web, e existem aqueles que são utilizados para rastrear o comportamento do usuário em diversos sites da internet, para a criação de bancos de dados sobre o indivíduo. "Isso torna possível conhecer de uma maneira muito mais ampla o mercado, diminuir riscos e principalmente, delimitar segmentos específicos para lhes direcionar publicidade" (SCHMIDT, 2018, on-line).

Mas a questão que permeia os debates é até que ponto a utilização dos dados é autorizada, e se o compartilhamento destes foi, realmente, permitido, ressalte-se que o usuário não possui o hábito de ler as políticas de privacidade, apenas confirmando-as sem ter a ciência do que ali está escrito. Essas informações para as lojas online, por exemplo, são determinantes para que elas enviem propagandas e captem aquele indivíduo como um consumidor.

> [...] com as inúmeras possibilidades de processamento dos dados pessoais pelos meios automatizados, tão como a quase ilimitada capacidade de armazenamento, combinação e cruzamento de informações, é possível a formação de quadros de personalidade quase completos, aumentando exponencialmente as hipóteses de consulta e influência nos comportamentos dos indivíduos. Isso expõe ainda mais os usuários na Internet, reforçando a necessidade de estudo e regulamentação legislativa do tema (SOUZA, 2018, on-line).

Partindo deste pressuposto, vale destacar que, na maioria das vezes, o dado coletado recebe outra finalidade pelo operador. E é este desvio de finalidade, que deixa a pessoa usuária vulnerável.

As redes sociais tornaram-se a maior fonte de coleta de dados, pois ali as pessoas disparam diversas informações. Através de um rápido acesso, por exemplo, é possível catalogar determinadas preferências e gostos pessoais, construindo-se assim, um avatar do usuário. Paulo

Alves, em seu artigo "Big data: O segredo por trás da Eleição de Trump" para a página eletrônica Showmetech traz o método de perfilização criado pelo pesquisador Michal Kosinski:

> Kosinski provou que, com base em uma média de 68 likes do Facebook por usuário, era possível prever sua cor da pele (95% de precisão), sua orientação sexual (88%) e sua filiação aos partidos Democrata ou Republicano (85%). Mas, ele não parou por aí. Inteligência, afiliação religiosa, bem como uso de álcool, cigarro e drogas, tudo poderia ser determinado. Com esses dados era até possível deduzir se os pais de alguém eram divorciados. A capacidade de prever a resposta de alguém era a principal demonstração de força do modelo. Kosinski continuou a trabalhar (...) seu mecanismo já era melhor do que psicólogos para avaliar pessoas apenas com base em 10 curtidas de Facebook. 70 curtidas eram suficientes para saber mais até do que os amigos de alguém, 150 mais do que os pais. Para conhecer uma pessoa mais do que o seu parceiro, bastavam 300 curtidas. Com mais likes do que isso era possível conhecer mais até do que a própria pessoa sabia sobre si (ALVES, 2017, on-line).

A partir desta análise, podemos afirmar que com uma inocente curtida nas redes sociais, o controlador pode obter a ficha completa do indivíduo. Assim, segundo SCHIMIDT (2018) "a internet tornou-se um ambiente que oferece uma série de riscos aos usuários, pelos amplos meios de identificação de dados de interesse".

3 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

3.1 A Importância de uma Legislação para a Proteção dos Usuários da Internet

A Lei Geral de Proteção de Dados - LGDP, promulgada no ano de 2018, inspirada no regulamento de proteção de dados europeu, objetiva tratar dos dados pessoais dos indivíduos tanto pela iniciativa privada quanto pelo poder público. Silva e Silva argumentam que:

> [...] os estados europeus desde a década de oitenta normatizam a matéria a partir de sucessivas Diretivas, aperfeiçoadas sempre que o desenvolvimento tecnológico impôs novos ritmos às interações sociais e às transações econômicas. Essa abertura, garantida pela adoção de princípios (lealdade, respeito à finalidade do recolhimento aos dados, proporcionalidade) e as constantes revisões empreendidas permitem que a legislação não se cristalize e se mantenha em constante sintonia com os usuários. Como se percebe, o foco de proteção é a pessoa, e não meramente os interesses econômicos (2013, p. 24).

Pinheiro (2018) lembra de que a nova lei atua diretamente na base de dados pertencente às pessoas, e que em seu bojo, engloba um conjunto de normas que visam a cumprir as garantias no campo da proteção aos direitos humanos, e também no âmbito digital. A autora ainda analisa que a nova lei é uma garantia ao tratar de liberdade, de segurança e de dignidade:

> Destaque-se que a proteção das pessoas físicas relativamente ao tratamento dos seus dados pessoais é um direito fundamental, garantido por diversas legislações em muitos países. Na Europa, já estava previsto na Carta dos Direitos Fundamentais da União Europeia e no Tratado sobre o Funcionamento da União Europeia; no Brasil, já tinha previsão no Marco Civil da Internet e na Lei do Cadastro Positivo, mas a questão ainda era, muitas vezes, observada de forma difusa e sem objetividade no tocante aos critérios que serão considerados adequados para determinar se houve ou não guarda, manuseio e descarte dentro dos padrões mínimos de segurança condizentes (PINHEIRO, 2018, p. 18).

A partir do entendimento da autora percebemos a importância da aprovação da lei em comento, principalmente diante do atual cenário em que os negócios digitais estão inseridos,

entendendo ser a informação a novíssima moeda de troca utilizada pelas pessoas, para poder adquirir bens, produtos e serviços. Já em relação à segurança, a lei veio preencher lacunas. Assim, Silva e Silva afirmam que:

> Observa-se que a necessidade em proteger juridicamente o cidadão resulta do fato de que os dados pessoais adquiriram nos últimos anos forte componente econômico devido à possibilidade de sua comercialização, o que atrai empresas e fornecedores que atuam no ambiente virtual a utilizarem as mais variadas estratégias para obter dados dos internautas. Com efeito, os dados pessoais de um consumidor traduzem aspectos de sua personalidade e revelam comportamentos e preferências, tornando-o um alvo fácil de mensagens publicitárias. Quando se trata da Internet o tema ganha inda mais interesse tendo em vista a possibilidade de criação de perfis psicológicos que revelam os hábitos de consumo, os gostos e preferências do indivíduo e, uma vez formado o perfil, posteriormente esse consumidor passa a ser alvo de publicidades indesejadas, e-mails que oferecem serviços, produtos e uma série de outras "promoções" que parecem elaboradas e direcionadas especialmente a ele, tudo articulado com base nos dados antes recolhidos. Percebe-se, pois, que as novas tecnologias informacionais, especialmente a Internet, convertem a informação em uma riqueza fundamental da sociedade, o que acentua a necessidade de sua proteção (2013, p. 6).

No que tange ao direito digital, percebe-se que serão abrangentes os efeitos da nova lei. Contudo, é importante salientar que tal legislação não alcança somente as redes sociais e afins, mas qualquer empresa ou organização que faça coleta de dados dos seus clientes e que os guarde em seus bancos de informações.

Então, ao analisar um paralelo em relação a LGPD e o GDPR, percebe-se que ambas as leis possuem como finalidade a regulamentação dos dados pessoais, objetivando, consequentemente, a proteção de direitos fundamentais dos cidadãos. O regulamento europeu define as normas referentes ao tratamento aos dados pessoais referentes aos cidadãos do bloco europeu, seja por uma única pessoa ou por uma corporação ou organização. No entanto, ele não abrange as pessoas que já faleceram ou os organismos sociais dotados de personalidade jurídica. Percebe-se, então, que a nova legislação brasileira, com efeito, tem como base a lei européia, quando se trata deste tema. É na verdade uma tendência mundial, resultado da conjectura contemporânea. Vale lembrar que, somente no Brasil, a rede social Facebook possui mais de 127 milhões de usuários (BASTOS, 2018).

Antes de aprofundar na lei base da pesquisa, lei nº 13.709, torna-se fundamental informar que o Código de Defesa do Consumidor, Lei nº 8.078/1990 foi um dos primeiros sobre os bancos de dados e cadastro de consumidores, em seu art. 43. Posteriormente, o Código Civil de 2002, Lei nº 10.406, também se aproxima do tema, porém, nesse caso, mais preocupado com a delimitação mais atual dos direitos da personalidade, no âmbito da constitucionalização do Direito Civil (GODINHO, 2013). Ademais, é importante registrar a Lei do Cadastro Positivo, Lei nº 12.414/2011, que tem como objetivo regulamentar o disposto no CDC. Todos esses diplomas servem de base para proteção de dados.

A sigla LGPD representa o termo Lei geral de proteção de dados, lei nº 13.709, sancionada pelo Presidente da República em exercício na época, Michel Temer, em 14 de agosto de 2018, que entrou em vigor em 18 de setembro de 2020. A LGPD é análoga à GDPR (General Data Protection Regulation) da União Européia, que está em vigor desde 25 de maio de 2018. Contudo, os legisladores determinaram que a Vacatio Legis seria de 18 meses, mas após a sua entrada em vigor, esse prazo foi alterado para 24 meses, a ser apurado que a Lei apenas entraria em vigor no dia 16 de agosto de 2020. Uma das razões que determinaram a alteração desse prazo foi a crise causada pela Covid19, a fim de normalizar o impacto econômico provocado pela pandemia de corona vírus.

A LGPD é de autoria do Deputado Federal Milton Monti, que iniciou-se com o projeto de lei, PL 4.060/2012, o qual instituiu discussões acerca da matéria em território nacional. A proposição foi submetida à apreciação da Câmara dos Deputados com a seguinte justificativa:

> O presente Projeto de lei tem por objetivo dar ordenamento jurídico e institucional ao tratamento de dados pessoais, bem como a proteção dos direitos individuais das pessoas, de acordo com a Constituição da República Federativa do Brasil (MILTON MONTI, 2012, p.7).

Com o intuito de evitar o processamento indevido de dados, por meio de instituições públicas e privadas, deu-se início a regularização desta matéria no Brasil. Observa-se que a lei traz em seu bojo que as pessoas singulares ou coletivas de direito público ou privado tratem os dados pessoais, em que se inclui aqueles contidos nos meios digitais, de forma a proteger os direitos básicos e fundamentais de um Estado Democrático de Direito (SOARES, 2020, p.16). Em suma, a LGPD foi criada para proteger a privacidade dos dados pessoais das pessoas físicas, para que não sejam utilizados por terceiros de forma ilegal.

Importante destacar que, a lei se refere aos dados pessoais, aplicando-se à pessoa natural ou jurídica, pública ou privada, que realize tratamento de dados pessoais, ou seja, que exerça atividade em que se utilizem dados pessoais (coleta, armazenamento, compartilhamento, exclusão etc.), aplica-se ainda para dados coletados dentro do território brasileiro, não se aplicando a dados gerados.

A LGPD na sua própria lei nº 13.079/18, no seu artigo 2º estabeleceu os fundamentos para a devida utilização dos dados pessoais:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

3.2 Dados Pessoais

Para entender melhor a LGPD faz-se necessário definir de forma mais clara e contundente o que são dados pessoais. Os dados pessoais são informações que possam levar à identificação de uma pessoa, de maneira direta ou indireta. Ao falar de dados pessoais diretos, a primeira coisa que deve ser lembrada é que, estes não necessitam de nenhum processamento para identificação direta e eficaz do indivíduo, como o nome, o número do RG, ou do CPF. Já os dados pessoais indiretos dependem da junção de várias informações, para que uma pessoa possa ser identificada, ou seja, a partir de um processamento, como o número da placa de um carro, por exemplo, com a junção dos dados cadastrais presentes no DETRAN, tornam possível a identificação da pessoa física a qual tem a posse do veículo cadastrado sobre o número da placa em questão.

Os dados pessoais passam pela análise de duas teorias: a reducionista e a expansionista. No entendimento reducionista, para ser considerado dado pessoal, este deverá especificar e determinar a pessoa. É necessário, portanto, haver um vínculo direto e imediato entre o dado e a pessoa a que este se refira para caracterizá-lo como dado pessoal. Já para teoria expansionista, têm-se como dados pessoais todas as informações que digam respeito a uma pessoa identificada ou identificável. (BIONI, 2015).

Neste sentido,

> Ainda que divergentes, tais teorizações detêm o mesmo centro gravitacional. Ambas demandam uma análise contextual donde está inserido um dado, aferindo-se o seu grau de identificabilidade para, então, desencadear a compreensão se uma determinada informação está relacionada a uma pessoa identificada ou identificável. (SCHWARTZ; SOLOVE, 2011).

Adotando a teoria expansionista, a LGPD define, expressamente, dado pessoal em seu art. 5º, inciso I, como: "informação relacionada à pessoa natural identificada ou identificável" (BRASIL, 2018, s. p.). Assim, no direito brasileiro os dados que atraem repercussão jurídica são todos aqueles que sejam aptos a identificar uma pessoa natural.
A Lei trata de forma diferente duas categorias principais de dados pessoais: os dados de menores de 18 anos e os dados considerados sensíveis pela lei, como falaremos abaixo.

3.2.1 Dados de menores de 18 anos

Os dados pessoais dos menores de 18 anos deverão ser expostos, com o consentimento dos pais ou responsáveis legais. A LGPD informa que o controlador dos dados deve fazer o possível para captar o consentimento do responsável legal do menor, em seu art. 14, I.
Contudo, existem algumas exceções, como por exemplo, nos casos de saúde, nos quais o consentimento deve ser desconsiderado, podendo dessa forma, realizar o tratamento dos dados do menor, a fim de garantir o bem estar e a saúde da criança e do adolescente.

3.2.2 Dados sensíveis

Nos termos do art. 5º, II da LGPD,

> dados sensíveis são dados pessoais que versem sobre a "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).

Dados sensíveis são aqueles mais subjetivos, ligados ao comportamento do indivíduo, por isso, apresentam um maior potencial lesivo, exigindo, consequentemente, um regime jurídico próprio mais protetivo, o qual encontra previsão na Seção II do Capítulo II da LGPD.

3.3 Tratamento de Dados

Dá-se o tratamento de dados, a toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
A pessoa poderá exercer vários papéis no ciclo dos dados, sendo fundamental identificar suas principais responsabilidades. O art. 5° da LGPD define controlador, operador e encarregado, *in verbis*:

> Art. 5º Para os fins desta Lei, considera-se:
> ...
> 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;

> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); *(Redação dada pela Lei nº 13.853, de 2019)* *Vigência*
> IX - agentes de tratamento: o controlador e o operador (BRASIL, 2018).

Ao analisar a LGPD observar-se-á que o legislador inovou ao obrigar os controladores a disponibilizarem uma pessoa, que segundo o artigo 5º, inciso VIII da Lei, servirá como canal de comunicação entre o titular, entre os agentes de tratamento e entre a Autoridade Nacional de Proteção de Dados (ANPD), agência fiscalizadora, vinculada à Presidência da República, com autonomia técnica e decisória para realizar a fiscalização do cumprimento da Lei nº 13.709/2018, em território nacional.

3.3.1 Partes Envolvidas

a) Titular dos dados

Pessoa física que fornece seus dados pessoais ao consumir algum produto ou serviço. Este é o maior beneficiário da cobertura protetiva oferecida pela LGPD. A lei garante a sua liberdade, a sua privacidade e a livre expressão no desenvolvimento de sua personalidade. Portanto, é sobre esta pessoa que recairá as regras de proteção oferecidas pela LGPD.

b) Controlador

Pessoa jurídica ou física que recebe os dados pessoais de um titular para executar algum tratamento destes dados. Seu principal papel é tomar as decisões relativas ao tratamento dos dados pessoais de seus titulares e proteger a privacidade das pessoas físicas que lhe confiaram seus dados.

c) Operador

A pessoa contratada pelo controlador, que será responsável por nomear e preparar os relatórios de impacto, incluindo dados pessoais confidenciais, relacionados às operações tratamento.

d) Encarregado (DPO)

Pessoa que também será contratada pelo controlador, e que tem como principal função a intermediação e a comunicação entre as demais partes. O DPO é o representante dos titulares para os controladores. Este também auxiliará os controladores de dados e os operadores, direcionando-os na melhor forma para o tratamento dos dados, e a realização de auditoria.

e) Autoridade Nacional de Processamento de dados (ANPD)

Órgão do Governo responsável por fiscalizar a conformidade com a LGPD por parte das demais partes envolvidas. Ele será responsável pela aplicação de multas e pela realização de auditorias, verificando a aderência da LGPD dentro das organizações.
De acordo com a estrutura definida pelo Decreto nº 10.474/2020, ANPD exerce quatro funções básicas: Normativa; Educativa, Fiscalizatória e Sancionatória.

3.4 Princípios da lei geral de proteção de dados pessoais

Ao elencar os princípios na LGPD, o legislador preocupou-se em sua forma de aplicação, contudo, podemos observar que além dos princípios, deve-se observar a boa-fé. Nesse caso, a boa-fé é a objetiva, ou seja, àquela que é direcionada a condutas específicas, principalmente em relações jurídicas de caráter obrigacional (LÔBO, 2017).

Como já mencionado, a boa-fé foi o princípio que o legislador deu ênfase, e este é um princípio já conhecido do ordenamento jurídico brasileiro que disciplina amplamente as relações jurídicas, sejam elas de direito público, sejam de direito privado. A boa-fé trata diretamente da conduta das partes, exigindo-se destes uma conduta de cooperação e lealdade, relacionando-se à existência de deveres anexos (TARTUCE, 2017).

De acordo com Dhiulia Santos (2019), o consentimento do titular dos dados deve basear-se nos princípios regidos no artigo 6° da LGPD. Sendo que os princípios contidos no artigo 6° não anulam o vigor dos princípios da jurisdição brasileira.

O art. 6° da LGPD elenca os princípios informadores do tratamento de dados, os quais têm a importante função de orientar a atividade de tratamento de dados pessoais. O artigo 6º indica, portanto, onze princípios que vão orientar a atividade de tratamento de dados pessoais, *in verbis*:

> 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 (BRASIL, 2018).

Ao aplicar o princípio da boa-fé ao tratamento e proteção dos dados pessoais, respaldar-se-à a tutela da legítima expectativa do titular em face do controlador e do tratamento empregado por este, a qual é concebida diante das circunstâncias concretas em que se deu o consentimento e a finalidade que o respaldou (MIRAGEM, 2019).

Associado ao princípio da boa-fé está o princípio da finalidade, que diz respeito aos fundamentos do tratamento de dados, ou seja, pelo princípio da finalidade o tratamento de dados pessoais está diretamente interligado à motivação da coleta de dados.

Miragem (2019) nos explica que:

> Aquele que pretende obter o consentimento do titular dos dados, obriga-se a declinar expressamente as finalidades para as quais pretende utilizar os dados e, nestes termos,

> vincula-se aos termos desta sua manifestação pré-negocial. A utilização dos dados, seja para tratamento ou compartilhamento desviada das finalidades expressas quando da obtenção do consentimento, torna-o ineficaz e ilícita a conduta, ensejando responsabilidade, bem como todos os meios de tutela efetiva do direito do titular dos dados (MIRAGEM, 2019, p. 6).

Os princípios da adequação e da necessidade estão correlacionados ao princípio da finalidade, sendo a adequação a: "compatibilidade do tratamento com as finalidades informadas ao titular" e a necessidade a: "limitação do tratamento ao mínimo necessário para a realização de suas finalidades" (BRASIL, 2018, s. p.).

Os princípios do livre acesso, da qualidade dos dados e da transparência, são garantias dos titulares dos dados, além de informações claras, precisas e acessíveis sobre a realização do tratamento e sobre os agentes envolvidos. E, por fim, os princípios da segurança, prevenção, não discriminação e responsabilização, além do princípio da prestação de contas, também constituem garantias aos titulares dos dados pessoais, porém são responsáveis por orientar e ditar deveres e condutas para atuação dos sujeitos do tratamento de dados pessoais.

No tocante ao princípio da segurança, exige-se do controlador e do operador "a 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" (BRASIL, 2018, s. p.).

> A violação do dever de segurança, neste particular, implica na responsabilidade objetiva do fornecedor pelos danos causados, o que será a hipótese em que os dados venham a ser acessados por pessoas ou de modo não autorizado, ou ainda situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Tais hipóteses de acesso não autorizado, acidentes ou atos ilícitos a par do regime de responsabilização previsto na própria LGPD caracterizam espécie de risco inerente à atividade de tratamento de dados, ou seja, fortuito interno, situação que não é apta a afastar a responsabilidade dos respectivos controladores de dados. (MIRAGEM, 2019, p. 12-13).

Ainda sobre o princípio da segurança:

> A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 ou "LGPD"), que está em vigor desde 18 de setembro de 2020, reconhece a segurança como um dos princípios a serem observados por aqueles que exercem atividades de tratamento de dados pessoais; assim, de acordo com a LGPD, o princípio da segurança significa a "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" (VEIRANOS ADVOGADOS, 2021).

No que diz respeito ao princípio da prevenção, aqui é tratado sobre os riscos que o tratamento de dados pode gerar aos titulares e, por essa razão, os responsáveis devem adotar medidas que sejam aptas a prevenir a ocorrência de danos.

Por último, os princípios da não discriminação e da responsabilização e prestação de contas informam sobre a "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos" (BRASIL, 2018, s. p.)

RESPONSABILIDADE CIVIL

4.1 Segundo o ordenamento jurídico brasileiro

O vigente Código Civil brasileiro, em seu artigo 186, estabeleceu que todo aquele que suscitar uma perda material, ou moral a outrem, por ação ou por omissão voluntária, por negligência ou por imprudência, comete um ato ilícito. Em sequência, o artigo 187 do mesmo Código adicionou que: "também comete ato ilícito o titular de um direito que ao exercê-lo,

excede manifestamente os limites impostos pelos seus fins econômicos ou social, pela boa-fé ou pelos bons costumes". (BRASIL, 2002).

A leitura dos artigos, acima citados, sugere que o alicerce adotado pelo Código Civil pátrio, quanto à responsabilidade civil, foi o da teoria subjetiva, ou teoria da culpa, a qual caracteriza-se quando o fato danoso é assumido por quem o praticou, a fim de reparar os danos causados a terceiros, admitindo-se a existência de culpa, nexo de causalidade e um dano. Assim como, Maria Helena Diniz (1998, p.34 *apud* Dassan, 2017) explicita:

> A aplicação de medidas que obriguem alguém a reparar dano moral ou patrimonial causado a terceiros em razão de ato 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).

Entende-se, portanto, que o dever jurídico, quando não respeitado, ou quando não cumprido, gera uma obrigação civil, e portanto, a violação desta obrigação gera a responsabilidade civil, que é definida por Rodrigues (2002, p. 6) como: "a obrigação que pode incumbir uma pessoa a reparar o agravo causado à outra, por fato próprio, ou por fato de pessoas ou coisas que dela dependam".

Do exposto, conclui-se que a natureza jurídica da responsabilidade civil é sancionatória, assim sendo, cabe ao julgador examinar a conduta ilícita, o nexo entre a conduta e o dano sofrido pela vítima com o intuito de evitar tanto o rastreamento digital (*online tracking*), quanto o vazamento de dados pessoais sem autorização do titular a fim de evitar o "crescimento do network de atores que agem às sombras, mobilizando dinheiro e mídia para ganhos privados, mesmo quando agem oficialmente em nome do negócio ou do governo"(John Gilliom e Torin Monahan, 2013, s/p. *apud* FRAZÃO, 2019, p.25).

4.1.1 Responsabilidade Civil Subjetiva

A o pensar em responsabilidade civil na LGPD, há uma clara separação entre as relações civis (do cidadão) e relações de consumo. No que diz respeito aos contratos, se aplica a regra geral do Código Civil, onde a responsabilidade que se leva em conta é a do agente. Vale também destacar que, em se tratando do aspecto da lei em comento, a previsão da responsabilidade não é somente do controlador, mas também do operador.

Já vimos que o operador está submetido aos comandos do controlador, porém este desenvolve atividades de tratamento de dados sujeitas aos ditames da Lei da mesma forma. A própria lei no art. 42 institui que há solidariedade, entre controlador e operador, na obrigação de reparação dos danos, *in verbis*:

> Art. 42, §1º, 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.

O tratamento de dados é desenvolvido, normalmente, por uma rede, e para o seu funcionamento pode haver vários agentes na cadeia produtiva ao comando de mais de um controlador. Nesse caso, o inciso II do §1º, expressa que serão solidários todos os controladores. Para a comprovação da culpa, o legislador utilizará os dispositivos encontrados no Código de Processo Civil (CPC), desta maneira, pode-se observar que a legislação nacional é capaz de dar resposta nos casos de reparação de danos.

4.1.2 Responsabilidade Civil Objetiva

A responsabilidade civil objetiva é aplicada, por determinação legal, em casos especiais que decorre da Lei. No caso da LGPD, está prevista em duas situações: tratamento de dados no âmbito das relações de consumo, por força do art. 45 da Lei, e tratamento de dados pelo poder público, conforme art. 37, §6º da Constituição Federal pátria.
Por isso, o CDC assegura o consumidor em vários aspectos decorrentes das relações de consumo, por isso a LGPD determina que nos casos concernentes a relações consumeristas, deverá aplicar-se o CDC.

4.2 Breve análise das diferentes correntes existentes no direito brasileiro quanto à responsabilidade civil no ambiente virtual

A responsabilidade civil no campo da internet tornou-se tema constante nas pautas jurídicas, principalmente no que se diz respeito às recorrentes situações de vazamento de dados pessoais. Desde março de 2020, quando a Organização Mundial de Saúde (OMS) declarou estado de emergência internacional, e o Brasil decretou seu primeiro *lock down* para evitar a contaminação da população pelo vírus *Sars-Cov 2*; o uso da internet demonstrou um aumento de 40% a 50%, segundo dados da Agência Nacional de Telefonia (Anatel) publicados no site Globo.com.

Big Data são dados maiores, complexos e que chegam em grande velocidade, e que um software tradicional de processamento não é suficiente para gerenciá-los (ORACLE, *online*). No campo da *Big Data*, Bahia (2014, pg 36) sustenta que: "a responsabilidade civil na internet é um tema novo e ainda não pacificado no Poder judiciário, bem é verdade que há várias decisões contraditórias, ou seja, posicionamento díspares, gerando insegurança jurídica".

Devido à dificuldade de se comprovar a culpa, em alguns casos concretos, a jurisprudência posicionou-se através da teoria do risco decorrente da atividade, a fim de discorrer que o "agente é responsável pelos riscos que sua atividade promove" (Venosa, 2014, p. 13 apud Bahia, 2014, p.7), bem como, com a teoria do risco criado e do risco benefício.

5 Posicionamento dos Tribunais brasileiros

É crescente o número de vazamento de dados, conforme dados abaixo:

> Uma pesquisa recente do Massachusetts Institute of Technology ("MIT") publicada no Journal of Data and Information Quality da ACM (Association for Computing Machinery) aponta que vazamentos de dados aumentaram 493% no Brasil, sendo que mais de 205 milhões de dados de brasileiros vazaram de forma criminosa em 2019. Em número de incidentes relevantes, o país saltou de 3, em 2018, para 16 em 2019, de acordo com a pesquisa (VEIRANOS ADVOGADOS, *online*, 2021).

Sobre o aumento de vazamento de dados Castilho aponta (2022):

> Em 2021, o Brasil foi o sexto país mais atingido por vazamentos de dados, de acordo com um levantamento da empresa Surfshark, que atua na área de ferramentas de privacidade e segurança online. No âmbito empresarial não foi diferente. Só no primeiro semestre de 2021, pelo menos 69 instituições brasileiras foram alvo de ataques de vazamento e sequestro de dados, conforme dados da Apura Cyber Intelligence (CASTILHO, *online*, 2022).

Obviamente, o reflexo da situação hodierna é o aumento do número de processos nos Tribunais de Justiça brasileiros que versam sobre vazamento de dados, conforme algumas decisões que serão abordadas a seguir:

> Inteiro Teor: 2021.0000698477 APELANTE: WILLIANS SANTOS AMARAL APELADO: ELETROPAULO METROPOLITANA ELETRICIDADE DE SÃO PAULO S/A COMARCA: OSASCO MAGISTRADO PROLATOR DA DECISÃO: Dra. Claudia Guimarães dos Santos. EMENTA. DANO MORAL VAZAMENTO DE DADOS CÓDIGO DE DEFESA DO CONSUMIDOR DEVER DE SEGURANÇA.
> 1 Reconhecida a falha no sistema, ante a invasão por terceiros, ocasionando o vazamento de dados pessoais do consumidor, patente o dever de indenizar pelos danos morais sofridos;
> 2 Indenização por danos morais fixada no montante pleiteado, ou seja, em R$ 10.000,00, corrigidos do arbitramento e acrescido de juros de mora de 1% ao mês, a partir da citação. RECURSO PROVIDO

Neste primeiro caso houve o vazamento de dados no momento em que o consumidor estava realizando uma compra, então o julgador responsabilizou a empresa dona da plataforma e também arbitrou um valor de reparação por dano moral.

> Apelação cível 10008655320218260007. Ação de Obrigação de Fazer CC Indenizatória. Prestação de Serviços. Energia Elétrica. Vazamento de Dados Pessoais. Danos Morais. Senteça de improcedência. II- Autora que é titular de unidade consumidora de energia elétrica junto à ré e teve seus dados vazados - incontroverso o vazamento de dados da autora – aplicação ao caso do CDC, lei 13709-2018 Lei Geral de Proteção de dados – obrigação da ré de proteger os dados pessoais de seus clientes. Por falha na prestação do serviço, terceiro tiveram acesso aos dados pessoais da cliente. ..Danos morais contudo, não caracterizados. Para que haja o dever de indenizar, necessário aferir se o vazamento de dados causou algum dano a autora – ausência de demonstração de situação fática vexatória causada pelo fato...(TJSP, 2022).

Observa-se que há um posicionamento diferente nessa decisão, o julgador entendeu que se não houve uma situação que realmente tenha causado prejuízo pelo vazamento de dados, não há reparação de danos, porém reconheceu a falha na prestação de serviço por parte da ré. Denota-se, portanto, que a LGPD (lei de estudo desta pesquisa) foi aplicada pelo julgador em ambas as decisões.

Contudo, em recente matéria publicada no site JOTA, a repórter Letícia Paiva escreveu referente a não aplicação de condenação em mais de 70% dos casos, apesar de levarem à baila a LGPD, conforme trecho abaixo:

> Após menos de dois anos em vigor, a Lei Geral de Proteção de Dados (LGPD) já acumula casos nos tribunais e começa a ter delineadas as principais tendências sobre como a ela é aplicada pelo Judiciário. Em 2021, foram ao menos 465 decisões sobre o tema – 77% delas não resultaram em condenação, tendo sido extintas ou julgadas improcedentes (PAIVA, 2022).

No entanto, para que seja configurada a responsabilidade civil, há três determinantes, quais sejam: a conduta, o nexo de causalidade e o dano.

CONSIDERAÇÕES FINAIS

O presente trabalho trouxe como tema a Responsabilidade Civil no Vazamento de Dados Pessoais, alicerçado pela Lei Geral de Proteção de Dados nº 13.709/2018, um marco para as instituições privadas e públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais.

A LGPD utiliza-se de fundamentos em que seja priorizada a proteção dos indivíduos, porém o titular dos dados e consumidor dos bens ainda continuam vulneráveis, vez que as informações passaram a circular cada vez mais deixando a intimidade e a capacidade de escolha a mercê dos interesses econômicos das grandes empresas.

A Lei Geral de Proteção de Dados é satisfatória ao ponto que atende diversas demandas, bem como, as relações em que se aplicam a responsabilidade civil subjetiva e objetiva, de modo a efetivar a reparação do titular, preservando os fundamentos constitucionais.

Dessa forma, a análise da responsabilidade civil, é extremamente necessária, ao passo que serão compreendidas a possível falha no tratamento, e a prevenção das investidas realizadas. Para tanto, exige-se o estabelecimento de um diálogo de todo o arcabouço legal ora apresentado. Ao analisar as inovações trazidas pela LGPD é possível verificar um considerável avanço para a prevenção do vazamento de dados, objeto do presente artigo, sendo possível o vislumbre de um futuro promissor para a tutela de dados.

Para que a prevenção seja efetiva entende-se, por conseguinte, a necessidade dos usuários buscarem por maiores informações sobre os perigos "do online", analisando a veracidade de sites e de e-mails recebidos, sem fornecer dados de maneira aleatória, assim como, a existência de uma efetiva tutela prática e legislativa para a proteção de dados, que esteja atenta às mudanças exponenciais que o mundo virtual possibilita.

Constatou-se, portanto, que a LGPD cumpre com o seu papel de proteção de dados, pois assegura aos titulares a forma mais justa e moderna de responsabilização civil que há no nosso ordenamento jurídico. Dessa forma, se diz que os objetivos deste trabalho puderam ser contemplados.

REFERÊNCIAS

ALVES, Paulo. BIG DATA: o segredo por trás da eleição de Trump. 2017. Site Showmetech. Disponível em: https://www.showmetech.com.br/big-data-trump/. Acesso em: 04 nov. 2019.

BAHIA, John Hélder Oliveira. **Responsabilidade civil na internet**. Revista da Faculdade de Direito - UFBA. Salvador. Ed. espec. Dezembro 2014). Disponível em: http://web.unijorge.edu.br/sites/searajuridica/pdf/anteriores/2014/2/searajuridica_2014_2_pag30.pdf. Acesso em: 1 maio de 2021.

BASTOS, Athena. **Direito digital**: guia da lei geral de proteção de dados pessoais: LGPD. 2018. Disponível em: https://blog.sajadv.com.br/direito-digital-lei-de-protecaode-dados/. Acesso em: 20 maio 2022.

BIONI, Bruno Ricardo. **Xeque-mate**: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. São Paulo: GPOPAI, 2015.

BRASIL. **Lei de Acesso a Informação (Lei n° 12.527/11)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 05 abril 2022.

BRASIL. **Lei Marco Civil da Internet (Lei nº 12.965)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 abril 2022.

BRASIL. **Projeto de Lei 4.060/2012**. Disponível em:https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750#:~:text=autoridades%20administrativas%20competentes.-,Art.,noventa%20dias%20ap%C3%B3s%20sua%20publica%C3%A7%C3%A3o.&text=O%20presente%20Projeto%20de%20lei,da%20Rep%C3%BAblica%20Federativa%20do%20Brasil. Acesso em: 15 de abril de 2022.

BRASIL. **Inteiro Teor 2021.0000698477**. Disponível em: https://tj-sp.jusbrasil.com.br/jurisprudencia/1280608603/apelacao-civel-ac-10001447120218260405-sp-1000144-7120218260405/inteiro-teor-1280608627. Acesso em: 01 maio de 2022.

BRASIL. **Constituição (1988). Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Congresso Nacional. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em 2 de abril de 2022.

BRASIL. **Lei nº 13.709, Lei Geral de Proteção de Dados Pessoais**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em 2 de abril de 2022.

BRASIL. **Lei de Cadastro Positivo**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 10 maio 2022.

BRASIL. **Lei Carolina Dieckman, Lei n. 12.737/12**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 20 abril 2022.

Para um exame detalhado da Lei nº 12.414, de 2011, ver: BESSA, Leonardo Roscoe. Cadastro positivo: comentários à Lei 12.414, de 9 de junho de 2011. São Paulo: Revista dos Tribunais, 2011.

CASTILHO. Luiz Ricardo de. **O que podemos aprender com ano marcado por casos de vazamentos de dados**. Disponível em: *https://www.conjur.com.br/2022-abr-19/luiz-castilho-casos-vazamentos-dados2*. Acesso em 10 maio de 2022.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 08 abril 2022.

DONEDA, Danilo Cesar Maganhoto. **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. Disponível em: *https://egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm*. Acesso em: 18 de abril de 2022.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 02 abril. 2022.

EXAME. Disponível em: https://exame.com/tecnologia/documentos-mostram-que-dilma-rousseff-foi-espionada-pelos-eua/. Acesso em: 28 jun. 2022.

FRAZÃO, Ana;TEPEDINO, Gustavo; OLIVA, Milena. **A Lei Geral de proteção de dados e suas repercussões no Direito brasileiro.** São Paulo: Ed.Thomson Reuters Brasil Conteúdo e Tecnologia Ltda, 2019. Disponível em: https://www.academia.edu/40040675/Fundamentos_da_prote%C3%A7%C3%A3o_dos_dados_pessoais_No%C3%A7%C3%B5es_introdut%C3%B3rias_para_a_compreens%C3%A3o_da_import%C3%A2ncia_da_Lei_Geral_de_Prote%C3%A7%C3%A3o_de_dados. Acesso em: 5 maio 2021.

GODINHO, A. M. **O fenômeno da constitucionalização**: um novo olhar sobre o Direito Civil. Revista Libertas, Janeiro 2013.

OECD (2002), Diretrizes da OCDE sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais, OECD Publishing, Paris, https://doi.org/10.1787/9789264196391-en

PAIVA, Letícia. **LGPD: 77% das decisões que citam lei não resultaram em condenação em 2021**. https://www.jota.info/justica/lgpd-condenacao-77-das-decisoes-nao-27012022. acesso em: 02 de maio de 2022.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais comentários à lei n. 13.709/2018**: LGPD. São Paulo: Saraiva, 2018. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553608324/cfi/0!/4/2@100:0.00. Acesso em: 14 maio 2020.

LÔBO, P. **Direito Civil**: parte geral. 6. ed. São Paulo: Saraiva, 2017.

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, n.2, p. 173-222, nov. 2019. Disponível em: https://brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-odireito-do-consumidor.pdf. Acesso em: 08 maio. 2022.

RODRIGUES, Sílvio. **Direito Civil Responsabilidade Civil**, 20ª Edição, 2002. Editora Saraiva.

SANTOS, Dhiulia de Oliveira. **A validade do consentimento do usuário à luz da lei geral de proteção de dados pessoais**: lei n. 13.709/2018. 2019. 50 f. TCC (Graduação) - Curso de Direito,

Centro Universitário de Brasília - Uniceub, Brasília, 2019. Disponível em: https://repositorio.uniceub.br/jspui/handle/prefix/13802. Acesso em: 5 maio. 2022.

SOUZA, Thiago Pinheiro Vieira de. A proteção de dados pessoais como direito fundamental e a incivilidade do uso de cookies. 2018. 65 f. Monografia (Bacharelado em Direito) – Curso de Graduação em Direito, Universidade Federal de Uberlândia, Uberlândia, 2018. Disponível em: https://repositorio.ufu.br/handle/123456789/23198. Acesso em: 09 abril. 2022

SCHWARTZ, Paul M.; SOLOVE, George Washington. **The PII Problem**: Privacy and a New Concept of Personally Identifiable Information. New York University Law Review, New York, v. 86, n. 2, p. 1814-1823, 2011. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366. Acesso em: 22 maio. 2022.

SCHMIDT, Tiago Ramos. A defesa do consumidor nos serviços de plataformas e a nova lei geral de proteção de dados pessoais. 2018. Monografia (Graduação em Direito) – Faculdade de Ciências Jurídicas e sociais, Centro Universitário de Brasilia, Brasilia, 2018. Disponível em: https://repositorio.uniceub.br/jspui/handle/prefix/12908. Acesso em 15 de abril de 2022.

SOARES, Rafael Ramos, Lei de Proteção de Dados – LGPD: Direito à Privacidade no Mundo Globalizado, 2020 (Graduação em Direito) – Pontifícia Universidade Católica de Goiás. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1201. Acesso em: 15 de abril 2002.

SILVA, Rosane Leal; SILVA, Letícia Brum. **A proteção jurídica de dados pessoais na internet:** análise comparada do tratamento jurídico do tema na União Europeia e no Brasil. Direito e novas tecnologias. Florianópolis: FUNJAB, 2013. Disponível em: http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65. Acesso em: 5 jun. 2022.

TARTUCE, Flávio. **Manual de direito civil**: volume único. 7 ed. Rio de Janeiro: Forense, 2017.

VERANO ADVOGADOS. Vazamentos de dados aumentaram 493% no Brasil, segundo pesquisa do MIT. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit/. Acesso em 10 maio de 2022.

WARREN, Samuel; BRANDEIS, Louis D. **The Right to Privacy**. In: Harvard Law Review, Vol. 4, N. 5. Ano 1890. P, 193-220