A RESPONSABILIZAÇÃO CIVIL PELA DIVULGAÇÃO INDEVIDA DE DADOS PESSOAIS DOS USUÁRIOS DE REDES SOCIAIS

Vitor Hugo Sepulveda Filho[1]
Giovanna Pagani Scaramussa[2]

1 INTRODUÇÃO

O avanço tecnológico e a ampla utilização das redes sociais, sobretudo devido ao armazenamento de dados pessoais dos seus usuários - como nome, data de nascimento, e-mail, entre outras informações pessoais - acarretaram a necessidade de regularizar a divulgação de tais dados, a fim de solucionar o grave problema contemporâneo que é a divulgação indevida de dados pessoais.

O uso de redes sociais é um hábito notadamente difundido nas sociedades contemporâneas. Em vista desse uso demasiado das redes sociais, não é raro encontrar situações em que os usuários dessas plataformas têm seus perfis “invadidos” por agentes externos, que buscam acessar dados pessoais não divulgados amplamente, como documentos, endereço residencial e dados bancários, para fins ilícitos.

Nesse cenário, foi editada a Lei nº 13.709/2018, amplamente conhecida como Lei Geral de Proteção de Dados Pessoais, responsável não só por organizar normativamente as regras que seriam aplicadas ao tema, bem como por conceituar termos essenciais a esta regularização e dispor, por fim, a forma como seria concretizada a responsabilização do(s) agente(s) responsável(is) por divulgar indevidamente os dados pessoais por ela protegidos.

O presente artigo visa, portanto, aprofundar-se pontualmente no aspecto da responsabilização de agente prevista na Lei nº 13.709/2018. Serão estudados, para tanto, os aspectos gerais do instituto da responsabilidade civil, destacando os

---

[1] Graduando em Direito pela Faculdade de Direito de Cachoeiro de Itapemirim.

[2] Professora Orientadora. Bacharel em Direito pela Faculdade de Direito de Cachoeiro de Itapemirim. Advogada. Especialista em Direito Civil e Empresarial.

requisitos e pressupostos necessários para efetivar, nos casos concretos, a proteção normativa destinada aos dados pessoais por meio da Lei Geral de Proteção de Dados Pessoais.

Além disso, a presente pesquisa propõe-se a realizar ponderações quanto à Lei nº 13.709/2018, responsável por dispor sobre a proteção de dados de pessoas físicas e jurídicas, bem como a respeito de outras previsões legais e posicionamento jurisprudencial acerca da responsabilização civil pelo vazamento de dados pessoais de usuários das redes sociais.

2 METODOLOGIA

A presente pesquisa visa aprofundar os conhecimentos acerca da responsabilização civil dos agentes que divulgam indevidamente dados pessoais dos usuários de redes sociais.

Para o desenvolvimento do presente estudo será adotada a pesquisa exploratória, a qual, de acordo com Gil (2007, p. 17 *apud* Gerhardt e Silveira 2007), n.p.), tem por objetivo tornar o tema mais explícito, ou construir novas hipóteses.

A pesquisa exploratória será fundamentada no método de pesquisa bibliográfica, através da coleta de elementos textuais e análise de legislação, doutrinas e jurisprudência, a fim de proporcionar melhor compreensão da temática discutida e tornar possível explanar o assunto de forma coerente e acessível.

Portanto, por tratar-se de estudo voltado à revisão bibliográfica, para alcançar o objetivo traçado é necessário efetuar pesquisas e entender conceitos relacionados ao tema e publicados em materiais como livros, artigos e reportagens.

3 REFERENCIAL TEÓRICO

As sociedades contemporâneas vivenciam o contexto da realidade tecnológica, de modo que as Tecnologias Digitais de Informação e Comunicação (TDIC), como, por

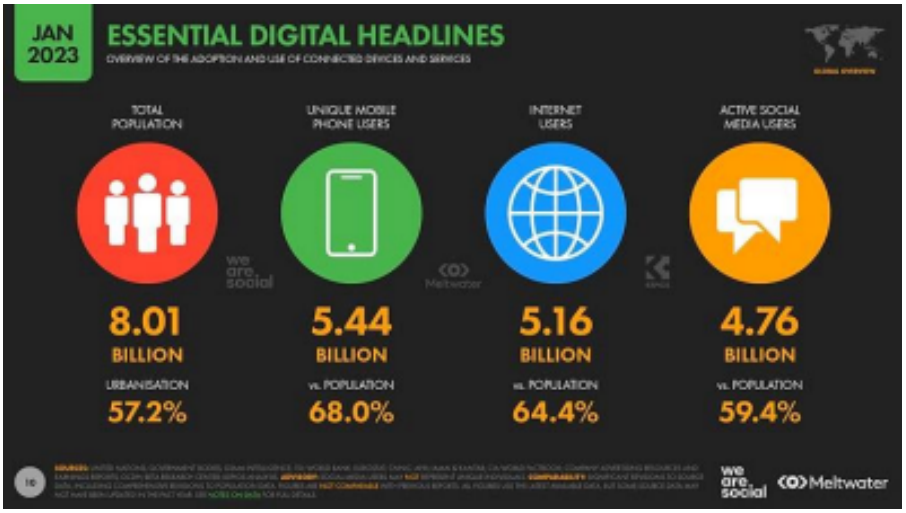
exemplo, as redes sociais, estão cada vez mais presentes no cotidiano das pessoas. Segundo Galvão, Jesus e Ramos (2012 *apud* Santos, 2016, p. 14):

> As Tecnologias Digitais de informação e Comunicação (TDIC`s) não são apenas a Internet e sim um conjunto de equipamentos e aplicações tecnológicas, que têm na maioria das vezes a utilização da internet como meio de propagação e que se tornam um canal de aprendizagem. Embora não substituam as tecnologias convencionais (como rádio e televisão), que continuarão sendo utilizadas e possuem, cada qual, a sua função. No âmbito da educação, as TDIC`s podem ser entendidas como ferramentas de suporte e devem ser orientadas segundo os objetivos da educação, pois a obtenção de ótimos resultados depende de determinarmos de forma clara e objetiva o que pretendemos trabalhar em sala de aula para depois definir qual tecnologia se enquadra melhor para alcançar o resultado esperado no processo de ensino e aprendizagem, ou seja, escolher primeiro a tecnologia a ser utilizada nem sempre trará um resultado satisfatório, pois existem vários fatores que devem ser observados.

De acordo com o Relatório de Visão Geral Global Digital (2023, n.p.), elaborado pela Pesquisa We Are Social, a população mundial atingiu a marca de 8,01 bilhões de pessoas no início de 2023.

Dentro deste quantitativo, o relatório aponta que 5,16 bilhões de pessoas têm acesso à internet, o que corresponde a 64,4% (sessenta e quatro vírgula quatro por cento) da população mundial, ao passo que 4,76 bilhões de pessoas são usuários de mídia social, isto é, um pouco menos de 60% (sessenta) da população global.

Imagem 01: Visão geral da adoção e uso dos dispositivos e serviços conectados.



Fonte: Relatório de Visão Geral Global Digital 2023.

Ressalta-se que as redes sociais, de acordo com Boyd e Ellison (2007 *apud* Recuero, 2009, p. 191), são sites em que o usuário constrói seu perfil, isto é, sua identidade social, a fim de interagir com outros usuários cadastrados através de comentários ou mensagens, sendo possível, ainda, que cada um desses usuários compartilhe características e/ou imagens pessoais nas redes sociais, acarretando na exposição pública da identidade do usuário cadastrado.

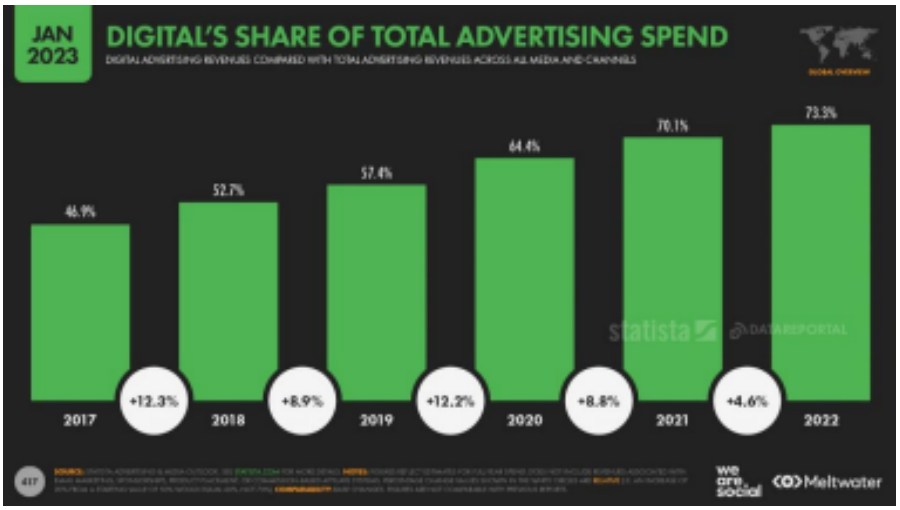
Desse modo, a utilização em massa das redes sociais representa também a divulgação em massa de informações pessoais dos seus usuários, tornando necessária a proteção de dados dos internautas que acessam tais redes sociais.

O conceito de informação abordado nesta pesquisa tem por base a definição feita por Whitman (2013 *apud* Izumi e Tomazetti, 2019, p. 06), na qual compreende se como “um conjunto de dados sobre determinado tipo de assunto com diferentes níveis de importância para determinados grupos de pessoas ou empresas”.

Nesse ponto, a respeito da importância que esses dados podem apresentar às empresas, deve-se destacar o fato de que a realidade tecnológica encontra-se presente também na economia, razão pela qual a proteção de dados dos usuários da internet, sobretudo daqueles que utilizam redes sociais, é imprescindível, pois a privacidade (inclusive de seus dados bancários) é bem jurídico essencial e inerente à pessoa humana.

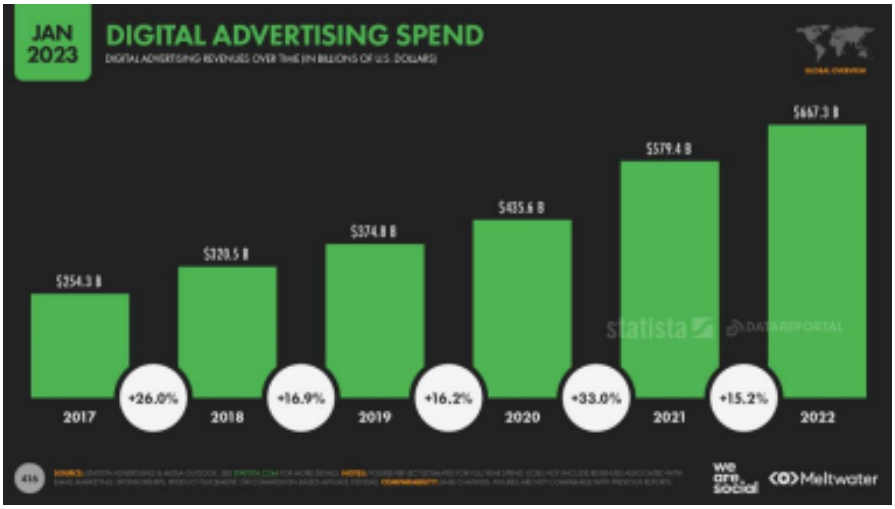
A respeito da relevância das publicidades digitais, o Relatório de Visão Geral Global Digital (2023, n.p.) aponta o crescimento exponencial do setor de publicidade digital, sobretudo no cenário pandêmico e pós-pandemia da COVID-19. Desse modo, as receitas dos anúncios digitais aumentaram 78% (setenta e oito por cento) desde 2019, alcançando a arrecadação de US$667 bilhões (seiscentos e sessenta e sete bilhões de dólares) em 2022.

Imagem 02: Receitas de publicidade digital em comparação com as receitas totais de publicidade em todas as mídias e canais.



Fonte: Relatório de Visão Geral Global Digital 2023.

Imagem 03: Receitas de publicidade digital ao longo do tempo em bilhões de dólares americanos.



Fonte: Relatório de Visão Geral Global Digital 2023.

É perceptível, portanto, que as empresas buscam alcançar cada vez mais os consumidores por meio da publicidade digital, enviando diversos anúncios e links patrocinados relacionados com as preferências de buscas dos usuários das redes sociais, sendo que tais informações são obtidas por meio de *cookies* existentes nos mais diversos sites e nas redes sociais.

Vale mencionar que os *cookies*, de acordo com Barreda (2021, n.p.), são “pedaços de código que dão a um site uma espécie de memória de curto prazo, permitindo que ele se lembre de pequenos pedaços de sua navegação”.

Assim, a segurança da informação é indispensável na utilização das redes sociais, pois visa preservar os dados pessoais desses usuários tanto de grandes empresas quanto de outros usuários que pretendem angariar vantagens indevidas com tais informações.

Nessa sistemática, Hintzberg (2018 *apud* Izumi e Tomazetti, 2019, p. 06) indicou que a base da segurança da informação é composta por três princípios: Confidencialidade, Integridade e Disponibilidade, representados pela sigla CIA.

Imagem 04: Representação sistemática dos fundamentos da Segurança da Informação.

Fonte: Fundamentos da Segurança da Informação Hintzberg (2018).

Segundo Hintzberg (2018 *apud* Izumi e Tomazetti, 2019, p. 06), a confidencialidade dos dados significa que apenas pessoas autorizadas terão acesso aos dados protegidos, mantendo-os fora do alcance de pessoas indesejadas; a integralidade dos dados garante que a informação não foi alterada ou comprometida durante seu processamento ou envio; e a disponibilidade garante que as pessoas autorizadas tenham acesso à informação desejada em um curto período de tempo.

É imperioso destacar que Santos (2016, p. 16) ressalta o fato de os dados

pessoais, como datas de nascimento, nomes completos, fotografias, nomes de escolas, entre outros, serem os principais alvos de atividade de *hackers*. Isso porque esses dados pessoais podem ser utilizados pelo invasores (*hackers*) para acessar outras contas do usuário existentes na internet, como e-mail ou sites de compras, através do sistema de recuperação de senha, o qual muitas vezes é realizado por meio de perguntas a respeito da vida pessoal do usuário.

Os autores Hamada e Nassif (2019 *apud* Izumi e Tomazetti, 2019, p. 08) salientam:

> Se de alguma maneira a informação é divulgada por algum outro meio, o invasor tiver acesso às respostas das perguntas, outros serviços utilizados pelo usuário podem ser comprometidos. O invasor apenas precisa fornecer a resposta correta a respeito da vítima para "comprovar" que é realmente o dono da conta, assim o sistema libera a troca da senha para ter acesso a conta.

A divulgação indevida de informações ou dados pessoais revela-se tão preocupante que algumas das mais importantes plataformas digitais e redes sociais já sofreram com o "vazamento" de dados de seus usuários, dentre as quais podem ser citadas:

- Facebook: Segundo Gauchazh (2018 *apud* Izumi e Tomazetti, 2019, p. 08), aproximadamente "30 milhões de contas de usuários do Facebook tiveram seus dados como nome, conversas privadas e preferências vazadas à empresas privadas";
- Twitter: De acordo com Tiinside (2017 *apud* Izumi e Tomazetti, 2019, p. 08), os desenvolvedores da rede social obtiveram acesso à conversas privadas e postagens com acesso restringido pelo usuário-autor "devido a um bug encontrado na API da plataforma. O site afirma que [...] apenas 1% dos seus 335 milhões de usuários foram afetados";
- Consoante a reportagem elaborada pelo portal Techtudo (2019, n.p.), a rede social Google+ foi oficialmente encerrada devido a dois episódios de vazamento de dados pessoais, nos anos de 2018 e 2019, que afetaram mais de 50 (cinquenta)

milhões de usuários com a divulgação de dados como profissão, nome, e-mail, idade, entre outros.

Destaca-se que recentemente a Polícia Civil do Distrito Federal (PCDF) prendeu dois *hackers* envolvidos em um esquema de venda de dados sigilosos. De acordo com a reportagem divulgada pelo portal Convergência Digital (2023, n.p.), cerca de 200 (duzentos) milhões de dados pessoais (como fotos, assinaturas digitais, veículos e registros de armas) estavam expostos, sendo tais informações "usadas para diversas fraudes eletrônicas, violações da intimidade dos cidadãos e elaboração de dossiês contra autoridades públicas".

A CNN Brasil (2023, n.p.) divulgou, ainda, que entre as vítimas da divulgação indevida de dados encontram-se "ministros do Supremo Tribunal Federal (STF), governadores e deputados distritais e federais". A reportagem também explica que a "PCDF afirma que os criminosos também tinham acesso às câmeras de OCR (leitura de placas), permitindo a localização das últimas passagens das vítimas nas rodovias de todo o país e, portanto, possibilitando o acompanhamento de suas rotinas".

Diante desse cenário, o Poder Legislativo pátrio, visando a proteção de dados pessoais dos usuários de internet, editou a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) -, que se apresenta como um marco histórico na regulamentação sobre o tratamento de dados pessoais no Brasil, pois abarca os dados armazenados tanto em meios físicos quanto plataformas digitais, seja por instituições públicas ou privadas.

3.1 Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais

Anteriormente à LGPD, a proteção de dados pessoais já constava no rol de direitos e garantias fundamentais do art. 5º, LXXIX da Constituição Federal (CF/88), em vista da promulgação da Emenda Constitucional nº 115/2022. Contudo, a LGPD demonstrou-se como marco histórico ao tratar do tema em maior amplitude e profundidade. Assim, por ser a proteção e a privacidade de dados uma garantia fundamental, o art. 1º da LGPD dispõe que as normas regulamentadoras sobre o

tratamento de dados alcançam não só as pessoas naturais (pessoas físicas), como também atinge as pessoas jurídicas:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
>
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

É imperioso destacar, nesse momento, que a LGPD faz algumas diferenciações entre alguns tipos de dados pessoais, classificando-os entre dado pessoal, dado pessoal sensível e dado anonimizado.

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> [...]

Deve-se ressaltar também que a LGPD é aplicável a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica (PJ), de direito público ou privado. Vale destacar, quando o tratamento de dados é realizado por pessoa jurídica, a proteção desses dados permanece sendo garantida independentemente do meio, do país de sede da PJ ou do país no qual estejam localizados os dados, desde que a operação de tratamento de dados seja:

a) realizada no Brasil;
b) a atividade de tratamento tenha por objetivo a oferta de bens ou serviços ou o manejo de dados de indivíduos localizados no país;

c) que os dados pessoais (objeto do tratamento) tenham sido coletados em território nacional.

Entretanto, estão excluídos da aplicação da LGPD alguns meios de tratamentos de dados, a exemplo daqueles realizados para fins exclusivamente jornalísticos, artísticos e acadêmicos, além de informações relacionadas exclusivamente à segurança pública, defesa nacional, segurança do Estado e a atividades de investigação e repressão de infrações penais.

Ante a posição de garantia fundamental da proteção de dados, é possível notar que os principais fundamentos da LGPT correspondem ao respeito à privacidade, à inviolabilidade da intimidade e ao desenvolvimento econômico e tecnológico, o que se depreende do art. 2º da referida legislação.

Além disso, uma importante característica da LGPD é que seu art. 6º, além de apontar os princípios que devem nortear as atividades de tratamento de dados, também explica o modo como tais princípios devem ser aplicados na prática.

> 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.

Essa particularidade da LGPD evidencia, portanto, a preocupação do legislador em fundamentar a autodeterminação informativa da Lei nº 13.709/2018. Ou seja, com a finalidade de resguardar a privacidade de cada indivíduo e de ratificar o posto de garantia fundamental da proteção de dados, a LGPD optou por esclarecer de modo expresso a forma como cada agente (pessoa física ou jurídica) deve se portar quando exercer atividade de tratamento de dados pessoais de outrem.

Contudo, é corriqueiro deparar-se com situações de “vazamento” de dados pessoais, sobretudo em meios eletrônicos. Essa divulgação indevida dos dados pessoais, segundo Izumi e Tomazetti (2019, p. 03) pode ocorrer tanto por falha na segurança de tais dados como pela ação dos denominados *hackers*, que invadem sites de comunicação, de instituições bancárias ou mesmo redes sociais.

É nesse contexto de divulgação indevida de dados pessoais que a presente pesquisa busca discorrer sobre a forma como ocorre a responsabilização civil é desenvolvida e aplicada no contexto legal da Lei Geral de Proteção de Dados Pessoais.

3.2 Responsabilidade civil

Inicialmente, é preciso entender o instituto da responsabilidade civil. De acordo com os ensinamentos de Gonçalves (2018, n.p.), a responsabilidade civil teve início nas primeiras civilizações, sendo construída ao longo dos séculos e sofrendo diversas influências antes mesmo de possuir previsão legal.

Ainda hoje, o instituto é regido pelo princípio do *neminem laedere*, o qual, de acordo com Leite (2009, n.p.), pode ser traduzido pela premissa de que a ninguém é facultado causar prejuízo a outro.

Porém, Bozzi (2017, n.p.) explica que, no início, a responsabilidade era apenas uma consequência prática da vida cotidiana, como um tipo de sanção social,

completamente desvinculada às noções de Direito, sendo imposta a quem causasse algum dano a outra pessoa.

Com o decorrer dos anos, começaram a ser substituídas as penas corporais por compensação econômica, passando a existir diferenciação sistemática entre pena e reparação com a criação do conceito de bens públicos e privados. Logo, de acordo com Bozzi (2017, n.p.) o Estado assumiu "[...] a função punitiva, fazendo surgir, então, a ação de indenização, onde o prejudicado deveria acionar o causador do dano para que este o restituísse dos prejuízos causados".

A sistematização da responsabilidade civil fez com que surgissem pressupostos para sua adequação, sendo eles:

a) Conduta: Para que possa se falar em responsabilidade, antes deverá haver uma conduta humana voluntária;
b) Dano: O dano é compreendido como uma lesão causada a um bem jurídico tutelado;
c) Nexo de causalidade: Para que esteja caracterizada a responsabilidade civil deverá haver nexo causal, isto é, relação de causa e consequência entre a conduta praticada e o dano obtido;
d) Culpa: A culpa certamente é um elemento compositor da responsabilidade civil, contudo, ela somente será avaliada quando tratar-se de responsabilidade subjetiva do causador do dano.

É imprescindível destacar o papel do elemento "culpa" no contexto da responsabilidade civil. Todavia, esse aspecto somente passou a ter uma importância vislumbrada a partir da Lei Aquiliana, sendo incluído ao ordenamento jurídico romano devido à influência grega, por meio do preceito *impunitur est qui sine culpa et dolo malo casu quodam damnum committit*, isto é, aquele que causou dano a outrem sem culpa ou dolo não será punido, tal como ressalta Bozzi (2017, n.p.).

O Código Civil de Napoleão, por sua vez, considerava a culpa como base da conceituação de responsabilidade civil, sendo inimaginável vincular o agente à

responsabilização sem que houvesse culpa em sua conduta. Em consequência da grande representação mundial deste Código, o Brasil, como apontado por

Gonçalves (2018, n.p.), passou a adotar o mesmo conceito de responsabilidade civil no Código Civil de 1916. Anos após, com diversas outras influências mundiais, alterações de condutas sociais e atualizações jurisprudenciais – já sob a luz do Código Civil (CC) de 2002 – o conceito de responsabilidade civil no ordenamento jurídico pátrio também modificou-se, de modo que, segundo Gonçalves (2018, n.p.), a depender da ótica do fundamento jurídico utilizado, a culpa não mais é abarcada como elemento fundamental de composição da responsabilidade civil, assumindo, dessa forma, a existência da responsabilidade civil objetiva.

Portanto, responsabilidade civil subjetiva, de acordo com os ensinamentos de Franqueira (2007, n.p.), é aquela em que é necessário demonstrar a subjetividade "residente na *psique* do ofensor", através da externalização de sua vontade (dolo) ou na falta de cuidado na conduta (ou seja, por meio das modalidades de culpa negligência, imprudência e imperícia). Em outras palavras, nessa modalidade de responsabilização civil é preciso restar evidente que o agente quis causar o dano por meio de sua conduta, ou, se não o quis conscientemente, agiu de forma que o possibilitou de acontecer quando era perfeitamente possível evitá-lo.

Por outro lado, a responsabilidade civil objetiva dispensa comprovação de culpa para acarretar a obrigação de indenizar. Isso porque, tal modalidade é baseada na teoria do risco, isto é, no entendimento de que o agente que desenvolve a atividade de risco deverá responder também pelos danos por ela causados, sem que se evidencie sua relação subjetiva (culpa ou dolo), sendo necessário, portanto, apenas a caracterização do nexo de causalidade existente entre a conduta praticada e o resultado danoso obtido.

Essa modalidade de responsabilidade civil atualmente possui previsão legal no parágrafo único do art. 927 do CC/2002, *in verbis*:

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.

> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

Nesse sentido, Gonçalves (2018, p. 49) ensina sobre a teoria do risco:

> Para esta teoria, toda pessoa que exerce alguma atividade cria um risco para terceiros. E deve ser obrigada a repará-lo, ainda que sua conduta seja isenta de culpa. A responsabilidade civil desloca-se da noção de culpa para a ideia de risco, ora encarada como "risco proveito", que se funda no princípio segundo o qual é reparável o dano causado a outrem em consequência de uma atividade realizada em benefício do responsável [...]; ora mais genericamente como "risco criado", a que se subordina todo aquele que, sem indagação de culpa, expuser alguém a suportá-lo.

Portanto, a diferença fundamental entre as duas modalidades de responsabilidade civil é a necessidade de se auferir a existência do elemento subjetivo culpa no momento de concretizar a obrigação indenizatória do agente.

4 RESULTADOS

A LGPD dedicou uma sessão inteira para tratar da responsabilidade e do ressarcimento de danos causados ao titular dos dados pessoais/sensíveis. Como regra geral, o art. 42 da LGPD apresenta a seguinte redação:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
>
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
>
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
>
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Não obstante a isso, Barbosa (2021, p. 475 *apud* Capanema, 2020, p. 163-170) destaca que:

> [...] o legislador reconhece que a proteção de dados é um microssistema, com normas previstas em diversas leis, sendo a LGPD a sua base estrutural. A responsabilidade civil na LGPD não decorre apenas da violação desse microssistema jurídico de proteção de dados, sendo necessário interpretar a regra geral prevista no caput do art. 42, em conjunto com o parágrafo único do art. 44 da lei.

Existem, portanto, duas hipóteses para caracterização da responsabilidade civil com base na LGPD: I) descumprimento das normas de proteção de dados; II) violação de normas técnicas de segurança e proteção de dados.

Desse modo, a LGPD apresenta como regra geral a responsabilidade civil objetiva, uma vez que os danos de vazamento dos dados decorre, nos dizeres de Flumignan (2021, n.p.), exatamente “da violação dos deveres decorrentes da tutela dos dados pessoais e, portanto, não necessitando de discussão acerca da culpa do agente”.

Além disso, o §2º do art. 42 da LGPD indica que caberá à vítima comprovar o nexo de causalidade entre o resultado danoso e a conduta do controlador ou operador dos dados pessoais, sendo possível, ainda, que o juiz determine inversão do ônus da prova quando considerar a alegação da vítima verossímil ou identificar sua hipossuficiência para produção de provas.

É nesse sentido que decidiu a Segunda Turma do STJ (Superior Tribunal de Justiça) no Acórdão do Agravo em Recurso Especial nº 2.130.619/SP

(2022/0152262-2). Além disso, nesta decisão, o STJ ainda ressaltou a diferenciação que a LGPD fez entre dados pessoais e dados sensíveis, de modo que o vazamento de dados pessoais comuns, ainda que seja considerado falha no tratamento de dados, por si só, não irá configurar dano à vítima.

> **PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO.**
> I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais. II - A sentença julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa. III - A tese de culpa exclusiva de terceiro não foi, em nenhum momento, abordada pelo Tribunal Estadual, mesmo após a oposição de embargos de declaração apontando a suposta omissão. Nesse contexto, incide, na hipótese, a Súmula n. 211/STJ. In casu, não há falar em prequestionamento ficto, previsão do art. 1.025 do CPC/2015, isso porque, em conformidade com a jurisprudência do STJ, para sua incidência deve a parte ter alegado devidamente em suas razões recursais ofensa ao art. 1022 do CPC/2015, de modo a permitir sanar eventual omissão através de novo julgamento dos embargos de declaração, ou a análise da matéria tida por omissa diretamente por esta Corte. Tal não se verificou no presente feito. Precedente: AgInt no REsp 1737467/SC, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 8/6/2020, DJe 17/6/2020. IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis. V - O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações. VI - Agravo conhecido e recurso especial parcialmente conhecido e, nessa parte, provido.

Por outro lado, o art. 43 da LGPD aponta excludentes de ilicitude. *In verbis*:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
>
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

São, portanto, causas que rompem o nexo causal entre o dano e a conduta do controlador ou operador dos dados pessoais: o tratamento irregular desses dados; a inobservância das legislações e normas sobre o tema; e a comprovação de culpa exclusiva do titular dos dados pessoais ou de terceiro.

Vale mencionar, porém, que a LGPD não regulamenta casos de culpa concorrente da vítima ou situações de caso fortuito ou de força maior. Nesse sentido, Barbosa (2021, p. 481) afirma:

> [...] a LGPD não apresenta o caso fortuito ou a força maior como causas excludentes do dever de indenizar. Do ponto de vista prático, destaca-se que fazem alusão a fatos estranhos à vontade do devedor ou do interessado, gerando prejuízos em razão de acontecimentos que escapam do poder do agente. O caso fortuito ou a força maior têm o condão de afastar até mesmo a responsabilidade objetiva, justamente por evidenciar rompimento do nexo de causalidade.13 A atividade de tratamento de dados, assim como qualquer outra atividade, não está incólume a eventos imprevisíveis e irresistíveis que afetem negativamente seu funcionamento. Invasões ou falhas nos sistemas de segurança, seguidas pelo incidente de vazamento dos dados pessoais dos titulares, representam, para a atividade em si, uma grande preocupação, pois poderão ocorrer ainda que os agentes de tratamento tenham tomado todas as medidas preventivas e de segurança cabíveis, utilizando-se das melhores práticas de mercado para atingir tal objetivo. E sendo a LGPD omissa nesse sentido, cabe indagar se tais eventos, alheios à atuação e à vontade do controlador, afastariam, ou não, os efeitos da responsabilidade civil. Percebe-se que essas excludentes dependem da produção de prova por parte do agente. Portanto, o processo será muito mais complexo e extenso.

Por fim, o art. 44 da LGPD evidencia quando o tratamento de dados será considerado irregular.

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
>
> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
>
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança

> dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Percebe-se, portanto, que a responsabilização civil quanto ao vazamento de dados com base na LGPD dependerá de algumas circunstâncias para ser concretizada. É preciso, inicialmente, averiguar a natureza dos dados pessoais que

foram irregular ou ilegalmente divulgados, isto é, se são dados pessoais comuns ou dados pessoais sensíveis, nos termos do art. 5º da LGPD.

Após, deve-se apurar se houve, de fato, prejuízo (dano) à vítima e a existência de nexo de causalidade entre a ação do operador/controlador de dados e o resultado danoso, vez que a modalidade de responsabilização adotada pela LGPD é a responsabilidade civil objetiva, que dispensa por completo aferição de culpa, mas ainda requer a ocorrência dos outros requisitos para caracterizar a responsabilidade do agente.

5 CONCLUSÃO

O presente estudo demonstrou como o sistema de responsabilidade civil da LGPD se estrutura. Ao confrontar as previsões constantes nas normas da LGPD com demais legislações do ordenamento jurídico pátrio e com o posicionamento jurisprudencial adotado, sobretudo no âmbito do Superior Tribunal de Justiça, é possível notar que o método de responsabilização dos agentes operadores e controladores de dados adotados pela LGPD é a responsabilidade civil objetiva.

Isso porque, a Lei Geral de Proteção de Dados Pessoais não menciona averiguação de culpa do agente causador do dano, mas tão somente indica a forma como tais agentes responderão quando for comprovado o dano e o nexo causal com sua conduta - ou omissão.

Além disso, a LGPD ainda apresenta causas excludentes de ilicitude do agente operador ou controlador de dados, bem como afirma a necessidade de ser comprovada a relação existente entre o resultado danoso e a conduta do operador ou controlador

dos dados pessoais.

Portanto, a LGPD se alinha com toda a legislação vigente e, de modo coerente e seguro, visa garantir a reparação justa e efetiva à vítima de vazamento indevido de dados, levando em consideração as especificidades dos casos concretos.

REFERÊNCIAS

BARBOSA, Miguel Eyer Nogueira. A responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In* Responsabilidade Civil dos Provedores de Internet (Coord). ISBN 968-65-87823-34-8. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/prefix/15068/3/EBOOK%20-%20Responsabilidade%20civil%20dos%20provedores%20de%20internet.pdf. Acesso em 13 de set. 2023.

BARREDA, Alejandra Ramos.Aceitar cookies pode afetar a segurança dos seus dados. **CNN Brasil**. Disponível em: https://www.cnnbrasil.com.br/tecnologia/voce-deve-aceitar-o-uso-de-cookies-na-internet-e-melhor-voce-pensar-duas-vezes/. Acesso em: 04 de jun. 2023.

BOZZI, Paula da Cunha. Aspectos gerais da responsabilidade civil. **Portal Jus**. [2017] Disponível em: https://jus.com.br/artigos/58301/aspectos-gerais-da-responsabilidade-civil. Acesso em: 10 de abr. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**, de 05 de outubro de 1988. Brasília, DF: Senado Federal. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 10 de jun. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 de abr. 2023.

BRASIL. Superior Tribunal de Justiça. Agravo em Recurso Especial nº 2.130.619 - SP (2022/0152262-2). Segunda Turma, Relator Min. Francisco Falcão. Data de julgamento: 07/03/2023. Data de publicação: 13/03/2023. Disponível em: https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=178204788&registro_numero=202201522622&peticao_numero=&publicacao_data=20230310&formato=PDF&_gl=1*q2110h*_ga*MTAzNzI0MzQ0Ni4xNjgyMjA3OTI2*_ga_F31N0L6Z6D*MTY5NDg3NjM4NS43

LjEuMTY5NDg3NjU1Ny42MC4wLjA. Acesso em: 16 de set. 2023.

FLUMIGNAN, Wévertton Gabriel Gomes. Análise da responsabilidade civil no âmbito do Marco Civil da Internet e da Lei Geral de Proteção de Dados. **Portal Migalhas**. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/343301/responsabilidade-civil-no-ambito-do-marco-civil-da-internet-e-da-lgpd. Acesso em: 10 de set. 2023.

FRANQUEIRA, Guilherme de Souza Costa. O papel da culpa na responsabilidade civil. **Portal da PUC Rio**. Disponível em: http://www.puc-rio.br/pibic/relatorio_resumo2007/relatorios/dir/relatorio_guilherme_franqueira.pdf. Acesso em: 13 de abr. 2023.

GERHARDT, Tatiana Engel e SILVEIRA, DeinseTolfo. Métodos de Pesquisa. **EAD**. Disponível em: http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf. Acesso em: 12 de abr. 2023.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro: Responsabilidade Civil.** 13ª ed. São Paulo: Saraiva, 2018, 04 vol.

Google+ chega ao fim após vazamentos de dados e baixa popularidade. **Techtudo**. Disponível em: https://www.techtudo.com.br/noticias/2019/04/google-chega-ao-fim-apos-vazamentos-de-dados-e-baixa-popularidade.ghtml. Acesso em: 10 de jun. 2023.

LEITE, Ravênia Márcia de Oliveira. A responsabilidade civil e os danos indenizáveis. **ConJur**. Disponível em: https://www.conjur.com.br/2009-set-09/conceito-responsabilidade-civil-danos-indenizaveis. Acesso em 13 de abr. 2023.

Polícia Civil do DF prende hackers suspeitos de vazar 200 milhões de dados pessoais. **Convergência Digital**. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Policia-Civil-do-DF-prende-hackers-suspeitos-de-vazar-200-milhoes-de-dados-pessoais-63494.html?UserActiveTemplate=mobile%2Csite. Acesso em: 18 de jun. 2023.

Polícia prende hackers que vendiam dados de ministros do STF, governadores e deputados.**CNN Brasil**. Disponível em: https://www.cnnbrasil.com.br/politica/policia-prende-hackers-que-vendiam-dados-de ministros-do-stf-governadores-e-deputados/. Acesso em 14 de jun. 2023.

RECUERO, Raquel. **Redes sociais na internet**. Porto Alegre: Meridional, 2009. p. 191.

Relatório de Visão Geral Global Digital 2023. **We Are Social**. Disponível em: https://wearesocial.com/uk/blog/2023/01/digital-2023/. Acesso em: 13 de mai. 2023.

SANTOS, Marco Antonio Fernandes dos. *Segurança na cultura digital. Repositório Institucional*. Trabalho de Conclusão de Curso (Especialização em em Educação na Cultura Digital) - Universidade Federal de Santa Catarina, Santa Catarina, 2016. Disponível em: https://repositorio.ufsc.br/handle/123456789/168731?show=full. Acesso em: 11 de jun. 2023.

Um marco na regulamentação sobre dados pessoais no Brasil. **Superior Tribunal de Justiça**. Disponível em: https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protecao-de-dados-pessoais-lgpd. Acesso em: 20 de abr. 2023.