ASSOCIAÇÃO CARUARUENSE DE ENSINO SUPERIOR
CENTRO UNIVERSITÁRIO TABOSA DE ALMEIDA - ASCES/UNITA
BACHARELADO EM DIREITO

MARIA CICILIA ALVES SERCUNDES
MARIA VITÓRIA FRANÇA SILVA
REBECCA BEATRIZ DE OLIVEIRA FÉLIX

ANÁLISE DA RESPONSABILIDADE CIVIL APLICADA NAS DECISÕES DE CRIMES POR VAZAMENTO DE DADOS PESSOAIS SOB A ÓTICA DA LEI N.º 13.709/2018 - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

CARUARU
2023

ANÁLISE DA RESPONSABILIDADE CIVIL APLICADA NAS DECISÕES DE CRIMES POR VAZAMENTO DE DADOS PESSOAIS SOB A ÓTICA DA LEI N.º 13.709/2018 - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Trabalho de Conclusão de Curso apresentado ao Centro Universitário Tabosa de Almeida (ASCES-UNITA) como requisito parcial para obtenção do Título de Bacharéis em Direito.
Orientador: Prof. Msc. Saulo Silva de Miranda

CARUARU

2023

RESUMO

O presente estudo analisa como a legislação brasileira e o poder judiciário tem lidado com o novo cenário de crimes virtuais, especificamente as irregularidades no tratamento de dados pessoais tutelado pela Lei Geral de Proteção de Dados Pessoais. Levando em consideração a ausência da completude na aplicação da responsabilização dos agentes pela Autoridade Nacional de Proteção de Dados (ANPD) vez que o órgão tem como dever fiscalizar e aplicar sanções, entretanto, ainda não teria regulamentado a metodologia para aplicação das penas por vazamento de dados. Dessa forma, através de uma análise bibliográfica, busca-se consolidar o entendimento de como tem sido a atuação dos magistrados. Tendo em vista a interpretação de responsabilidade civil na lei de dados que causa divergência entre doutrinadores, percebe-se que nos tribunais a supremacia na aplicação tem se dado de forma objetiva, ao passo que o Código de Defesa do Consumidor é utilizado quando as decisões litigam sobre relações de consumo, nestes casos, é possível perceber a predominância da responsabilidade objetiva nas decisões, entretanto, ainda há decisões que entendem que a responsabilidade civil seria subjetiva. Neste contexto, faz-se necessária a presente discussão vez que a dualidade quanto a responsabilidade civil na Lei Geral de Proteção de Dados tem sido uma das grandes discussões desde o advento da lei, tanto entre os doutrinadores quanto nos tribunais, dessa forma tem-se um cenário instável quando da aplicação das penalidades ocorridas pelos crimes por vazamentos de dados.

Palavras-chave: LGPD; ANPD; Agentes de tratamento; Dados Pessoais; Crimesvirtuais.

ABSTRACT

The present study analyzes how the Brazilian legislation and the judiciary have been dealing with the new scenario of virtual crimes, specifically the irregularities in the processing of personal data protected by the General Law for the Protection of Personal Data. Taking into account the lack of completeness in the application of the accountability of agents by the National Data Protection Authority (ANPD) since the body has the duty to supervise and apply sanctions, however, it would not have regulated the methodology for applying penalties for data leakage data. In this way, through a bibliographical analysis, we seek to consolidate the understanding of how the magistrates have been acting. Bearing in mind the interpretation of civil liability in the data law that causes divergence among scholars, it is clear that in the courts the supremacy in the application has been given objectively, while the Consumer Protection Code is used when the decisions litigate regarding consumer relations, in these cases, it is possible to perceive the predominance of objective responsibility in decisions, however, there are still decisions that understand that civil responsibility would be subjective. In this context, the present discussion is necessary since the duality regarding civil liability in the General Data Protection Law has been one of the great discussions since the advent of the law, both among scholars and in the courts, thus an unstable scenario when applying the penalties incurred for crimes due to data leaks. Keywords: LGPD; ANPD; treatment agents; Personal data; Virtual crimes.

SUMÁRIO

1. INTRODUÇÃO

Tendo em vista o avanço no recolhimento de informações pessoais, graças à amplitude do ambiente virtual, observou-se que a utilização desses dados estavam ocorrendo para prática de ilícitos com informações obtidas de forma criminosa, conhecido como *phishing*, que se concretiza quando o golpista se passa por um funcionário de operadora ou instituição financeira, por exemplo, e realiza o roubo aos dados pessoais da vítima, manipulando-a a informar seus dados pessoais, acessando dessa forma redes sociais, aplicativos de bancos e etc.

O problema nisso tudo é o enorme risco de utilização desses dados pessoais, muitas vezes colhidos sem o consentimento de seus titulares (ROQUE, 2021). Autores entendem que, nesse caso, se os cidadãos não conseguem saber nem mesmo os dados que são coletados, têm dificuldades ainda maiores para compreender as inúmeras destinações que a eles pode ser dada e a extensão do impacto destas em suas vidas (FRAZÃO, 2021).

Na medida em que as violações às pessoas cresciam na sociedade, principalmente no ambiente virtual, surge a necessidade de proteção jurídica que resguardasse os dados pessoais destes usuários.

O desenho da responsabilidade civil na Lei n° 13.709/18, a Lei Geral de Proteção de Dados é discutida na doutrina brasileira por autores que enxergam falhas e omissões na redação da lei que podem atrapalhar na interpretação em busca de um sentido completo e capaz de cumprir com seu objetivo no tecido normativo brasileiro.

O estudo leva em conta a vulnerabilidade do usuário e busca entender como os tribunais interpretam os crimes virtuais e como aplicam a responsabilização do agente de tratamento dos dados em um caso de vazamento dos dados pessoais.

Assim como traz à tona a figura da ANPD, órgão responsável por fiscalizar e aplicar penalidades em caso do não cumprimento da lei, entretanto, observou-se que passados quase três anos desde a LGPD, o órgão ainda não teria regulamentado a metodologia para aplicação das penas por vazamento de dados, o que certamente resultou em interpretações dúbias quanto à efetividade da aplicação das sanções.

Ao fim, após análise da aplicação dos artigos 42 e 43 da Lei de Geral Proteção de Dados em jurisprudências, a conclusão é de que a dualidade na interpretação é uma opção do legislador como um incentivo para a devida adequação das empresas à LGPD, que, se adequadas, sempre levam a uma visão de exclusão da culpabilidade na responsabilidade subjetiva.

Quanto ao órgão de fiscalização, Autoridade Nacional de Proteção de Dados, é indiscutível a necessidade de uma efetiva participação na fiscalização e aplicação das devidas

sanções, vez que uma falha nesse órgão importa diretamente na impunidade do agente responsável pelo vazamento de dados, até o presente momento, a ANPD não se encontra participante ativa nas decisões envolvendo esse tipo de ilícito.

Todavia, nas decisões analisadas, o caminho nos leva a ótica da responsabilidade civil objetiva aos agentes, por se tratar diretamente de relações de consumo, decisões que, poderiam ter tomado um rumo diverso e específico com a devida aplicação das sanções fiscalizatórias da ANPD.

2. CONSIDERAÇÕES SOBRE OS ILÍCITOS DIGITAIS

Para a finalidade desse artigo, é necessário um entendimento preliminar acerca dos crimes virtuais. Diante da evidente expansão dos novos "espaços" sociais, nos deparamos com a prática de condutas ilícitas com frequência na internet, principalmente quando falamos de dispositivos móveis, tais como aparelhos celulares, computadores, que estão cada vez mais presentes no nosso cotidiano.

Os tipos de crimes cibernéticos vão incluir: fraude por e-mail e pela internet; fraude de identidades (onde informações pessoais são roubadas e usadas); roubo de dados financeiros ou de pagamento com cartão; roubo e venda de dados corporativos; ciberextorsão (exigir dinheiro para evitar um ataque ameaçado); ataques de *ransomware* (um tipo de ciberextrusteio); *cryptojacking* (onde hackers exploram criptomoedas usando recursos que não possuem); espionagem cibernética (onde hackers acessam dados do governo ou de uma empresa); interferência em sistemas de modo a comprometer uma rede; violação de direitos autorais; jogos de azar ilegais; venda de itens ilegais on-line; incitação, produção ou posse de pornografia infantil. (KARPERSKY, 2022).

Tais crimes, sendo os mais comuns no Brasil são os de furto e compartilhamento de dados, crimes contra honra e estelionato virtual, estão em crescimento constante e serão os crimes abordados no estudo.

De acordo com o relatório da Accenture os ataques de segurança aumentaram 31% de 2020 a 2021, repercutindo no resultado de 206 para 270 ataques por empresa.

A *Javelin Strategy & Research* publicou um estudo sobre golpes de fraude de identidade e fraude de empréstimo, *Identity Fraud Study* (Estudo sobre fraude de identidade) em 2021, constatando que as perdas por fraude de identidade no ano totalizaram US$ 56 bilhões, particularmente na pandemia, onde se verificou uma maior imersão das pessoas aos meios de interação por telefone, mídias sociais etc.

Vemos o impacto desses crimes quando acarretam danos financeiros bem como a perda de confiança e reputação de uma empresa em face aos clientes por exemplo.

2.1 Ilícitos Mediante Obtenção e Venda de Dados Pessoais

Em relação aos ilícitos cometidos por vazamento de dados pessoais, tem sido uma das questões maisatuais, que merecem considerações nesse estudo, tendo em vista o poder que esse crime tem decausar um verdadeiro caos na vida de uma pessoa.

Com a facilidade virtual também veio os grandes riscos para os usuários, as senhas bancárias compartilhadas de forma online, compras virtuais, e-mails e a troca de mensagens via WhatsApp deu abertura a vulnerabilidade para os ladrões de fazer cartões de crédito com os nomes das vítimas, cartões clonados por compra na internet através de links, roubos bancários, compras sem autorização do cliente e usuário.

Uma das grandes problemáticas atualmente em relação a esse novo cenário de crimes é que alguns consistem em uma aceitação em "termos de concordância" sem a prévia leitura e conhecimento dos serviços que estão sendo ofertados. Normalmente em link de WhatsApp, site, aplicativos, download existem esses termos de concordância e fazem com que sejam vazados e roubadas informações bancárias, CPF, RG, senhas de cartões de crédito e o usuário na maioria das vezes não está ciente do que se trata e o que está contratando a partir daquele momento.

Francisco Gomes Júnior, presidente da ADDP (Associação de Defesa de Dados Pessoais e Consumidor) e sócio do OGF Advogados, associam os dados ao algoritmo:

> "Os dados pessoais passam a ter grande valor. Além de identificar, transmitem preferências políticas, religiosas, de opção sexual e demais valores íntimos. Os posts feitos em mídias sociais são armazenados pelas redes como Facebook, Instagram ou TikTok com a autorização do usuário, através dos termos de concordância que são aceitos sem ler."

Um exemplo dessas vendas e roubo de dados foi o site "Tudo Sobre Todos", que foi matéria de investigação do Ministério Público do Distrito Federal. Constatou-se que esse site fazia a cobrança de R$ 30,00 (trinta reais) por um pacote que dava direito a consulta e venda de dados pessoais. Nome, CPF, RG, Telefone, Endereço, data de nascimento e entre outros. Eles pegaram como base a plataforma de vendas e compras "Mercado Livre" e de lá eles pegavam as informações dos usuários, números de cartões de crédito, contas bancárias.

A Empresa Mercado Livre foi informada pelo MP e fez a suspensão permanente do usuário da conta "Tudo Sobre Todos" e repassou ao MP os dados cadastrais que eram usados por eles.

Em uma outra matéria podemos ver que estão sendo vendido por criminosos informações que são tiradas de cadastros de órgãos oficiais. Informações que estão no cadastro do Sus, Secretaria Nacional de Trânsito, na Receita Federal, no INSS e até mesmo informações do Sistema Nacional de Armas da Polícia Federal. Quem faz a assinatura semanalmente ou mensalmente paga um valor de até R$ 50,00 e você pode criar um login e senha para ter acesso a todos os dados e informações.

A TV Globo que foi responsável pela matéria, contatou sites em que ocorrem as vendas as informações que estão liberadas nesses sites são: RG, CPF, Endereço, Título de Eleitor e dados de veículos, placas, chassi e o RENAVAM.

Nesses sites legais existem diversos tipos de serviços e são variados os valores dos pacotes custando de R$ 50,00 até R$ 200,00. De acordo com o Advogado Paulo Vidigal, especialista em crimes digitais, quem fornece essas informações pessoais às quadrilhas também comete crime.

3. ALCANCE DA LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AO AMBIENTE VIRTUAL

Quando nos referimos diretamente às infrações penais, temos os elementos de conduta, tipicidade, ilicitude e culpabilidade. Esses conceitos são muito bem contemplados pelo Código Penal Brasileiro.

Quanto a conduta, temos a dolosa, que é quando o agente quer o resultado ou assume o risco de produzi-lo (art. 18, I, do CP) e a culposa onde o agente dá causa ao resultado em virtude de sua imprudência, negligência ou imperícia (art. 18, II, do CP). Entendemos, portanto, que todo crime é doloso e somente será culposo se houver ressalva expressa em lei, nos termos do parágrafo único do artigo 18 do CP.

Todavia, em matéria de crimes na era digital se torna extremamente difícil e delicado a aplicação literal dos conceitos penais, porque uma "máquina" não consegue diferenciar "dolo" e "culpa" nas condutas executadas. Até podemos usar como exemplo o envio de um vírus por *e-mail* recebido por uma pessoa e, de forma inocente, compartilhado para outras pessoas, sem de fato entender que tal ação acarretará um roubo de dados ou invasão do dispositivo por terceiro malicioso.

Interessante citar que a legislação brasileira ainda traz alguns dispositivos que auxiliam na busca pela proteção dos usuários na internet, conforme a tabela a seguir:

Tipicidade	Dispositivo legal	Penalidade/Sanção
Invasão de dispositivo informático	Lei 12.737/2012 (Lei Carolina Dieckmann)	Detenção de 3 (três) meses a 1 (um) ano, e multa. Além das majorantes em casos de prejuízo econômico.
Vazamento de dados pessoais	Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais)	I - Advertência, com indicação de prazo para adoção de medidas corretivas; II - Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - Multa diária, observado o limite total a que se refere o inciso II; IV - Publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - Bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - Eliminação dos dados pessoais a que se refere a infração;
Falha ou defeito na prestação de serviço	Lei 8.078/1990 (Código de Defesa do Consumidor)	I - Muta; II - Apreensão do produto; III - Inutilização do produto; IV - Cassação do registro do produto junto ao órgão competente; V - Proibição de fabricação do produto; VI - Suspensão de fornecimento de produtos ou serviço; VII - Suspensão temporária de atividade;

		VIII - revogação de concessão ou permissão de uso; IX - Cassação de licença do estabelecimento ou de atividade; X - Interdição, total ou parcial, de estabelecimento, de obra ou de atividade; XI - Intervenção administrativa; XII - Imposição de contrapropaganda.

Esse estudo se mostra necessário para que haja a correta interpretação quanto a responsabilização por danos causados e caminha em busca da completude na aplicação do direito, essa completude significa uma falta de lacunas e ocorre quando o ordenamento jurídico tem uma norma para regular qualquer caso (BOBBIO, 1982, p. 113).

4. O SISTEMA DE RESPONSABILIDADE CIVIL DOS AGENTES NOS DELITOS POR VAZAMENTO DE DADOS - SOB A ÓTICA DA LGPD E DO CDC

O estudo da responsabilidade civil se consolida na premissa de que a ninguém é facultado causar dano a outrem. *Neminem laedere*, esse princípio expressa um ideal de um compromisso tácito entre os indivíduos e que é encontrado no Código Civil:

> "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito".

Todo ser humano tem direito em ter sua privacidade, sendo aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade (FERRI, Giovanni B. 1985). Com vista nesse princípio constitucional de direito à privacidade do cidadão brasileiro a LGPD vem com todo respaldo para garantia e prevenção de afrontas a esse direito fundamental. Com a referida lei, acompanhamos o nascimento de um novo ramo do direito, com seus princípios primordialmente criados em defesa da privacidade que nos leva diretamente aos dados pessoais.

O dano consiste na efetiva violação a um interesse jurídico tutelado, o qual pode ser patrimonial (material) ou extrapatrimonial (moral). Para que haja dano indenizável necessário se faz que haja violação a interesse juridicamente tutelado e que o dano seja certo. A falta de dano torna sem objeto a pretensão a sua reparação.

A interpretação de ato ilícito na legislação de proteção de dados passou a ser observada sob o ponto de vista do elemento subjetivo, a culpa (BIONI, Bruno. 2020.), mas veremos que em decisões analisadas nos capítulos a seguir, podem possuir o teor objetivo.

A opção do legislador na interpretação da responsabilidade subjetiva na LGPD tem a possibilidade de excludente de ilicitude caso eles demonstrem que foram tomadas as diligências necessárias de segurança. No artigo 43, dispõe acerca desse excludente quando provarem corretamente o cuidado necessário na aplicação da legislação.

E temos então o cerne das discussões sobre a aplicação da responsabilidade civil subjetiva ou objetiva, pois a LGPD não é clara nesse sentido, provoca uma possibilidade de divergência na aplicabilidade da responsabilidade civil pelo intérprete e ao aplicador da lei.

Vamos diretamente à lei, a Seção III, a LGPD trata "Da Responsabilidade e do Ressarcimento de Danos", sendo este os trechos que devemos nos atentar na leitura desse estudo:

> "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.
> § 1° 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.
> § 2° 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.
> § 3° 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.
> § 4° Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso."
> 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.
> Mediante a apresentação de provas suficientes que isentem de responsabilidade os agentes do tratamento de dados (que são o controlador e/ou o operador), a mesma isenção de responsabilidade lhe deverá ser garantida.

> 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."

Os artigos citados trazem a demonstração da ilicitude do tratamento de dados e retira a responsabilidade na hipótese de eles estarem devidamente adaptados à legislação de dados. Ou seja, basta estar adaptado à LGPD que terá a aplicação de responsabilidade subjetiva. O maior ponto a ser analisado nos próximos capítulos desse estudo é justamente a aplicação desses artigos nas decisões recentes.

> "Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente."

Ou seja, dependendo do tipo de violação de direitos do titular poderão ser aplicadas penalidades/sanções sob a ótica da legislação consumerista (Código de Defesa do Consumidor) e/ou pela regra geral do Código Civil Brasileiro (artigos 186, 187 e 927).

No tocante à responsabilidade civil desses agentes de tratamento, a legislação prevê que ainda que o operador deva se limitar a executar as ordens do controlador haverá a responsabilização solidária, quando descumprida a normas previstas na LGPD.

Ao tratar da responsabilização desses agentes frente ao vazamento de dados, Lara Rocha (2020, p. 20) argumenta que:

> "Além disso, mesmo que o Titular tenha manifestamente tornado públicos seus dados, o Controlador e o Operador não estão isentos de suas responsabilidades, especialmente no que diz respeito ao livre acesso do Titular às informações baseadas em seus dados, forma e duração do tratamento realizado com eles, e a possíveis compartilhamentos que Controlador e Operador possam ter feito."

Dessa análise, pode-se observar claramente o fundamento da privacidade trazido pela LGPD, dessa forma, o dado postado, mesmo que se torne público, aquele que vier a utilizá-lo deve respeitar os direitos do titular do dado, previstos na legislação.

É possível concluir que, junto com o advento da LGPD surgiu a responsabilização dos agentes de tratamentos detentores de dados pessoas dos usuários de serviços, no tocante a responsabilidade civil desses agentes, pode-se observar que, quando tratar-se de matérias referentes ao descumprimento da LGPD, essa responsabilidade será solidária, ainda que o operador esteja de acordo com os comandos do controlador.

Entretanto, como citado anteriormente, podemos concluir que na LGPD existem dois regimes distintos, onde, a depender do caso concreto, essa responsabilização poderá ser objetiva ou subjetiva.

4.1 Da Teoria do Risco

A opção legislativa dos referidos artigos do CDC tem como base a teoria do risco, que se o fornecedor ou prestador de serviço cria um risco, ele deve se responsabilizar por ele, na intenção de que as vítimas não fiquem sem reparação dos danos caso ocorra falha no fornecimento e prestação de algum serviço.

A própria LGPD reconhece a aplicabilidade do CDC, ao tratamento de dados pessoais nas relações de consumo, já ensejava o debate para a responsabilidade sem culpa. A própria cláusula da responsabilidade objetiva do Código Civil já dispusera sobre a matéria. Nesse cenário, um parecer da Comissão Especial constituída pela Câmara dos Deputados afirmava, expressamente:

> "A atividade de tratamento de dados pessoais constitui atividade de risco, o que atrai a incidência da responsabilidade objetiva ao agente de tratamento, ou seja, aquela segundo a qual não há necessidade de perquirir a existência de culpa para obrigar o causador do dano a repará-lo. Esta já é a regra geral do direito brasileiro para toda e qualquer atividade de risco, conforme previsto no parágrafo único do artigo 927 do Código Civil, como também constitui a base da responsabilização dos fornecedores nas relações de consumo"

5. VAZAMENTO DE DADOS PESSOAIS NOS TRIBUNAIS - ANÁLISE JURISPRUDENCIAL E A APLICAÇÃO DOS CONCEITOS

Neste capítulo será feita uma análise jurisprudencial do teor das decisões na intenção de verificar a responsabilidade civil dos agentes e como influencia nas penalidades aplicadas à violação no tratamento de dados pessoais.

O primeiro caso se que trata do processo n° 1006108-87.2021.8.26.0100, da 10ª Vara Cível do Tribunal de Justiça de São Paulo, refere-se a uma relação contratual entre o requerente (pessoa física autora da demanda) e o requerido (empresa concessionária de distribuição de energia elétrica) para prestação de serviços de fornecimento de energia elétrica, na qual o autor teve seus dados cadastrais acessados por terceiros, em decorrência de acidente de segurança interno na empresa. Vejamos:

> "APELAÇÃO. Ação de obrigação de fazer e indenização por danos morais. Sentença que julgou improcedente a ação. Inconformismo da parte autora.

> Energia elétrica. Vazamento de dados do sistema da ELETROPAULO. Ação de indenização por danos morais. Falha na prestação de serviço de proteção aos dados. Responsabilidade objetiva configurada (artigo 14, CDC) que, por si só, não é capaz de causar dano moral. Ausência de comprovação da efetiva violação a direito de personalidade da parte autora, bem como da efetiva ocorrência de prejuízos. Inexistência de dano "in re ipsa". Indenização indevida. Sentença mantida. Recurso improvido.
> (TJ-SP - AC: 10061088720218260100 SP 1006108-87.2021.8.26.0100, Relator: Rodolfo Cesar Milano, Data de Julgamento: 28/03/2022, 35ª Câmara de Direito Privado, Data de Publicação: 28/03/2022).

Em análise a sentença, verifica-se que o entendimento do magistrado é de que ainda que ocorra vazamento de dados pessoais, o titular dos dados deve comprovar a existência de culpa, no caso em questão o magistrado entende que não houve indicação precisa de que o vazamento de dados da requerente, decorreu de culpa da empresa requerida. Dessa forma, o magistrado entende que o ônus probante caberia ao autor, sendo assim, a responsabilidade é vista como subjetiva.

Ademais, o réu confirma que foi vítima de hacker e que houve o vazamento de alguns dados pessoais, entretanto, o magistrado considerando não haver culpa por parte da ré, optou por não a condenar.

Ainda assim, é considerado pelo magistrado que os supostos dados vazados não são considerados como sensíveis e que a alegação do autor não estava amparada em provas robustas.

Contudo, é importante destacar que a LGPD não faz esta distinção para fins de responsabilização no artigo 42 da lei. O tratamento ilícito tanto de dados pessoais sensíveis quanto dados pessoais “comuns” é passível de responsabilização e indenização.

Em sentença, o magistrado indeferiu todos os pedidos do autor, por entender que não havia elementos e provas robustas aptas a ensejar a condenação do réu.

Dessa forma, é possível observar que neste caso concreto, o magistrado considerou que a responsabilidade civil seria subjetiva, uma vez que, apesar de reconhecer que houve o vazamento de dados, optou por não condenar a empresa, usando como argumento a não comprovação da culpa da requerente.

Em outro processo, o qual trata da mesma situação relatada na decisão anterior, houve entendimento diverso.

Em sentença, o magistrado indeferiu os pedidos que versavam acerca da responsabilização por supostos danos morais e vazamento de dados. Entretanto, o Autor interpôs o recurso de apelação Cível n° 1008308-35.2020.8.26.0704 buscando a reforma da sentença. Veja-se:

> "LEI GERAL DE PROTEÇÂO DE DADOS PESSOAIS (LGPD) E DIREITO DO CONSUMIDOR. AÇÃO COM PRECEITOS CONDENATÓRIOS. Sentença de improcedência dos pedidos. Recurso de apelação do autor. Vazamento de pessoais não sensíveis do autor (nome completo, números de RG e CPF, endereço de e-mail e telefone), sob responsabilidade da ré. LGPD. Responsabilidade civil ativa ou proativa. Doutrina. Código de Defesa do Consumidor. Responsabilidade civilobjetiva. Ausência de provas, todavia, de violação à dignidade humana do autor e seus substratos, isto é, liberdade, igualdade, solidariedade e integridade psicofísica. Autor que não demonstrou, a partir do exame do caso concreto, que, da violação a seus dados pessoais, a ocorrência de danos morais. Dados que não são sensíveis e são de fácil acesso a qualquer pessoa. Precedentes. Ampla divulgação da violação já realizada. Recolhimento dos dados. Inviabilidade, considerando-se a ausência de finalização das investigações. Pedidos julgados parcialmente procedentes, todavia, com o reconhecimento da ocorrência de vazamento dos dados pessoais não sensíveis do autor e condenando-se a ré na apresentação de informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados, fornecendo declaração completa que indique sua origem, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, assim como a cópia exata de todos os dados referentes ao titular constantes em seus bancos de dados, conforme o art. 19, II, da LGPD. Determinação para envio de cópia dos autos à Autoridade Nacional de Proteção de Danos (art. 55-A da LGPD). RECURSO PARCIALMENTE PROVIDO.''

No tocante à responsabilidade civil o magistrado destaca tratar-se de responsabilidade civil objetiva, ao passo que considera que a LGPD assume o CDC como um de seus fundamentos, no que diz respeito ao rol de garantias e direitos do titular de dados pessoais e dos deveres dos tratadores e coletores de dados pessoais.

Em suma, o entendimento jurisprudencial neste caso, é de que a responsabilidade civil é objetiva, uma vez que se tratando de relação de consumo o art. 45 da LGPD prevê que devem ser aplicadas as regras de responsabilidade previstas no Código de Defesa do Consumidor.

Além disso, com relação à acusação de que, com a LGPD e com a adoção de um regime objetivo de responsabilização civil, haveria uma ampliação do número de demandas indenizatórias, inibindo o desenvolvimento e a indústria, bem como de novas tecnologias, o magistrado destaca a fala da doutrinadora Maria Celina Bodin de Moraes, veja-se:

> "(...) falso dilema pois a história já demonstrou que a adoção dos modelos de culpa presumida ou de responsabilidade objetiva, que flexibilizaram a dificuldade da prova da culpa, não limitaram o desenvolvimento de novas tecnologias. Ao contrário: assegurou-se o pleno desenvolvimento tecnológico e industrial e os custos dos modelos de responsabilização objetivos, em especial nas relações de consumo, foram incorporados pelo mercado sem prejuízo do ressarcimento das vítimas de danos injustos, implementando-se o modelo solidarista de responsabilidade fundado na atenção e no cuidado para com o lesado. Ademais, já pontuava Rodotà, o argumento de eventual aumento dos custos de proteção dos dados pessoais para as empresas não é decisivo, vez que não se pode estimar que interesses ligados à proteção de dados pessoais dos titulares sejam de status inferior aos interesses empresariais"

Em relação ao caso concreto, houve parcial reforma da sentença, ao passo que o magistrado reconheceu a violação cometida pela ré no vazamento de dados pessoais não sensíveis do autor sem, contudo, haver demonstração nos autos de prejuízo moral indenizável.

Dessa forma, a ré foi condenada a apresentar informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados do autor, conforme o art. 18, VII, da LGPD, devendo fornecer declaração completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, assim como a cópia exata de todos os dados referentes ao titular constantes em seus bancos de dados

Verifica-se nessa decisão que foi reconhecido o vazamento de dados, sendo a empresa responsabilizada de forma objetiva e condenada a multa de R$ 500,00 ao dia caso não apresente informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados do autor, entretanto, o magistrado não reconheceu demonstração nos autos de prejuízo moral indenizável.

Tratam-se de demandas materialmente idênticas, as quais litigam sobre a mesma situação ocorrida em uma empresa de energia elétrica, entretanto, nota-se que houve entendimento diverso dos magistrados. Ocorre que, enquanto no primeiro processo o magistrado entendeu que seria necessária a existência de culpa da empresa para que fosse passível à aplicação das penalidades requeridas, no segundo caso o magistrado considerou que se tratando de uma relação de consumo, deve-se aplicar a responsabilidade objetiva prevista no Código de Defesa do Consumidor.

O terceiro caso trata-se do recurso inominável cível nº 073873716.2020.8.07.0016 que foi julgado pela Primeira Turma Recursal Dos Juizados Especiais do Distrito Federal, neste caso verifica-se uma das situações mais recorrentes: o vazamento de dados por instituições financeiras. Vejamos:

> JUIZADO ESPECIAL CÍVEL. DIREITO DO CONSUMIDOR. FRAUDE BANCÁRIA. SUBTRAÇÃO DE VALORES. FORTUITO INTERNO. SÚMULA 479 DO STJ. LEI GERAL DE PROTEÇÃO DE DADOS. DANO MORAL. CONFIGURADO. RECURSO CONHECIDO E PARCIALMENTE PROVIDO. 1. Acórdão lavrado de acordo com a disposição inserta nos artigos 2º e 46, da Lei 9.099, de 26.09.1995 e artigo 103, §§ 1º e 2º, do Regimento Interno das Turmas Recursais. Presentes os pressupostos específicos, conheço do recurso. 2. Recurso inominado interposto pela autora/recorrente para reformar a sentença que julgou improcedente o pedido deduzido na petição inicial, consistente em condenar o réu/recorrido ao pagamento de indenização por danos morais no valor de R$ 39.920,00 (trinta e nove mil novecentos e vinte reais). 3. Alega a recorrente que, em 23.07.2020, recebeu contato telefônico do recorrido parao fim de lhe noticiar acerca de bloqueio na conta por ela titularizada. O recorrido teria promovido a referida operação em função da realização de transações de alto valor. Relata que se dirigiu ao estabelecimento bancário

do recorrido e adotou as medidas cabíveis. Outrossim, afirma que os valores subtraídos se destinavam a aquisição de bem imóvel, tendo esse evento lhe causado abalos à sua personalidade. 4. A relação jurídica estabelecida entre as partes é de natureza consumerista, devendo a controvérsia ser solucionada sob a ótica do sistema jurídico autônomo instituído pelo Código de Defesa do Consumidor (Lei n.º 8.078/1990). 5. O artigo 14 estabelece que o fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos, tratando-se, portanto, de responsabilidade objetiva. 6. Ademais, a súmula n.º 479 do STJ prevê as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. 7. No caso dos autos, restou evidenciada a ocorrência de fortuito interno, o qual possibilitou que terceiros subtraíssem elevada quantia mantida pela recorrente em estabelecimento bancário do recorrido, o que caracteriza, portanto, má-prestação do serviço, especialmente na guarda de dados sensíveis da recorrente. Reforça a existência de falha nos procedimentos de segurança a circunstância de ter o recorrido procedido à restituição dos valores em favor da recorrente, conforme foi noticiado ao ID 23671406. 8. A Lei n.º 13.709, de 14.08.2018, que dispõe sobre a proteção de dados pessoais, ora denominada Lei Geral de Proteção de Dados (LGPD), prevê no artigo 6º, inciso VII, que as atividades de tratamento de dados pessoais deverão observar a boa-fé e o princípio da segurança. Esse princípio trata da 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. Ademais, o princípio da prevenção dispõe sobre a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, nos termos do artigo 6º, inciso VIII. Da análise dos autos, verifica-se que tais medidas não foram adotadas pelo recorrido, ou foram insuficientes para evitar o infortúnio vivenciado pela recorrente. 9. Quanto ao pedido de indenização por danos morais, há evidências de que a conduta do recorrido provocou abalos à personalidade, honra e fama da recorrente. 10. A fixação do valor a título de dano moral deve levar em conta critérios doutrinários e jurisprudenciais, tais como o efeito pedagógico e inibitório para o ofensor e a vedação ao enriquecimento sem causa da ofendida ou empobrecimento do ofensor. 11. Ademais, a indenização deve ser proporcional à lesão à honra, à moral ou à dignidadeda ofendida, às circunstâncias que envolvem o fato, às condições pessoais e econômicas dos envolvidos, e à gravidade objetiva do dano moral. 12. Sob tais aspectos, fixo como indenização por danos morais o valor de R$ 3.000,00 (três mil reais). 13. Conheço do recurso e lhe dou parcial provimento. Sentença reformada para condenar o recorrido ao pagamento de indenização por danos morais no valor de R$ 3.000,00 (três mil reais), corrigidos monetariamente desde a data do arbitramento, nos termos da súmula n.º 362 do STJ. 14. Sem custas e sem honorários advocatícios, nos termos do artigo 55, da Lei n.º 9.099, de 26.09.1995. Gratuidade de justiça concedida nesta oportunidade.

(TJ-DF 07387371620208070016 DF 0738737-16.2020.8.07.0016, Relator: ANTONIO FERNANDES DA LUZ, Data de Julgamento: 30/07/2021, Primeira Turma Recursal, Data de Publicação: Publicado no DJE: 23/08/2021. Pág.: Sem Página Cadastrada.)

Nestes casos, o entendimento jurisprudencial tem sido o de que a responsabilidade civil independe de culpa, uma vez que se trata de falha na prestação do serviço.

O artigo 14 do Código de Defesa do Consumidor estabelece que o fornecedor (no caso, o banco) responde mesmo em casos de força maior, como é o caso da prática de crime de estelionato por terceiro, devendo indenizar os danos causados ao consumidor.

Sendo assim, em mais uma análise podemos verificar a utilização do CDC, vez que na maioria dos processos que envolvem o vazamento de dados é considerada a presença de prestação de serviços, dessa forma, assim como no processo anterior foi considerada que a responsabilidade dos agentes responsáveis pelo vazamento de dados será objetiva.

Ainda assim, se tratando de instituições financeiras, cabe ressaltar que em alguns julgados a Súmula 479 do STJ é posta em destaque, vejamos o corpo textual da citada Súmula:

> Súmula 479/STJ, "as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias"

Dessa forma, é importante destacar que, mesmo posteriormente a responsabilidade na Lei Geral de Proteção de Dados sendo considerada subjetiva, nestes casos, tratando-se de instituições financeira, a responsabilidade, via de regra, será objetiva.

O quarto processo em análise trata-se do recurso de Apelação Cível nº 1006311-89.2020.8.26.0001 que teve seu provimento negado, vez que foram reconhecidos os danos morais causados à autora e concedida a indenização a título de danos morais. Vejamos:

> "APELAÇÃO – AÇÃO CONDENATÓRIA – PRESTAÇÃO DE SERVIÇOS EDUCACIONAIS – VAZAMENTO DE DADOS PESSOAIS POR PREPOSTO – CELULAR DA AUTORA PASSADO A UM TERCEIRO – RECEBIMENTO DE MENSAGENS DE ASSÉDIO SEXUAL – RECURSO DE AMBAS AS PARTES – LEGITIMIDADE PASSIVA DA RÉ – RESPONSABILIDADE PELOS DANOS DECORRENTES DA VIOLAÇÃO AO TRATAMENTO DE DADOS PESSOAIS – LEI GERAL DE PROTEÇÃO DE DADOS – DANOS MORAIS EVIDENTES – MAJORAÇÃO – GRAVE VIOLAÇÃO À INTIMIDADE E À PRIVACIDADE 1 – A empresa controladora de dados pessoais é figura legítima para figurar no polo passivo de demanda que objetive a indenização pelo vazamento de dados da autora orquestrados por preposto da ré, que repassou o celular da autora para um colega para fins de assédio sexual (LGPD, art. 42). 2 – A ré, ao dar causa ao vazamento de dados, responde pelos danos morais sofridos (LGPD, art. 5º, VI e 42, caput). 3 – É cabível a indenização por danos morais, considerando a violação grave ao direito à intimidade e à privacidade causado pela quebra do dever de proteção de dados pessoais, o que propiciou assédio sexual agressivo. 4 – Indenização majorada, pois a gravidade da situação, a séria negligência da empresa, a postura recalcitrante em reconhecer o erro, e a incipiente jurisprudência estadual autorizam resposta mais enérgica. Valor de dez mil reais que se mostra mais condizente com o cenário narrado. RECURSO DA RÉ NÃO PROVIDO. RECURSO DA AUTORA PROVIDO.

> (TJ-SP - AC: 10063118920208260001 SP 1006311-89.2020.8.26.0001, Relator: Maria Lúcia Pizzotti, Data de Julgamento: 01/09/2021, 30ª Câmara de Direito Privado, Data de Publicação: 01/09/2021).”

O caso em tela aborda a situação em que a ré (empresa de comércio de livros e informática) possuía o número de celular da autora por meio de um contrato de prestação de serviços firmado entre ambas, nesse contexto, ocorreu o vazamento dos dados da autora para um terceiro que a importunou de forma reiterada, chegando a autora, inclusive, a ser vítima de assédio.

A parte ré apresentou recurso de apelação que teve provimento negado, vez que em juízo o magistrado manteve a sentença que condenou a empresa ré ao pagamento de indenização por danos morais.

Apesar da responsabilidade civil não ter sido o principal ponto de discussão no processo, percebe-se que esta foi considerada pelo magistrado como objetiva, sendo assim, depreende-se da decisão o seguinte trecho:

> “A falha na proteção de dados atrai a responsabilidade da empresa ré enquanto controladora de dados pessoais. Portanto, responde pelos danos morais sofridos pela”

Sendo assim, vemos mais uma decisão que considerada a responsabilidade da portadora de dados como sendo objetiva, de forma que, independentemente da existência de culpa, o autor da conduta responde pela reparação do dano.

Dessa forma, ao fim da presente análise jurisprudencial podemos observar que em grande parte das decisões a responsabilidade civil é considerada objetiva, ao passo que o Código de Defesa do Consumidor é utilizado quando tratam de relações de consumo, entretanto, ainda é possível verificar a dualidade nas decisões, vez que em alguns casos a responsabilidade é considerada subjetiva.

6. CONSIDERAÇÕES SOBRE O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS (ANPD)

Com a entrada em vigor da Lei Geral de Proteção de dados houve a necessidade da criação de um órgão independente que tivesse o papel de analisar e regulamentar os pontos controversos da lei, nesse contexto, surge a Autoridade Nacional de Proteção de Dados - ANPD, órgão federal, que tem como uns de seus objetivos editar e fiscalizar as normas e procedimentos sobre a proteção e a transferência de dados pessoais no país.

Ainda assim, a ANPD também exerce papel de natureza normativa e deliberativa, de forma que, soma-se ainda a sua competência a aplicação de sanções administrativas em caráter terminativo, sobre a interpretação da LGPD, as suas competências e os casos omissos.

A existência de uma autoridade administrativa que supervisione a efetiva aplicação dos conceitos estabelecidos na lei de dados é de extrema necessidade, para justamente aproximar as esferas do mercado e do setor público com o cidadão e seus direitos fundamentais no que tange a proteção de dados.

Diante de toda essa impossibilidade de contemplação integral nos tribunais da fiscalização do órgão, até o presente estudo, a ANPD não se encontra ativa nas decisões analisadas. O Regulamento de Dosimetria e Aplicação de Sanções Administrativas pela ANPD, chamado de "norma de dosimetria" foi publicado no dia 27 de fevereiro de 2023. Os objetivos elencados na norma é regulamentar os artigos 52 e 53 da LGPD, definindo critérios e parâmetros para as sanções pecuniárias, bem como as formas e dosimetrias para o cálculo do valor-base das multas e alterar os artigo 32, 55 e 62 da Resolução n° 1° CD/ANPD, com vistas a aprimorar o processo administrativo sancionador e de fiscalização, dando à ANPD uma atuação repressiva, respeitando o devido processo legal e o contraditório, de modo a proporcionar segurança jurídica e transparência a todos os envolvidos.

Nesse contexto, o órgão regulará e supervisionará agentes econômicos, como empresas e instituições financeiras, assim como governos municipais, estaduais e federal e dentre as sanções passíveis a sua aplicação podemos citar: Advertência; Multa simples, de até 2% (dois por cento) do faturamento da empresa, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais), por infração; Multa diária, com limite total de R$ 50.000.000,00 (cinquenta milhões de reais); Publicização da infração; Bloqueio dos dados pessoais; Eliminação dos dados pessoais; Suspensão parcial do funcionamento do banco de dados por no máximo de 6 (seis) meses, prorrogável por igual período, até que se regularize a situação; Suspensão do exercício da atividade de tratamento dos dados pessoais por no máximo de 6 (seis) meses, prorrogável por igual período; Proibição parcial ou total do exercício de atividades relacionadasa tratamento de dados. Com exceção das multas, todas as demais sanções poderão ser aplicadasao Poder Público (GOV.BR, 2023).

Ou seja, segundo a análise jurisprudencial feita nesse estudo, as decisões poderiam ter tomado um rumo mais criterioso e específico, ao invés apenas da aplicação da alternativa de responsabilidade subjetiva às empresas que não se encontravam adaptadas à LGPD.

7. CONCLUSÃO

Quando analisadas as decisões e acórdãos, observamos que a pauta de responsabilidade civil é sanada dependendo do caso e do ponto de vista que foi usado.

Um caso sob n° 1006108-87.2021.8.26.0100, onde a empresa de energia possui cadastro dos clientes, onde houve ataque hacker contra o banco de dados da empresa e o magistrado optou pela não condenação pois ataque hacker seria caso fortuito externo e não culpa da empresa, ou seja, foi julgado com responsabilidade subjetiva, temos a violação de normas técnicas, voltadas à segurança e proteção dos dados. Sendo assim, a decisão foi reformada sob apelação n. 1008308-35.2020.8.26.0704, após interposição de recurso do autor que se deu de forma objetiva, em observância do CDC, condenando a empresa à multas diárias até confirmação da origem dos dados, que são requisitos exigidos de uma empresa com a devida adaptação da LGPD.

Ainda nas duas decisões seguintes, destaca-se a responsabilidade independente de culpa conferida às instituições bancárias por meio de súmula e mais uma consequência, na Apelação Cível nº 1006311-89.2020.8.26.0001, vitimando a autora a assédio em decorrência do crime de vazamento.

É possível identificar duas situações de responsabilidade civil na LGPD: a) violação de normas jurídicas, do microssistema de proteção de dados; b) violação de normas técnicas, voltadas à segurança e proteção de dados pessoais.

Entende-se que em caso de vazamento de dados temos sim uma relação de consumo que foi ferida, ou seja, podem ser aplicadas ambas as leis sob ponto de vista de que a violação da legislação da LGPD que possibilitou o ilícito de vazamento caracterizando diretamente uma quebra de contrato, ou seja, uma violação expressa no CDC. Dessa forma, vemos como a Lei de Proteção de Dados e de Defesa do Consumidor estão conectadas, casos de ilicitude com o tratamento dos dados.

O legislador, ao aplicar lei de dados não espelha os excludentes do CDC, mas sim exime a responsabilização dos agentes caso demonstrem que tomaram as medidas necessárias para proteger os dados de acessos não autorizados, e esses elementos afastam automaticamente uma responsabilização objetiva sob à luz da LGPD. Por isso que temos essa dualidade no entendimento. Segundo as intenções Bruno Bioni e Daniel Dias com os estudos nesse sentido é de que:

> “deve-se, assim, avançar para além da análise binária do regime jurídico de responsabilidade civil da LGPD, julgando-o de natureza objetiva ou subjetiva. Isto porque não deve haver dúvidas de que a política legislativa

> adotada exige a investigação em torno de um juízo de culpa dos agentes de tratamento de dados, mas, ao mesmo tempo, prescreve uma série de elementos com alto potencial de erosão dos filtros para que os agentes de tratamentos de dados sejam responsabilizados. O resultado parece ir no sentido de um regime jurídico de responsabilidade civil subjetiva com alto grau de objetividade."

A lei ainda possui pouco tempo de vigência, mas os estudos são de extrema importância para sanar interpretações dúbias que podem afastar a aplicação correta do dever de indenizar uma vítima de um crime por vazamento dos seus dados pessoais. Entretanto, os argumentos da "responsabilidade subjetiva com alto grau de objetividade" parecem refletir melhor a orientação legislativa.

REFERÊNCIAS BIBLIOGRÁFICAS

ALENCAR, Gliner; LIMA, Marcelo de; FIRMO, André. **O Efeito da Conscientização de Usuários no Meio Corporativo no Combate à Engenharia Social e Phishing**. In: SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO (SBSI), 9. , 2013, João Pessoa. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2013. p. 254-259. DOI: https://doi.org/10.5753/sbsi.2013.5694. Acesso em: 27/03/2022.

ANPD publica regulamento de aplicação de sanções administrativas. Gov.br. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria>. Acesso em: 27/02/2023.

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. a. 9. n. 3. 202. Disponível em <https://civilistica.emnuvens.com.br/redc/article/view/662/506>. Acesso em 24/11/2022

BOBBIO, Norberto. **Teoria do Ordenamento Jurídico**. Brasília: Editora UnB, 1982. Disponível em: < https://edisciplinas.usp.br/pluginfile.php/4212351/mod_folder/content/0/Norberto%20Bobbio%20-%20Teoria%20do%20Ordenamento%20J.pdf?forcedownload=1>. Acesso em: 19/05/2022.

BRASIL, **Lei n° 10.406**, de 10 de janeiro de 2002. Institui o Código Civil. Brasília. 2002.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: Senado Federal, 2018.

BRASIL. Código de defesa do consumidor. **Lei 8.078 de 11/09/90**. Brasília, Diário Oficial da União, 1990.

Canal Ciências Criminais, "Crimes Digitais: do que estamos falando?" Marcelo Crespo (2022). Disponível em: <https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/> Acesso em 20/09/2022

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. São Paulo: Thomson Reuters, 2018. p. 212-213.

Criminosos vendem dados pessoais pela internet utilizando cadastros de órgãos oficiais, por Jornal Nacional 'Folha de São Paulo". Disponível em: <https://g1.globo.com/jornal-nacional/noticia/2021/12/04/criminosos-vendem-dados-pessoais-pela-internet-utilizando-cadastros-de-orgaos-oficiais.ghtml> Acesso em 05/10/2022

FRAZÃO, Ana. **A Nova Lei Geral de Proteção de Dados Pessoais - Principais repercussões para a atividade empresarial**. Ano 2018. Disponível em: <http://www.professoraanafrazao.com.br/files/publicacoes/2018-08-30A_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais_Principais_repercussoes_para_a_atividade_empresarial_Parte_I.pdf>, Acesso em: 17/09/2022.

FRAZÃO, Ana. **Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados**. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1 .ed. São Paulo: Thomson Reuters Brasil, 2019. p. 23-52. Disponível em < https://bit.ly/3xURUxG>. Acessado em: 17/09/ 2022.

FROIS, Rebecca de Araújo; **LGPD: MECANISMOS DE SEGURANÇA, DA INVASÃO À PROTEÇÃO DE DADOS**. UniCEUB- Taquaritinga. P.20. Outubro, 2021. Acesso em: 19/05/2022.

GOMES, Francisco. **Saiba como funciona a Venda de Dados pessoais na Internet**. Disponível em: <https://www.migalhas.com.br/quentes/364537/saiba-como-funciona-a-venda-de-dados-pessoais-na-internet> Acesso em: 23/04/2022.

GRAU, Eros. **Ensaio e discurso sobre a interpretação/aplicação do direito**. São Paulo: Malheiros, 2006. p. 132.

IDENTITY FRAUD STUDY, 2021. Disponível em: <https://javelinstrategy.com/content/2021-identity-fraud-report-shifting-angles-identity-fraud> Acesso em 02/03/2022.

KARPERSKY, **Centro de Recursos**, 2022. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime> Acesso em 14/10/2022.

MALDONADO, Viviane Nobrega; OPICE BLUM, Renato (Coord.). **LGPD: Lei Geral de Proteção de Dados comentada**. São Paulo: Revista dos Tribunais, Thomson Reuters Brasil, 2019

MOARES, Maria Celina Bodin de Moraes e QUEIROZ, Quinelato em **"Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD**". In: Cadernos Adenauer XX, 2019, no 3, Proteção de dados pessoais: privacidade versus avanço tecnológico. Rio de Janeiro, Fundação Konrad Adenauer, outubro de 2019, pp. 113-136.

ORLOWSKI, Jeff. **O Dilema das Redes**. Netflix, 2020.

TRISTAN, Harris. **Google Former Design Ethicist**. 5'28" - 5'30". Acesso em: 19/05/2022.

ODIN DE MORAES, Maria Celina. **LGPD: um novo regime de responsabilização civil dito "proativo". Editorial à Civilistica**. Rio de Janeiro: a. 8, n. 3, 2019. Disponível em: <http://civilistica.com/lgpd-um-novo-regime/>. Acesso em 17/06/2022

O que é o Roubo de dados e como evitá-lo. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/data-theft> Acesso em 17/06/2022.

Os Agentes de Tratamento de Dados Pessoais na LGPD. Tenbu,2021. Disponível em <https://www.tenbu.com.br/os-agentes-de-tratamento-de-dados-pessoais-na-lgpd-2/>. Acesso em: 27/03/2022.

PINHEIRO, Patrícia Peck. **Direito digital**. 2. ed. São Paulo: Saraiva, 2008. p. 29. Acesso em: 19/05/2022

Relatório da Comissão Especial destinada a Proferir Parecer ao Projeto de Lei 4.060/2012, do Deputado Orlando Silva. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=SBT+1+PL406012+%253D%253E+PL+4060/2012>. Acesso em 11/07/2022

Responsabilidade civil dos agentes de tratamento de dados: subjetiva ou objetiva? Diogo Ramos Ferreira, 20/11/2019. Disponível em < https://www.jota.info/opiniao-e-analise/artigos/responsabilidade-civil-dos-agentes-de-tratamento-de-dados-subjetiva-ou-objetiva-20112019> Acesso em: 19/05/2022.

Responsabilidade Civil na LGPD. Machado Meyer Advogados, 04 dez. de 2020. Disponível em: <https://www.machadomeyer.com.br/pt/inteligencia-juridica/publicacoes-qij/tecnologia/responsabilidade-subjetiva-na-lgpd>. Acesso em: 27/03/2022

ROQUE, André. **A tutela coletiva dos dados pessoais na Lei Geral de Proteção de Dados Pessoais (LGPD)**. Revista Eletrônica de Direito Processual – REDP. Ano 13, v.20, n.2, p. 01-19, maio a ago. 2019. Disponível em: <https://doi.org/10.12957/redp.2019.42138>. Acessado em: 17 set 2022.

Site que vende dados pessoais de qualquer brasileiro é investigado pelo MP, por G1 DF, 13/07/2018. Matéria Disponível em: https://g1.globo.com/df/distrito-federal/noticia/site-que-vende-dados-pessoais-de-qualquer-brasileiro-e-investigado-pelo-mp.ghtml

State of Cybersecurity Report 2021 | 4th Annual Report | Accenture. Disponível em: https://www.accenture.com/us-en/insights/security/invest-cyber-resilience

STJ, 3ª T., **Resposta 1.517.800/PE**, Rel. Min. Ricardo Villas Bôas Cueva, ac. 02.05.2017, DJe 05.05.2017.

Tribunal de Justiça de São Paulo. **Apelação Cível nº 1006108-87.2021.8.26.0100**, Apelante: Renato Fontes Da Silva Braz, Apelado: Eletropaulo Metropolitana Eletricidade de São Paulo S/A, Relator: Rodolfo Cesar Milano Data de Julgamento: 28/03/2022, 35ª Câmara de Direito Privado, Data de Publicação: 28/03/2022.

Tribunal de Justiça de São Paulo. **Apelação Cível nº 1008308-35.2020.8.26.0704**, Apelante: Alexandre Cardoso, Apelado: Eletropaulo Metropolitana Eletricidade de São Paulo S/A, Relator: Alfredo Attié, Data de Julgamento: 16/11/2021, 27ª Câmara de Direito Privado, Data de Publicação: 16/11/2021).

Tribunal de Justiça do Distrito Federal. **Recurso Inominado Cível n° 0738737-16.2020.8.07.0016**, Recorrente: Natalia Scarano Gomes Coelho, Recorrido: Banco do Brasil S/A, Relator: Antonio Fernandes da Luz. Data de Publicação: Publicado no DJE : 23/08/2021 . Pág.: Sem Página Cadastrada.

Tribunal de Justiça do Estado de São Paulo da Comarca de São Paulo, Assunto: **Apelação Civil, N° do Processo: 1008308-35.2020.8.26.0704**, Apelante: Alexandre Cardoso, Apelado: Eletropaulo Metropolitana Eletricidade de São Paulo S/A, Relator: Alfredo Attié, São Paulo, 16 de novembro de 2021.

Tribunal de Justiça do Estado de São Paulo, Assunto: **Recurso Inominado, Nº do Processo: 1003086-21.2021.8.26.0003**, Recorrente: Ana Maria Nishimura da Cruz, Recorrido: Eletropaulo Metropolitana Eletricidade de São Paulo S/A, Relator: Carlos Eduardo Santos Pontes de Miranda. São Paulo, 25 de outubro de 2021.

TURBAN, Efraim; McLEAN, Ephraim. WETHERBE, James. **Tecnologia da Informação para Gestão: Transformando os Negócios na Economia Digital**. 3a . Ed. São Paulo: Bookman, 2004. Cap. 15, p. 532-563.

Vazamento e Roubo de Dados: Como se Precaver? Galvão & Silva Advocacia, matéria atualizada dia 15/02/2023. Disponível em: <https://www.galvaoesilva.com/roubo-de-dados/> Acesso em 28/05/2022

Your Data for Sale. Times, New York: Time Inc, v. 177, n.11, 21 mar. 2011. Acesso em: 27/03/2022.

Associação Caruaruense de Ensino Superior e Técnico - ASCES (Mantenedora)
CNPJ: 09.993.940/0001-01
Avenida Portugal, Nº 584. CEP: 55016-901 - Bairro Universitário - Caruaru/PE
+55 (81) 2103.2000 | Fax: (81) 2103.2053 | asces@asces.edu.br | www.asces.edu.br

PARECER FINAL DE TRABALHO DE CONCLUSÃO DE CURSO

BACHARELADO EM DIREITO

ESTUDANTES:	**MARIA CICILIA ALVES SERCUNDES** **MARIA VITÓRIA FRANÇA SILVA** **REBECCA BEATRIZ DE OLIVEIRA FELIX**
TÍTULO DO ARTIGO CIENTÍFICO:	**ANÁLISE DA RESPONSABILIDADE CIVIL APLICADA NAS DECISÕES DE CRIMES POR VAZAMENTO DE DADOS PESSOAIS SOB A ÓTICA DA LEI N.º 13.709/2018 - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

À

Coordenação do Núcleo de Trabalhos de Conclusão de Curso em Ciências Humanas, Sociais Aplicadas e Engenharias:

Saulo Silva de Miranda, professor-assistente desta IES, na qualidade de Orientador do Trabalho de Conclusão de Curso – TCC acima qualificado, vem respeitosamente apresentar o seguinte PARECER:

CONSIDERANDO QUE,

- As estudantes participaram dos encontros de orientação do TCC, cumprindo com os requisitos de assiduidade e pontualidade, tendo cumprido as obrigações perante a instituição e seu orientador quanto à elaboração do artigo;
- O grupo elaborou o TCC acima nomeado a partir de um tema relevante e atual, ainda em maturação no Brasil em razão de contar com uma legislação ainda nova, conseguiu contemplar em sua abordagem aspectos importantes em relação a avanços e desafios em relação ao tema;
- Os estudantes cumpriram os requisitos estabelecidos em relação aos aspectos formais, metodológicos e ortográficos previstos nas regras desse Núcleo.

RESOLVE:

Autorizar o depósito do TCC em epígrafe para submissão à banca de avaliação como requisito parcial para conclusão do curso de direito, se manifestando, desde já, pela sua aprovação, com a nota máxima.

É o parecer.

Caruaru-PE, 04 de março de 2023.

Saulo Silva de Miranda

Orientador