Scientia et Ratio
ISSN 2525-8532

RESPONSABILIDADE CIVIL DO ENGENHEIRO DE SOFTWARE FRENTE À LEI GERAL DE PROTEÇÃO DE DADOS

SOFTWARE ENGINEER'S CIVIL LIABILITY UNDER THE GENERAL DATA PROTECTION LAW

Artigo submetido em 10 de janeiro de 2023
Artigo aprovado em 22 de janeiro de 2023
Artigo publicado em 01 de junho de 2023

Scientia et Ratio
Ano III – Número 4 – Junho de 2023
ISSN 2525-8532

.

Autor:
Ayrana Maria Brito da Cunha[1]
Markus Samuel Leite Norat[2]

.

RESUMO: Este artigo tem por objetivo apresentar o tema sobre a Responsabilidade Civil conjuntamente com a Lei Geral de Proteção de Dados (LGPD), a qual no âmbito virtual tem por intuito tratar do procedimento de eventos contratuais entre o desenvolvedor e o usuário na base de proteção e comercialização da integridade de dados. A pesquisa em questão tem a finalidade de demonstrar como a modernização do ordenamento jurídico brasileiro se adaptou a este meio, abordando a possível responsabilidade do engenheiro de software nas

eventuais falhas como danos patrimoniais e morais no que tange a propriedade virtual e serviços prestados. De modo específico, a culpabilizar uma certa falha de programação por parte do desenvolvedor partindo da violação de um cuidado de dados, culminando com ressarcimento de danos, gerando uma grande discussão em que essa culpabilização pode ser resguardada com contratos, deixando o profissional virtual menos vulnerável a responsabilidade. A metodologia deste trabalho tem por característica de natureza qualitativa, método de abordagem dedutivo, bibliográfico e documental e de cunho exploratório, à luz de artigos científicos e websites, com o intuito de gerar um debate acerca do amparo jurídico e responsabilidade civil do desenvolvedor com o usuário, seguindo também as normas da Lei Geral de Proteção de Dados (Lei 13.709, de 2018). Esta norma também será utilizada para seguir com entendimento na resolução do seguinte problema da pesquisa, como são aplicadas e definidas a responsabilidade civil diante do desenvolvedor nas ocorrências de falhas de dados.

Palavras – chave: *responsabilidade civil; engenheiro de software; vazamento de dados; LGPD.*

ABSTRACT: This article aims to present the topic of Civil Liability in conjunction with the General Data Protection Law (LGPD), which in the virtual scope aims to deal with the procedure of contractual events between the developer and the user on the basis of protection and commercialization of data integrity. The research in question aims to demonstrate how the modernization of the Brazilian legal system has adapted to this environment, addressing the possible responsibility of the software engineer in any failures such as property and moral damages regarding virtual property and services provided. Specifically, blaming a certain programming error on the part of the developer starting from the violation of data care, culminating in compensation for damages, generating a great discussion in which this blaming can be protected with contracts, leaving the virtual professional less vulnerable responsibility. The methodology of this work is characterized by a qualitative nature, a deductive, bibliographical and documentary approach and exploratory

in nature, in the light of scientific articles and websites, with the aim of generating a debate about the legal protection and civil liability of the developer with the user, also following the rules of the General Data Protection Law (Law 13.709, of 2018). This norm will also be used to follow with understanding in the resolution of the following research problem, how the civil liability before the developer in the occurrences of data failures is applied and defined.

Keywords: civil liability; software engineer; data leakage; LGPD

INTRODUÇÃO

A apresentação deste artigo tem como finalidade abordar a forma de tratamento da proteção de dados pessoais e como a responsabilidade civil está inserida nas atividades que possam violar as diversas legislações de proteção de dados, tanto jurídicas quanto técnicas, em que pode ocasionar danos materiais ou morais na qual tem por ligação os agentes de proteção, assim denominado, o engenheiro de software com o usuário ou a coletividade em questão.

A LGDP (Leis Gerais de Proteção de Dados), que tem por regulamentação a proteção de dados tanto pessoais como gerais, atua gerando uma determinação de informações, e também criando limitações e prazos de utilização virtuais.

Desta forma, ela apresenta uma conjuntiva de direitos e deveres para os indivíduos que exercem a função de tratamento de dados. É importante ressaltar que existe uma complexa relação de múltiplas empresas privadas e até órgãos públicos que encontram diversos desafios para entrarem em conformidade com a LGPD, principalmente os engenheiros de software que são encarregados destes diversos tratamentos de dados, para que evitem os efeitos das sanções administrativas impostas pela ANPD (Autoridade Nacional de Proteção Dados, mas como também por ações jurídicas de responsabilidade civil, criando essa relação jurídica dos danos. Com a eventual intenção de evitar, ou pelo menos prevenir, surgindo nas legislações destinadas acerca da tutela e proteção de dados pessoais na sociedade que vivem em rede (CASTELLS, 2017).

Neste estudo será demonstrado as possíveis causas de vazamentos de dados, as vulnerabilidades do campo digital e as caracterizações de seus eventuais prejuízos, discutindo uma relação ao *quantum* indenizatório na vida dos demais usuários e como são adotadas medidas de segurança padrão previstas e reconhecidas pela LGDP, ou que se encaixe nas hipóteses de inclusão ou exclusão da responsabilidade civil previstas em lei, acerca de normas técnicas que estabelecem certas obrigações em sistemas eletrônicos.

Sendo assim, o objetivo principal deste estudo é mostrar como o sistema do ordenamento jurídico age sob aplicabilidade da responsabilidade civil na LGDP sobre os agentes de tratamento, vulgo, os engenheiros de software, adotadas jurisprudências com informativos atuais na sociedade modernizada.

1. RESPONSABILIDADE CIVIL

A responsabilidade civil trata-se de uma relação de obrigação por reparar eventuais danos causados por outrem em função de um ato por ele praticado, tais como: danos derivados de atos ilícitos, negligência, ofensa ou omissão de direitos. No decorrer do tempo e a modernização da sociedade em si, houve um amplo desenvolvimento jurídico, tanto quanto direitos de indenizações quanto prevenções de possíveis perdas no caso de a responsabilidade decair sobre o indivíduo de uma determinada situação.

Alguns dos elementos nas quais a caracterizam por certas condutas que decaem sobre este conceito jurídico, como a voluntariedade de um ato, o nexo causal que une ao efeito do dano, e por fim, a certeza de que houve lesão ao bem jurídico tutelado privado.

Havendo uma discussão acerca da responsabilidade objetiva ser a padrão nos âmbitos de relações de consumo, na qual consiste que, independente da existência de culpa, o autor da conduta responderá pela reparação do dano. Porém, existe o regime subjetivo na qual estabelece o vínculo lógico entre a ação e o dano sofrido, o nexo de causalidade, levando em conta necessariamente a culpa, violando um dever, seja por negligência, imprudência ou

imperícia.

De acordo com alguns pensamentos de doutrinadores na legislação de proteção de dados, é considerado contraditório a aplicação da responsabilidade objetiva como regra nas aplicações jurídicas em conjunto com a LGDP, em

decorrência de haver diversos fatores previstas em lei que já regulam medidas de adequação.

Com argumentos nas quais a inexistência de dependência da comprovação de culpa poderia levar algumas empresas a deixarem de investir diversos recursos em proteção de dados.

Por outro lado, há o ponto de vista na qual é favorável pela responsabilização protetiva, com teses nas quais estabelecem da possibilidade de uma margem orientada de dados, nas quais, tem riscos de cair em dependências de indivíduos de má-fé gerando um número de violações nas quais podem mudar o rumo de um grande sistema em processamento.

Indicando que o agente de tratamento deva observar a segurança desses dados, reconhecendo seus riscos de atividade, adotando diversas medidas específicas de sua proteção.

Porém, em contrapartida as duas teorias, uma responsabilidade ativa é vista como uma terceira alternativa no que tange a sua aplicação nos tribunais, na qual não é tratada pelas regras da teoria clássica acima citadas, neste novo regime é determinado que não é somente o cumprimento dos artigos da lei estão em questão, mas sim a forma que o agente deve comprovar que suas medidas de segurança têm eficácia e estão de acordo com a norma. Seguindo literalmente os Artigos 42 e 43, da LGPD.

Vejamos alguns doutrinadores que aderem a responsabilidade ativa em contradição aos debates doutrinários entre os regimes subjetivistas e objetivistas.

Fato é que ao analisar uma obrigação de indenização de um eventual dano, os tribunais determinem a violação à norma prevista e o nexo causal, podendo os agentes demonstrarem que não houve dano a norma e que a atividade não se realizou ou que decorreu de um resultado de culpa exclusiva de um terceiro. (MENDES, 2019.)

A Lei de Proteção de Dados Pessoais é muito calcada na perspectiva de risco. Isso significa dizer que você pode e deve esperar mais daqueles agentes de tratamento de dados pessoais cujas atividades têm um risco maior. Ou seja, o peso da lei vai ser calibrado de forma intensa para quem, por exemplo, trata dados pessoais sensíveis em larga escala. (BIONI e DIAS 2020, p 09 n 3)[3] . Questionando a uma pauta de debate no quesito binário dos dois regimes de responsabilidade, conforme:

‘’A doutrina brasileira tem focado a sua atenção em responder essencialmente uma pergunta: se o regime da responsabilidade é objetivo ou subjetivo. Por mais relevante que isso seja, não é essa questão que deve pautar o debate. Tal pergunta parece partir de uma premissa falsa de dualidade de regimes jurídicos de responsabilidade, objetiva ou subjetiva. Mais importante do que essa tentativa de classificação binária de responsabilidade, se objetiva ou subjetiva, é analisar mais de perto e, em detalhes, os elementos normativos que restringiriam ou alargariam a discussão de culpabilidade para fins de responsabilização no tratamento de dados pessoais. Ainda que a LGPD tenha esculpido um regime de responsabilidade civil subjetiva, as barreiras para a deflagração do dever de indenizar foram substancialmente diminuídas.’’ (BIONI, 2020, p 9)

É importante destacar que em ambos os pensamentos que têm razoabilidade no conceito de não fugir da culpabilidade e da responsabilidade, em que as medidas de segurança e possíveis prevenções têm de ser definitivas e consideráveis, não sendo uma mera regra vulnerável com grande risco de ser violada.

Seguindo uma premissa do Artigo 44, possuindo noção ampla acerca do tratamento irregular

em relação quando são observadas violações à legislação ou quando não for fornecida medidas de segurança de dados que são esperadas, ressaltando, a ampliação do conceito de culpa com finalidade de desenvolver a responsabilidade sob os agentes de tratamento de dados.

Dessa forma, está sendo desenvolvida uma maturidade cada vez maior no enfoque de desenvolvimento no mercado de software transformando uma aplicação de qualidade envolvendo a engenharia, que refletirão sobre as atividades que podem gerar responsabilização no profissional de informação, com pretensão de evitar maior erro do desenvolvedor, corrigindo e solucionando erros de programação ou bugs pelo engenheiro contratado.

1.1 RESPONSABILIDADE DO ENGENHEIRO DE SOFTWARE

A construção de um software leva uma série de fatores para seu processamento, sejam elas a funcionalidade e os tipos de suas restrições que devem ser determinadas, o projeto incluído na qual deve atender às especificações anteriores estabelecidas, a sua validação em atingir as solicitações dos clientes, e por fim, as suas mudanças de versões de acordo com as necessidades dos usuários clientes.

O respeito pelo cliente quanto na preservação e zelo da produção de software é totalmente fundamental, na qual é necessário a utilização de processos

de testes e instrumentos adequados, para prevenir falhas em decorrências de negligências que cause danos. (NAZARENO, 2009)

É aqui que se estabelece os cuidados do engenheiro de software, caracterizado como a pessoa indicada para servir na atuação dos canais de comunicação, nos termos do artigo 5º, da LGPD, em que é determinada o tratamento dos dados de acordo com os princípios estabelecidos em lei.

No que diz respeito às obrigação definir um ‘‘DPO’’ (*Data Protection Officer*)[4] função criada pelo responsável da proteção de dados coletados dentro de alguma organização, devendo ser um canal de contato em casos de problemas por não atender os requisitos da LGDP e seus princípios.

Reservando um *budget* nas quais investem para a qualquer mudança das suas versões de proteção atendendo e se adaptando o que for de necessidade a coletividade dos usuários em massa. Havendo um contrato de software com cláusulas claras das suas responsabilidades como desenvolvedor com o usuário em relação aos tratamentos de exportação e importando dos dados seguindo os termos da lei.

No que concerne os contratos, os mesmos devem incluir ressalvas de licenças de uso em que o sistema normalmente disponibiliza suas atualizações pelo criador do software, assim como o seu código fonte para garantir seu suporte, e o seu desenvolvimento interno, criando consentimentos expressos no contrato implantadas no sistema atendendo aos requisitos legais, havendo testes de validação à LGPD dos registros de acesso.

Nos requisitos de acordo com a lei estabelecer relatórios de impacto de proteção de dados, resumidamente, um estudo de vulnerabilidade, desenvolvendo um plano de contingência, saber como agir em determinadas situações como esta. (TOMASEVECIUS, 2021).

A referência à privacidade, outra responsabilidade importante é os relatórios com dados pessoais identificadas do usuário, é possível o riscos de vazamentos através do cliente. O que se verifica é que as funções e relações particulares que devem possuir uma certa assimetria entre o titular e o agente controlador/operador irão adentrar inúmeras incidências processuais e protetivas disciplinadas pela LGPD. Em vista disso, devendo auxiliar para evitar possíveis ações de responsabilidade.

1.2 CASOS DE AÇÃO JUDICIAL EM NEGLIGÊNCIA DE SOFTWARE

É muito comum a frequência de falhas graves que comprometem uma instalação e funcionamento de um software, havendo por resoluções as mediações dos contratantes em relação a implementação de um novo sistema.

Entretanto, há casos que devido ao tamanho do problema e a demora de ser solucionada recaem para o caminho da rescisão de contrato e do ressarcimento de danos pelo amparo do âmbito judicial, que custa menos e a maioria das vezes são vantajosas. As rescisões de contrato de forma judicial são vantajosas em relação a custos e obtém vantagem sobre o autor da ação no quesito de provas acerca de instalações ou desenvolvimentos mal feitos ou não realizados pela empresa contratada.

São adotadas em fundamentos jurídicos a aplicação nos casos em que a rescisão é buscada antes do prazo final de implementação do software, ou seja, o contrato não chegou ao termo final em decorrência de se mostrar evidente que a fornecedora não terá serventia na conclusão de instalação no prazo estipulado. Esta ruptura da relação contratual repentina obriga o próprio fornecedor, que tem por culpa, a indenizar as perdas e os lucros cessantes sofridos pela contratante.

Outra tese adotada pela doutrina que viabiliza a rescisão é o cumprimento não satisfatório do contrato, ou seja, o software adquirido não cumpre a finalidade na qual foi contratada, não suprindo a necessidade da empresa contratante em decorrência de ‘’bugs’’ e diversas falhas constantes. Havendo total frustração pelo adquirente, dando-lhe direito de buscar ressarcimento no abatimento do valor pactuado e na multa prevista no contrato.

Exemplos disso são os casos encontrados nos tribunais de rescisão de contrato de software, entre eles está no processo nº. 1005180-15.2021.8.26.0011, julgados no Tribunal de São Paulo, na qual a empresa que ajuizou a ação é a fornecedora do software em relação a empresa contratante, em que foi afirmada inadimplemento por parte da contratante, porém a mesma começou a sofrer diversos problemas de funcionamento e não houve correção do

software devido a uma extensa demora. Agindo assim, o entendimento do tribunal deu improcedência aos pedidos da fornecedora dando total isenção a empresa que contratou os serviços. (TRIBUNAL, 2022)

É cabível o inadimplemento antes da hora estipulada, caso o devedor não cumpra ou pratique ações contrárias ao cumprimento do contrato ou declarações neste sentido, contra a prestação na qual possa se deduzir que os dados objetivos existentes não haverá o seu cumprimento. Sendo assim, o autor poderá distribuir uma ação de resolução. (AGUIAR JÚNIOR, 2015).

Sendo assim, é evidente que há um precedente centralizado na justiça, na qual por consequências de vitórias tem por razão certos questionados advindos por parte de clientes e fornecedores, portanto a defesa judicial na prevenção de blindar o contundente em todos os casos é fundamental no quesito de resguardar.

2. VAZAMENTO DE DADOS

No maior convívio e a extrema dependência das informações de dados no cotidiano, considerando até como uma sobrevivência e identidade nos meios atuais. Um dos maiores prejuízos da modernidade consiste no próprio vazamento de dados derivada de falhas de seguranças geradas pelo próprio sistema e não averiguadas pelos agentes de tratamentos. O que é bastante comum, em diversos casos, abrangendo inúmeros dados desde biometria até dados bancários. Sendo um dano com caráter de efeito dominó, pois tem potencial de alcançar outras informações de um mesmo usuário em cadeia, fazendo-o refém de indivíduos de más intenções para exploração de seus dados, como para golpes financeiros, extorsões e tentativas de prejudicar os negócios e a imagem de uma pessoa ou empresa.

Informações sobre vazamentos vêm de sites privados, e a lei determina a responsabilidade de relatar incidentes de segurança como este à Agência Nacional de Proteção de Dados.(TOMASEVECIUS, 2021) Sendo assim, o vazamento de informações é caracterizado

uma violação ao rol de direitos do usuário titular, que em futuro, tem por configuração a um princípio de um dano moral com cumulação de dano material, caso o exercício do direito que foi violado tenha o típico dano emergente ou lucro cessado.Exemplo disto, é o tratamento de dados pessoais sem o consentimento do usuário ou fora das normas previstas, na qual um deles é mais conhecido como ‘’*spam*’’, cuja propaganda não solicitada de forma abusiva e abrangente ocorre freneticamente nas caixas eletrônicas de usuários, sendo revista pela LGDP.

O desígnio da LGPD em relação aos vazamentos de informações só é visado dados pessoais, ou seja, dados que levam a identificação de uma pessoa ou ligações de um todo que levam a único ponto de informação.

Havendo um caso de incidente de segurança, o engenheiro designado tem por obrigação avaliar no erro do software se o incidente tem chances de riscos ou danos de efeito em cadeia aos seus titulares de maior relevância. O que no caso de vazamento de dados pessoais já é considerado de suma importância e caráter grave, em decorrência da exposição para terceiros, o que pode surgir o acesso de imediato e o prejuízo ocorrente ao titular.

Tais consequências de um possível vazamento para uma empresa cujo tem a típica de agentes de tratamento é sofrer a responsabilização imposta por ações judiciais por parte dos titulares, sanções administrativas, perdas de quebras de contratos por fuga de informações relevantes, entre demais fatores que possam levar ao prejuízo danoso.

Os principais ataques maliciosos que visam sequestrar dados para fins de extorsão, e que são executadas através de credenciais roubadas ou comprometidas por erro de sistema vulnerável, falha em infraestrutura em nuvem, erros e *bugs* por falta de complemento no desenvolvimento da programação do software e *phishing.**[5]***

Uma das medidas em ocorrências de incidentes determinadas pela LGPD é que o engenheiro deve fazer a comunicação para a ANPD (Autoridade Nacional de Proteção de Dados) e ao

titular dos dados. Havendo descrição completa das informações vazadas, as medidas técnicas e de segurança adotadas pelo engenheiro na correção e solução da ocorrência para mitigar os efeitos dos danos.

Aplicadas também sanções interpostas pelo LGPD ao ter infrações à lei de sua forma geral, seja elas como: multa simples ou diária, a publicação do ato cometido, bloqueio geral dos dados pessoais e sua eliminação, suspensão das atividades de tratamento feito pelos agentes ou proibição parcial ou total. De acordo com os critérios previstos em lei, para fins de adoção de mecanismos internos com objetivos de correção adequado para os dados violados.

De acordo com o advogado, Renato Veiga, na qual caracteriza essas possíveis soluções na questão da imprevisibilidade nas consequências de erro:

‘’Caracterizar melhor os contratos, diferenciando contratos de meio (licenciamento, provimento de acesso) e contratos de fim (processamento, desenvolvimento,etc); Enfatizar a possibilidade de falhas e impor ao usuário o dever de conferência de resultados e de manter esquemas alternativos; Usar o mecanismo de preços para dosar a responsabilidade (menor preço, responsabilidade limitada).’’(RENATO, 2005, p.9)

As principais forma de evitar esses tipos de incidentes é a inclusão de medidas de forma adequadas de segurança de informação para entrar em conformidade com a LGDP, gerando diversos protocolos para criar um software de controle em relação a erros de programação que possam levar estes vazamentos, monitoradas por engenheiros que tendem a inspecionar grandes demandas no desenvolvimento rápido de novos sistemas.

3. LEI 13.709/2018 – Lei Geral de Proteção de Dados (LGPD)

Legislação visada em proteger a privacidade de cidadãos e sua liberdade na qual são usuários por todo tipo de sistema fornecidas pela modernidade. Em que regulamenta que

empresas e órgãos públicos tenham medidas de armazenamento, coleta e uso de dados gerais de pessoas no âmbito da segurança da informação.

Estabelecendo regras nas quais o usuário titular terá direitos em cima de seus dados gerenciadas por empresas que estão caracterizadas como agentes de tratamentos em determinados sistemas.

O número de casos de vazamentos conforme anteriormente exemplificadas gerou um fator relevante na preocupação de dados com riscos de invasão de privacidade e eventuais ataques, e como deveriam ser tratadas em questão de reparação e prevenção em relação aos impasses sobre o uso e proteção desses dados.

Fator essencial para garantir aos clientes das empresas que utilizam para prestação de um determinado serviço as informações pessoais sejam acordadas de

forma transparente a sua finalidade de armazenamento devidamente comprovadas. Mudando completamente a forma de gestão de arquivos e contratações de profissionais das informações no investimento de segurança. Garantindo a esses indivíduos o direito de responsabilizar qualquer eventual dano.

Estabelecida no Artigo 5º, inciso X da Constituição Federal na qual condiz: ‘’ *Inviolabilidade da honra, intimidade, imagem e vida privada, assim como o direito do cidadão à proteção de seus dados íntimos e pessoais*.’’ A LGPD norma em que consiste a garantia ao respeito à privacidade em geral.

Tratando-se da responsabilidade não tem por tamanha certeza qual regra ser adotada o agente de tratamento terá, dependendo dos casos encontrados poderá ser utilizada tanto a objetiva quanto subjetiva, ou surgindo de terceiras vias por meio de entendimentos doutrinários. Está regulamentada no Art. 5º, VI a IX, da LGPD, servindo como resposta pelos danos decorrentes da violação de dados, na qual é encontrada em situações de violações de

normas jurídicas e técnicas sobre a segurança e proteção de dados em geral se ocasionar dano material ou moral.

Em relação a competência as infrações da LGPD serão julgadas pela Justiça Comum, com exceção os casos trabalhistas.

Os requisitos para que o engenheiro de software desenvolva sistemas sem sofrer qualquer sanção no momento de coleta e processamento de acesso a dados impostas pela LGDP.

Um dos principais é a finalidade na qual os dados serão coletados e como serão tratados visando a ter fins legítimos e de total conhecimento do titular, sofrendo punição pela legislação de proteção de dados se fugir do propósito, exemplo disso é a mudança de dados para outro uso totalmente diferente.

Outro princípio interposto é a adequação que as informações serão analisadas de forma compatível com a finalidade do exemplo anterior citada, seguindo outro princípio do livre acesso na qual o usuário terá totalidade das informações e de forma gratuita em que a qualquer momento pode solicitar a exclusão desses dados de forma imediata.

Portanto, conjugando a adequação da lei a um novo cotidiano gerando uma mudança completa de cultura nas demais empresas privadas e órgãos públicos que mexem com os dados da coletividade sem qualquer supervisão. Havendo uma garantia da lei para os titulares a liberdade de informações de forma segura.

4. ENTENDIMENTOS DOS TRIBUNAIS DA RESPONSABILIDADE CIVIL NA LGPD

É de se relatar que os entendimentos doutrinários ou jurisprudências presentes nos tribunais acerca do volume de ações judiciais envolvendo sobre indenizações em cima de vazamento de dados.

Havendo uma grande quantidade de decisões antagônicas, não havendo uma regra favorável

acerca do tema. Entretanto, muitas decisões vão pelo lado de que uns simples vazamentos não configuram dano, não gerando qualquer dever de indenizar pelo agente de tratamento. Seguindo de forma exemplificativa alguns entendimentos providos do TJSP:

“Ausência de provas, todavia, de violação à dignidade humana da autora e seus substratos, isto é, liberdade, igualdade, solidariedade e integridade psicofísica. Autora que não demonstrou, a partir do exame do caso concreto, que, da violação a seus dados pessoais, houve a ocorrência de danos morais. Dados que não são sensíveis e são de fácil acesso a qualquer pessoa” (Apelação Cível 1000794- 59.2021.8.26.0554).’’

‘’ Conclui-se que tais informações, embora pessoais, não podem ser classificadas como sensíveis, porque não guardam pertinência com as liberdades individuais consagradas pela Constituição Federal, origem social e étnica, patrimônio genético ou orientação sexual, limitando-se a dados objetivos e claros voltados exclusivamente para a avaliação da situação econômica e análise de risco do apelante junto ao mercado de consumo, mostrando-se descabida a pretensão, mesmo sob a ótica do Código de Defesa do Consumido (TJSP, Apel.1042119-61.2021.8.26.0506, Rel. Des. RUY COPPOLA, 32ª Câmara de Direito Privado, j. 18/05/2022).’’

Considerando pelos relatores sobre a questão da sensibilidade que pode ou não atingir acerca do patrimônio ou dignidade da pessoa. Levando em questão a relatividade que os vazamentos de dados podem acarretar em coletividade sobre danos patrimoniais ou morais, dependendo ainda a critério dos magistrados. Mesmo a LGPD ser a salvaguarda dos direitos fundamentais, principalmente da liberdade e privacidade dos titulares.

Há exceções na qual um dado pessoal não é protegido pela LGDP, indo de acordo com o entendimento da maioria dos magistrados que não consideram a responsabilidade para arcar com os danos. De acordo com o artigo 4º, inciso I, da LGPD, tratando de dados com intuito somente particular sem fins econômicos não possui amparo legal ou tratar somente de dados

de pessoas jurídicas sem envolver qualquer manipulação de dados de pessoa física daí não existirá relação de aplicabilidade da LGPD.

5. CONSIDERAÇÕES FINAIS

Diante do entendimento, acerca da utilização de dados pessoais e seu tratamento, como é manifestada na sociedade que necessita dessa utilização. De como é importante o aprofundamento das regras da LGPD e demais regulamentos em relação ao software seja de maior conhecimento dos engenheiros operadores em questão. Sendo necessária, a sua compreensão tanto por parte do titular dos dados, quanto para o operador, por fim ter o dever de defender os seus direitos em juízo e para prevenção e minimização da responsabilidade de eventuais conflitos no tratamento de dados pessoas virtuais.

Surgindo assim, uma conjugação na adequação da lei no quesito de transformação e adequação na sociedade moderna e desenvolvimento econômico e social nas empresas e órgãos públicos. Gerando total proteção para ambas as partes e instruções essenciais para uma boa relação contratual dos provedores e titulares.

Em que esta pesquisa visa inicialmente mostrar no que foi proposto: a aplicabilidade da responsabilidade civil aos agentes operadores de dados diante das diversas modalidades de responsabilidade e seus informativos jurisprudenciais adotadas atualmente. Verificou-se que, em virtude de análise protetiva, no quesito de ser alvo de tratamento de dados, a responsabilidade ser abordada tanto no quesito objetivo ou subjetivo, partindo até de uma terceira via em que é aplicada a partir da comprovação ou não da eficácia do sistema do processamento de dados pelo agente, sendo analisada em que se deve ser imposta ou não a responsabilidade civil.

Delimitada acerca da responsabilidade do engenheiro de software no quesito de tratamento de dados e suas especificações contratuais com os titulares dos dados, seguindo os princípios estabelecidos pela LGPD, tais como as licenças de uso com intuito de garantir o

código de fonte para desenvolvimento do sistema específico contratado e seu suporte para eventuais falhas, havendo ressalvas tanto para o agente de tratamento quanto para o seu contratante. Gerando a discussão de como é averiguada os possíveis vazamentos em maior relevância de risco de efeito dominó em decorrência de negligência por parte da fornecedora do software, recaindo a rescisão contratual e ressarcimento de danos e perdas por conta do nível de prejuízo analisada pela ruptura contratual ou do seu não cumprimento, apelando pelo âmbito judicial.

Apesar disso, os riscos eminentes nas atividades de tratamento de dados em que os agentes e os titulares sofrem cotidianamente em virtude de diversas transformações na qual a tecnologia da informação e comunicação trazem no estilo de vida adentrada na sociedade de forma facilitadora, trazendo consigo uma vasta variedade de meios que necessitem de informações tanto transparentes como ocultas. Entre várias coisas, os entes particulares em conjunto com os órgãos públicos que utilizam desse meio digital, possam garantir uma forma de minimizar as consequências da responsabilidade civil na qualidade de culpa em decorrência das diversas falhas de software partindo da premissa de resguardar tanto o agente que desenvolve quanto a quem fornece os dados, havendo o suporte assistencial em cláusulas contratuais, como também seguindo os requisitos que a Lei Geral de Proteção de Dados (LGPD) impõe como forma de garantir este meio.

REFERÊNCIAS

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. 4. ed. São Paulo: Saraiva, 1990.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

HOEPERS, Cristine; STEDING-JESSEN, Klaus. **Fundamentos de Segurança da Informação**. [S. l.]: Escola de Governança da Internet no Brasil. Disponível em: https://bit.ly/2unOasd.

Acesso em: 03 out. 2022.

IMPERVA (EUA). **Phishing attacks: What is a phishing attack**. In: Phishing attack examples. [S. l.], 22 maio 2022. Disponível em: https://www.imperva.com/learn/application-security/phishing-attack-scam/ . Acesso em: 3 out. 2022

Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm . Acesso em: 12 out.2022.

MACHADO, Victor. **Os 10 princípios da LGPD que você usuário precisa saber!**: LGPD, COMPLIANCE, ÉTICA EMPRESARIAL. [*S. l.*], 22 jul. 2019. Disponível em:

https://www.victormachadoadv.com/news/2019/7/22/os-10-princpios-da-lgpd-que- voc-usurio-precisa-saber . Acesso em: 12 out. 2022.

MACHADO, Victor. **A LGPD e o desenvolvedor de software 16 aspectos práticos na sua atuação**. [S. l.], 8 nov. 2019. Disponível em: https://www.victormachadoadv.com/news/2019/11/18/a-lgpd-e-o-desenvolvedor-de-software-16-aspectos-prticos-na-sua-atuao . Acesso em: 12 out. 2022.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira**. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018**. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e as suas repercussões no Direito Brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

PEREIRA, Caio Mario da Silva. **Responsabilidade Civil**. 12. ed. rev. atual. ampl. Rio de Janeiro: Forense, 2018. Ebook. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530980320/ . Acesso em: 03 out.

2022

STOCO, Rui. **Tratado de Responsabilidade Civil**. 7. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2007.

SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. **Fundamentos Jusfilosóficos e Âmbito de Proteção do Direito Fundamental à Proteção de Dados Pessoais**. Direito Público, [S.l.], v. 17, n. 93, jul. 2020. Disponível em: https://portal.idp.emnuvens.com.br/direitopublico/article/view/4315 Acesso em: 12 out. 2022.

TORCHIA, Bruno Martins; MACHADO, Tacianny Mayara Silva. **A responsabilidade subjetiva prevista na Lei Geral de Proteção de Dados e a relação jurídica entre o controlador e o encarregado de proteção de dados**. In: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coord.). LGPD e administração pública: uma análise ampla dos impactos. São Paulo: Thomson Reuters, 2020. Ebook. Disponível em:https://proview.thomsonreuters.com/launchapp/title/rt/monografias/246338257/v1

/page/RB-46 Acesso em: 13 out. 2022.

VAINZOF, Rony. Disposições Preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Lei Geral de Proteção de Dados Comentada**. 2. ed. rev., atual e ampl. São Paulo: Thomson Reuters Brasil, 2020

WESENDONCK, Tula. A responsabilidade civil pelos riscos do desenvolvimento: evolução histórica e disciplina no Direito Comparado. Revista Direito & Justiça. Porto Alegre, v. 38, n. 2, p. 213-227. jul./dez. 2012. Disponível em: https://revistaseletronicas.pucrs.br/index.php/fadir/article/view/12549/8412 Acesso em: 03 out. 2022.

ZERO-DAY **vulnerability: what it is, and how it works**. Norton, [s. l.], [s. d.]. Disponível em: https://nr.tn/2G7038G . Acesso em: 03 out. 2022.

[1] Graduada em Direito pelo Centro Universitário de João Pessoa – UNIPÊ. Pós-graduanda em Direito Processual Civil pela Faculdade Gran.

[2] Doutorando em Ciências Jurídicas e Sociais. Mestre em Direito e Desenvolvimento Sustentável pelo Centro Universitário de João Pessoa – UNIPÊ. Especialização em Direito da Seguridade Social – Previdenciário e Prática Previdenciária. Especialização em Advocacia Extrajudicial. Especialização em Coordenação Pedagógica. Especialização em Direito da Criança, Juventude e Idosos. Especialização em Direito Educacional. Especialização em Tutoria em Educação a Distância e Docência do Ensino Superior. Especialização em Direito do Consumidor. Especialização em Direito Civil, Processo Civil e Direito do Consumidor. Especialização em Direito do Trabalho e Processual do Trabalho. Formação Pedagógica em andamento em Geografia. Formação Pedagógica em andamento em Ciências Biológicas. Graduação em Direito. Editor de Livros, Revistas e Sites. Advogado. Coordenador Pedagógico e Professor do Departamento de Pós-Graduação em Direito do Centro Universitário de João Pessoa – UNIPÊ; Professor convidado da Escola Nacional de Defesa do Consumidor do Ministério da Justiça; Professor do Curso de Graduação em Direito no Centro Universitário de João Pessoa – UNIPÊ; Membro Coordenador Editorial de Livros Jurídicos da Editora Edijur (São Paulo); Membro Diretor Geral e Editorial das seguintes Revistas Científicas: Scientia et Ratio; Revista Brasileira de Direito do Consumidor; Revista Brasileira de Direito e Processo Civil; Revista Brasileira de Direito Imobiliário; Revista Brasileira de Direito Penal; Revista Científica Jurídica Cognitio Juris, ISSN 2236-3009; e Ciência Jurídica; Membro do Conselho Editorial da Revista Luso-Brasileira de Direito do Consumo, ISSN 2237-1168; Autor de mais de 90 livros jurídicos e de diversos artigos científicos.

[3] MENDES, Laura Schertel. Contexto internacional e economia de dados pessoais; histórico da implementação da regulamentação europeia de proteção de dados (GPDR); Marco Civil da Internet, Código de Defesa do Consumidor e Cadastro Positivo; Lei Geral de Proteção de

Dados (LGPD) e Medida Provisória 869/2018. São Paulo: Escola da Defensoria Pública, 13 jun. 2019. Palestra proferida no Curso sobre a Lei Geral de Proteção de Dados

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais:construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor.Civilistica.com. Rio de Janeiro, a. 9, n. 3, 2020. Disponível em:<http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/>. Data de acesso.

Art. 44, LGDP – […]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[…]

[4] DPO – Diretor de proteção de dados, encarregado pela proteção de dados Budget – gestão de orçamentos O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA, (UE). O Regulamento Geral sobre a Proteção de Dados. 119. [S. l.], 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal- content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 3 out. 2022.

[5] IMPERVA (EUA). Phishing attacks: What is a phishing attack. In: Phishing attack examples. [S. l.], 22 maio 2022. Disponível em: https://www.imperva.com/learn/application-security/phishing-attack-scam/. Acesso em: 3 out. 2022. Phishing -é um tipo de engenharia em que um invasor envia uma mensagem fraudulenta (por exemplo, falsificada, falsa ou enganosa) projetada para induzir uma pessoa a revelar informações confidenciais ao invasor [1] ou implantar software malicioso na infraestrutura da vítima. crime de enganar as pessoas para que compartilhem informações confidenciais como senhas e número de cartões de crédito. Como em uma verdadeira pescaria.