INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS E O DANO MORAL *IN RE IPSA*

ROSSO, Angela Maria[1]
SOUZA, Ieda Maria Berger[2]

RESUMO:

A partir da percepção de que dados pessoais são o mais importante ativo na economia de dados e que o mau uso dessas informações pode conduzir a tratamentos altamente discriminatórios, gerou-se a necessidade de proteção do sujeito de dados. Seja como um aspecto do direito à privacidade ou como um direito fundamental autônomo, o tema ganhou relevância. A Lei n. 13.709/2018 trouxe às organizações um dever de segurança como um requisito de licitude para o tratamento dos dados, contudo não estabeleceu critérios de responsabilização por danos causados. Entre tantas discussões decorrentes na legislação de proteção de dados, uma que vem sendo enfrentada pelo Judiciário, ainda sem posicionamento uniforme, é se qualquer incidente que envolva o acesso indevido aos dados pessoais, configurando uma violação, é causa suficiente para o reconhecimento do dano moral presumido.

PALAVRAS-CHAVE: Proteção de dados pessoais, dano moral presumido, violação de dados pessoais.

DATA BREACHES AND PRESUMED NON-MATERIAL DAMAGE

ABSTRACT:

From the perception that personal data are the most important asset in the data-driven economy and the misuse of this information can lead to discriminatory treatments generated, by the need for protection of the data subject. Whether as an aspect of the right to privacy or as an autonomous fundamental right, the theme gained importance. The law number 13.709/2018, Brazilian data protection law brought to organizations a duty of security as a legality requirement for the data processing. However, it did not establish liability criteria to the cause of the damage. Among discussions about data protection law, one that has been faced by the judiciary without a uniform position is that any security incident that involves improper access to personal data, constituting a violation is sufficient cause for the recognition of the presumed non-material damage.

KEYWORDS: Personal data protection, presumed non-material damage, data breaches.

1 INTRODUÇÃO

A sobrevivência de diversos setores econômicos está diretamente vinculada ao tratamento de dados, especialmente dados pessoais. Na economia de dados, essa dependência torna-se evidente, uma vez que a tomada de decisão que precisa ser rápida e assertiva demanda a utilização de bases de dados cada vez maiores e processamentos ainda mais complexos. Consequentemente, as informações que podem ser obtidas a partir do tratamento desses dados os transformam em objeto de desejo do mercado e do próprio Estado, fato que motiva o número crescente de ataques digitais.

[1] Acadêmica do curso de Direito do Centro Universitário Fag: Angela Maria Rosso, e-mail: amrosso@gmail.com.
[2] Docente orientador do curso de Direito do Centro Universitário Fag: Ieda Maria Berger Souza, e-mail: iedasouza@msn.com

Tecnicamente cada vez mais bem elaborados, tais ataques objetivam tomar posse das bases de dados das organizações públicas ou privadas para posteriormente comercializá-las de forma não autorizada e quase sempre desconhecida pelos titulares dos dados.

O avanço das atividades relacionadas ao tratamento de dados pessoais permite a construção de análises detalhadas de perfil econômico, social, de consumo e de saúde, colocando em contraposição uma economia dependente dessas informações e um indivíduo impotente diante da utilização dos seus dados de forma indevida, inclusive para fins discriminatórios. Pode-se afirmar que a vida da pessoa está mapeada por algoritmos que determinam desde qual produto será ofertado para quem em uma campanha de marketing, passando pelo perfilhamento de posição política e ideológica, chegando a situações violadoras da dignidade humana, como a escolha de alguém para um emprego, o valor diferenciado para a contratação de um plano de saúde ou a prisão de inocentes a partir de reconhecimento facial falho.

Esse cenário mobilizou a sociedade civil a exigir do Estado alguma forma de interferência, a fim de regulamentar o uso das informações pessoais. Dessa forma, os legisladores foram instigados a criar leis de proteção de dados. Na União Europeia, por intermédio do Regulamento Geral de Proteção de Dados – RGPD - houve um endurecimento legislativo e sancionatório. Nos Estados Unidos, verificam-se várias leis setoriais e alguns dos estados implantaram suas próprias regras. Já no Brasil a Lei Geral de Proteção de Dados – LGPD – ganhou corpo e está em vias de entrar em vigor.

A utilização das informações pessoais deve, a partir de agora, seguir as disposições expressas nas legislações fazendo com que aumentem os acessos indevidos caracterizados por acessos não permitidos pela lei ou não autorizados pelo titular dos dados, implicando em violações de dados pessoais, como, por exemplo, compartilhamento e acesso por pessoas não autorizadas. Como consequência, o Judiciário tem sido acionado, uma vez que, a depender de qual modalidade de informação pessoal foi acessada indevidamente, o dano causado ao seu titular pode ser irreversível.

O posicionamento jurisdicional relativo ao uso indevido de dados pessoais ainda é bastante tímido e resultado de um momento histórico e legislativo diferente, anterior à existência de legislação reguladora. Até 2018 o Brasil não contava com uma legislação que tratasse efetivamente da proteção dos dados pessoais, acarretando assim um entendimento não uniforme. Decorre dessa situação a existência de julgados que entendem que o dano moral proveniente do acesso não autorizado aos dados pessoais é presumido, bem como há posicionamento de que não é. As discussões sobre o tema envolvem a importância e/ou nível de pessoalidade dos dados que foram

acessados indevidamente, apresentando decisões que se baseiam em uma espécie de valor do dado pessoal para o seu titular.

Diante da ausência dessa pacificação, resultante também da novidade do tema, no ordenamento jurídico nacional surge a problemática abordada pelo presente trabalho, a existência ou não de dano moral presumido decorrente do acesso não autorizado aos dados pessoais. Dentre as hipóteses a serem analisadas, duas serão aqui tratadas. A primeira defende a configuração do dano moral *in re ipsa* diante do acesso não autorizado, porque inequívoco o prejuízo extrapatrimonial do sujeito de dados. Em contraposição, há o entendimento de que o dano moral em caso de acesso não autorizado aos dados pessoais não é presumido, precisando ser provado pelo titular dos dados violados, visto que existe apenas expectativa de dano. Some-se a essa hipótese a conhecida vulnerabilidade dos sistemas de tecnologia que impedem ambientes totalmente seguros.

Diante do exposto, o presente trabalho adquire importância, uma vez que além da LGPD o Estado tem investido em políticas de incentivo da evolução tecnológica do país, especialmente no tocante aos Decretos nº 9.319/18 e nº 9.854/19, que tratam, respectivamente, da Estratégia Brasileira para a Transformação Digital e do Plano Nacional de Internet das Coisas. Ambos os projetos, essencialmente, dependem do tratamento de um grande volume de dados, incluindo os dados pessoais, para alcançarem seus objetivos.

Além disso, cresce no mundo a discussão acerca da utilização pelo próprio Estado de informações pessoais para monitoramento e vigilância dos cidadãos especialmente em situações de crise. Partindo do pressuposto de que quanto mais dados pessoais são utilizados pelas organizações, maior é a probabilidade de ocorrência de acessos indevidos ou vazamentos, o principal objetivo deste trabalho é buscar esclarecer com base na lei, no entendimento judicial comparado e na doutrina se a ocorrência de acessos não autorizados a dados pessoais bastaria para configurar o dano moral presumido.

Para atingir seu objetivo, o artigo inicia-se contextualizando a proteção de dados sob o aspecto de direito fundamental, esclarecendo questões técnicas sobre o dever de segurança e definindo o que seriam os acessos não autorizados aos dados pessoais. A seguir, aborda os danos que podem resultar do acesso indevido para o titular dos dados, adentrando, ainda, nos aspectos de caracterização do dano moral presumido. Na sequência faz uma análise do tratamento judicial dispensado no Brasil e no Judiciário dos Estados Unidos e de alguns países pertencentes à União Europeia, quando confrontados em relação ao tema. Por fim, apresenta as conclusões obtidas a partir da problemática e das hipóteses discutidas ao longo do texto.

2 CONTEXTUALIZAÇÃO: DIREITOS FUNDAMENTAIS

O rol de direitos fundamentais transformou-se e ampliou-se ao longo da história, adaptando-se à realidade fática. À medida que o ser humano se tornou o centro de atenção do Direito, novas garantias foram positivadas, para que ele consiga vivenciar sua humanidade.

Esse processo evolutivo de ampliação da proteção ao indivíduo está representado nas gerações de direitos fundamentais. Enquanto a primeira geração abarca direitos ligados à liberdade, afastando o Estado opressor pela imposição de uma obrigação de não fazer, a segunda geração - em outro momento histórico - traz uma exigência de prestação estatal positiva do Estado, em que se busca atingir a igualdade isonômica entre os indivíduos. A terceira geração passa pela percepção de que não basta a atuação do Estado para que o humano tenha uma vida digna; é preciso que um indivíduo esteja atento ao outro, criando assim direitos decorrentes da solidariedade (MARMELSTEIN, 2019).

Fato é que a sociedade não parou de evoluir, novos riscos à pessoa surgiram, muitos deles decorrentes do avanço tecnológico. Coube ao Direito acompanhar tais mudanças, uma vez que, se existem novas ameaças, novas garantias precisam ser criadas. Desse modo, para encampar esses novos direitos, a doutrina apresenta outras gerações compostas por novos direitos fundamentais, sendo um deles o direito à proteção de dados pessoais (DONEDA, 2020).

De acordo com Marmelstein (2019), os direitos fundamentais têm características próprias. Para que um direito se enquadre nessa categoria, é preciso que nele se possam identificar os aspectos ético e normativo. O primeiro, vinculado ao conteúdo do direito em si, representa uma limitação ao poder estatal, assume o papel de garantidor da dignidade humana; já o segundo, o aspecto normativo, só estará presente se o direito estiver institucionalizado e constitucionalizado.

Nas palavras do autor, “se determinada norma jurídica tiver ligação com o princípio da dignidade da pessoa humana ou com a limitação do poder e for reconhecida pela Constituição de um Estado Democrático de Direito como merecedora de uma proteção especial, é bastante provável que se esteja diante de um direito fundamental” (MARMELSTEIN, 2019, p.19).

Para o referido autor, apesar de a sociedade vivenciar uma clara expansão do rol de direitos fundamentais, há um crescimento nas ameaças à dignidade humana, vinculadas, principalmente, aos temas de segurança pública e ao liberalismo econômico, situação em que direitos relativos à privacidade e à liberdade têm sido mitigados e, por vezes, suprimidos.

2.1 A PROTEÇÃO DE DADOS COMO UM ASPECTO DO DIREITO À PRIVACIDADE

O direito à privacidade previsto no art.5º, X, da Constituição Federal é um direito fundamental. Um direito que surgiu no final do século XIX, fortemente ligado ao direito de propriedade, decorrente do desejo da burguesia de proteger-se do olhar alheio, passou pela concepção do "direito de ser deixado só", calcada por Warren e Brandeis (*apud* DONEDA, 2020, p.31), ganha atualmente novas feições para tratar do aspecto informacional. Sob esse prisma, afirma o autor que "a privacidade é um aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade".

Apesar de ser profundamente estudado, o direito à privacidade nunca encontrou definição fechada. Solove e Schwartz (2015) explicam que a lei não determina o que estaria abrangido no conceito de privacidade, mas que delimita algumas situações relativas à privacidade, que devem ser protegidas. Para alguns, a privacidade é o que separa a esfera privada da esfera pública, onde o Estado não pode alcançar. Ao longo do tempo, as definições variaram, contudo não se conseguiu encontrar uma definição precisa para o termo.

Por isso, ao tomar a proteção de dados como um aspecto da privacidade, há dificuldade em garantir a concretização de sua proteção diante da evolução da sociedade para um ambiente hiperconectado, que se intitula "sociedade da informação" (BIONI, 2019, p.4). Nessas sociedades, "nós somos as nossas informações, pois elas nos definem, nos classificam, nos etiquetam" (RODOTÀ, 2008, p.7). Trata-se de um tempo em que a informação, especialmente aquela atinente às pessoas, ganha *status* de ativo econômico para as organizações, tornando-se "o (novo) elemento estruturante que (re)organiza a sociedade" (BIONI, 2019, p.4).

Diante dessa configuração informacional social e econômica, o número de episódios de utilização ilegítima das informações de caráter pessoal multiplicou-se, sendo que alguns desses episódios têm potencial para atingir um número muito grande de indivíduos. Há uma mudança na forma de exposição da vida privada, que passa a se dar "com maior frequência por meio da divulgação de seus dados pessoais do que [...] por meios 'clássicos' de violação da privacidade" (DONEDA, 2020, p.23).

Dados pessoais carregam em si informações acerca de quem é o indivíduo social, econômica e biologicamente, uma vez que entre eles existem informações cadastrais, de consumo, de saúde, dados genéticos e biométricos, de posição ideológica ou religiosa que permitem identificar de forma única cada pessoa. Destaca, ainda, Doneda (2020) que esses dados devem ser considerados como componentes da personalidade humana e, por isso, merecem proteção especial, visto que, a partir deles, é possível construir uma representação do sujeito por meio da qual é possível a formação de

juízo de valor sobre o indivíduo representado. O resultado dessa análise poderá ser utilizado, por exemplo, para verificar se o indivíduo pode receber uma linha de crédito, entrar em um determinado país, se conseguirá ser empregado, qual o valor que custará seu plano de saúde.

Nesse contexto, a posse da informação pessoal ganha aspecto de poder e controle sobre o sujeito de dados. O aumento do fluxo informacional e o uso contumaz de processamentos transformam esses dados em fonte inesgotável de oportunidades. Assim, obter vantagens econômicas e mesmo políticas pela utilização dessas informações é uma possibilidade que pode levar a uma rotina de utilização não autorizada ou indevida. Afinal, quanto maior o número informações processadas, melhores as respostas obtidas para a utilização em atividades de *marketing*, de vendas, de controle social, implicando a violação de outros direitos fundamentais, dentre eles, o próprio direito à liberdade. Acarreta-se, assim, uma "perda de nossa autonomia, de nossa individualidade e, por fim, de nossa liberdade" (DONEDA, 2020, p.23).

Casos de repercussão internacional demonstram como o acesso não autorizado aos dados pessoais viola direitos fundamentais constitucionalmente previstos e ameaça a própria democracia. *Cambridge Analytica* ganhou espaço em todas as mídias e transformou-se em motivo de investigação do Congresso Americano, após a descoberta de que pesquisas realizadas pela organização, fazendo uso de acesso aos dados pessoais dos usuários de uma rede social, deram o tom da última eleição ocorrida nos Estados Unidos. Em breve resumo, o que ocorreu foi que, a partir do tratamento das informações pessoais a que teve acesso, a empresa realizou marketing direcionado de forma que eleitores indecisos foram convencidos a votar em um dos candidatos ao pleito. Além do processo eleitoral americano, a mesma técnica foi usada como forma de promover o *Brexit*, evento que decidiu pela saída do Reino Unido da União Europeia. Para Persily (2016), em ambas as situações, a liberdade de escolha dos indivíduos envolvidos foi cerceada, fazendo com que a própria sobrevivência da democracia fosse questionada diante dessa possibilidade de manipulação de dados.

Outro caso que merece ser apresentado é a exigência imposta pelo governo dos EUA, de acesso ao histórico dos últimos cinco anos de utilização das redes sociais, daqueles que desejarem o visto para acessar o país (VEJA, 2019). Tal situação afeta diretamente a liberdade de ir e vir das pessoas entre os países, uma vez que se submete a vida privada do indivíduo, situações que ele compartilhou, opiniões que emitiu em seu perfil nas redes sociais a um escrutínio como condição para aceitar aquela pessoa no país ou não.

Há, portanto, clara transcendência do direito à privacidade, uma vez que manifestamente a utilização dos dados pessoais pode levar à restrição de outros direitos, nesse sentido afirma Doneda

(2020). Contudo, é preciso que se registre que existem pesquisadores que seguem a linha de Schreiber (2019), de que o direito à proteção de dados é um aspecto do direito à privacidade, uma vez que este pode se subdividir em várias facetas.

2.2 A PROTEÇÃO DE DADOS COMO UM DIREITO AUTÔNOMO

A existência do direito à proteção de dados pessoais é inquestionável. O que se discute no Brasil é a necessidade de que ele seja incluído de forma expressa no rol dos direitos fundamentais como um direito autônomo e desvinculado do direito à privacidade.

Para Lambert (2018, p.46), existir um direito à proteção de dados representa "o reconhecimento legislativo e político que a sociedade respeita a proteção de dados e informações dos indivíduos". Essa compreensão é importante, devido ao valor econômico e estratégico que circunda tais dados, fazendo com que seja atribuída a tal direito autonomia, alcançando assim o *status* de um novo direito da personalidade. Afirma Doneda (2020, p. 33) que

> A informação pessoal – que compreende toda informação que se refere diretamente a uma pessoa – assume, portanto, importância por pressupostos diversos. Podemos estabelecer, de início, dois fatores que estão quase sempre entre as justificativas para a utilização de informações pessoais: o controle e a eficiência. Uma série de interesses se articula em torno desses dois fatores, envolvendo o Estado e entes privados.

Colocar a proteção dos dados pessoais sob o manto constitucional traz aos indivíduos a garantia de que, caso exista violação ao direito, ele esteja automaticamente salvaguardado pelo direito de reparação civil (BRASIL, 1988). Essa percepção é importante em um cenário em que o mercado e o próprio Estado estão cada vez mais dependentes das informações pessoais, o que torna os indivíduos cada vez mais suscetíveis aos prejuízos materiais e morais decorrentes de acessos não autorizados aos seus dados pessoais.

Dessa forma, a necessidade de proteção não se resume somente à inviolabilidade, como acontece com o direito à privacidade; ela é mais ampla. A necessidade existente é de se implementar a total transparência para preservar o controle sob a utilização de tais dados, conceito que decorre do direito à autodeterminação informativa, que se entende como a capacidade do sujeito de dados de saber e poder determinar, exercendo alguns tipos de controle sobre como seus dados pessoais serão tratados (CANOTILHO, 1941). Para Lambert (2018), o direito à proteção dos pessoais é uma forma de garantir que haja respeito, controle e segurança em relação aos tratamentos de dados realizados.

O cenário de mau uso constante das informações pessoais gerou a necessidade de regulamentação estatal do tema. Foram criadas leis que vedam tratamentos de dados que possam gerar informações discriminatórias, bem como o uso das informações pessoais sem o conhecimento do titular de dados. Há, com a instituição dessas leis, uma tentativa de preservação da personalidade do indivíduo pela existência de regramento claro acerca do que é permitido ou não, ou como define Lampert (2018), um reconhecimento do direito do indivíduo de preservar suas próprias informações.

Para a corrente que defende a autonomia do direito à proteção de dados, "Propugnar que o direito à proteção dos dados pessoais seria uma mera evolução do direito à privacidade é uma *construção dogmática falha* que dificulta a sua compreensão" (BIONI, 2019, p. 98-99). Essa parte da doutrina entende que o grau de impacto a que o indivíduo é submetido quando seus dados passam por decisões tomadas por algoritmos, e que podem ocasionar práticas discriminatórias violando a dignidade humana, excede o alcance do direito à privacidade, existindo razões, portanto, para que se estabeleça uma nova espécie de direito dentro da categoria de direitos da personalidade.

Essa perspectiva de independência entre privacidade e proteção de dados foi adotada em decisão célebre do Tribunal Constitucional Alemão em 1983. O Tribunal reconheceu o direito à autodeterminação informativa diante de várias reclamações que questionavam a constitucionalidade da Lei do Censo, que previa que dados dos indivíduos fossem coletados e comparados com os dados dos cidadãos, em posse da Administração Pública. No caso, decidiu a Corte que, diante do avanço tecnológico que processava um volume cada vez maior de dados pessoais, estava o indivíduo abrangido pela proteção do direito da personalidade constitucionalmente previsto:

> O direito fundamental garante o poder do indivíduo de decidir ele mesmo, em princípio, sobre a exibição e o uso de seus dados pessoais"; e continua: "As restrições deste direito à 'autodeterminação sobre a informação' são permitidas somente em caso de interesse predominante da comunidade0 (MARTINS, 2005, p. 233-234).

Outro país que merece destaque é Portugal, que dispõe em sua Constituição expressamente o direito à proteção dos dados pessoais, em seu artigo 35: "é proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei" (PORTUGAL, 1976). Além desses dois Estados, vale mencionar o art. 8º da Convenção Europeia para os Direitos do Homem, que apresenta o direito à proteção de dados pessoais como um direito fundamental (UNIÃO EUROPEIA, 2009).

Este parece também o caminho que está sendo trilhado no Brasil, embora o Marco Civil da Internet – Lei nº 12.965/2014 - tenha trazido a proteção de dados como um princípio a ser observado e que tenha reforçado a garantia da inviolabilidade da vida privada, e a Lei nº 13.709/2018 tenha regulamentado a utilização dos dados pessoais, tramita no Congresso Nacional a Proposta de Emenda Constitucional nº 17, que pretende incluir no artigo 5º da Constituição da República o inciso XII-A, colocando a proteção de dados pessoais no rol de direitos fundamentais expressamente previstos. Na justificação, com o intuito de desvincular o direito à proteção de dados do direito à privacidade, encontra-se o seguinte texto:

> De fato, a privacidade tem sido o ponto de partida de discussões e regulações dessa natureza, mas já se vislumbra, dadas as suas peculiaridades, uma autonomia valorativa em torno da proteção de dados pessoais, de maneira, inclusive, a merecer tornar-se um direito constitucionalmente assegurado (BRASIL, 2019).

Ressalta o documento que outros países, além do já citado Portugal, já constitucionalizaram o direito devido à importância crescente da matéria.

2.3 ASPECTOS GERAIS SOBRE A PROTEÇÃO DE DADOS

Percorrido o caminho histórico de surgimento desse direito e entendendo-o como direito autônomo, faz-se importante definir o seu conteúdo. A Lei nº 13.709/2019 apresenta, em seu art. 5º, I, o dado pessoal como sendo toda "informação relacionada à pessoa natural identificada ou identificável". Pondera BIONI (2019) que somente são alcançados pela lei os dados que recebem o adjetivo de pessoais, e que para chegar à conclusão acerca do pertencimento de um dado a essa classificação, será sempre necessário fazer uma análise do contexto onde o dado pode ser encontrado. Por isso, dados que, sob um primeiro olhar, não se enquadrariam como tal, podem, a depender do processamento que sofrerem, entrar nessa classificação. Dessa forma, pelo conceito de dado pessoal trazido pela LGPD, o rol de dados pessoais é inesgotável, porque o avanço da Inteligência Artificial permite que existam infinitos cruzamentos entre as mais variadas bases de dados distribuídas por todo o ciberuniverso.

Além do conceito geral de dados pessoais, a lei também traz em seu corpo um rol taxativo de dados referentes à pessoa humana, que são considerados sensíveis (BRASIL, 2019). Estão enquadrados nessa definição aqueles dados que possuem uma capacidade maior de violarem outros direitos fundamentais do indivíduo em caso de uso ou exposição indevida (RODOTA, 2004). Entre

eles encontram-se os dados étnicos, de opinião política, de convicção religiosa, dados ligados à saúde, entre outros.

Todo esforço doutrinário e legislativo está concentrado em colocar o sujeito de dados como o único com poder para determinar o que é feito com suas informações pessoais, sendo o único que tem o direito de sobre eles dispor, uma vez que são de sua exclusiva propriedade. Contudo, a efetivação desse direito só acontecerá se o detentor da posse dos dados pessoais cumprir adequadamente os ditames legais.

Nesse ponto, é imprescindível que seja determinada a diferença entre proprietários de dados e seus possuidores. Os primeiros são aqueles a quem a lei atribui a titularidade das informações pessoais. Quanto aos segundos, referidos pela lei como agentes de tratamento, são aqueles que detêm a guarda do dado pessoal e que os utilizam como insumo para a realização de atividades comerciais, econômicas e de políticas públicas, entre outros tratamentos possíveis. São eles que coletam, armazenam, compartilham, modificam, transferem ou realizam qualquer espécie de tratamento sobre os dados pessoais (BRASIL, 2018).

Esses agentes de tratamento que detêm a posse das informações pessoais são pessoas físicas ou jurídicas, de direito público ou privado, independentemente do setor em que atuem, e são classificados como controladores – que são aqueles que dizem o que será feito com o dado e que mantêm contato direto com o sujeito de dados, que utilizam essas informações para atingirem uma determinada finalidade; e os operadores, que, por sua vez, sob determinação dos controladores, realizarão as atividades de tratamento propriamente ditas, a fim de entregarem ao controlador o resultado desejado e entre eles convencionado (BUSSCHE e VOIGT, 2017).

2.3.1 Dever de Segurança

Objetivando efetivar o direito fundamental à proteção de dados, a legislação apresenta no art. 6º da Lei nº 13.709/2018, um rol de princípios que devem ser obedecidos no tratamento das informações pessoais. O dever de segurança é um dos princípios previstos já enraizados no Direito Civil, como a boa-fé, e determina que os agentes de tratamento devem garantir a segurança por meio 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". Reforça tal dever o artigo 44 da mesma lei, que afirma que "será irregular" o processamento de dados pessoais que "não fornecer a segurança que o titular dele pode esperar", salientando o parágrafo único do referido artigo que "responde pelos danos decorrentes da

violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança [...], der causa ao dano" (BRASIL, 2018).

Para a doutrina, o dever de segurança deve garantir que: "Dados pessoais devem ser tratados de modo que seja garantida a segurança apropriada dos dados pessoais, incluindo a proteção contra acesso não autorizado ou processamento ilícito e contra a perda acidental, destruição ou dano" (BUSSCHE e VOIGT, 2017, p. 92). A existência desse princípio na lei está calcada no risco de violação dos direitos fundamentais do sujeito de dados, proveniente da utilização indevida ou ilícita resultante de acessos indevidos ou não autorizados das suas informações pessoais. O risco pode ser exemplificado pela "discriminação, roubo de identidade ou fraude, perdas financeiras, dano reputacional ou qualquer outra desvantagem econômica ou social; [...] privação de direitos ou liberdades [...]; dados de crianças ou outras pessoas em situação de vulnerabilidade serem processados" (BUSSCHE e VOIGT, 2017, p. 40-41).

Assim, garantir a segurança no tratamento das informações pessoais é o meio para evitar que direitos fundamentais sejam violados. A LGPD dispõe em seu artigo 46, sobre a obrigatoriedade dos agentes de tratamento de empregarem mecanismos que evitem a violação dos dados pessoais, incluído acessos indevidos (BRASIL, 2018). Entende a doutrina que o nível de segurança adequado é aquele proporcional aos riscos que cada processamento representa para o seu titular. De acordo com Lambert (2018), o nível de segurança a ser empregado é definido pela probabilidade e gravidade de violação de determinados dados pessoais, por exemplo, informações de saúde merecem maior cuidado do que informações cadastrais.

As medidas de segurança a serem implementadas encontram guarida em padrões de boas práticas existentes no meio da Segurança da Informação. A família ISO 27000 é responsável por indicar quais controles devem ser implantados e como deve ser montado um sistema de gerenciamento de segurança da informação, de forma a garantir a segurança no tratamento de dados. A abordagem é construída sobre o tripé: confidencialidade – implementação de controles de segurança da informação para garantir que o dado somente pode ser acessado por pessoas, sistemas ou processos que tenham autorização para tal; integridade – controles de segurança da informação, que garantam que o dado não será alterado por pessoas, sistemas ou processos não autorizados; e, por fim, disponibilidade – o dado deve estar disponível sempre que pessoas, sistemas ou processos autorizadas precisarem ou desejarem acessá-lo (ABNT, 2014).

Dos três aspectos relativos ao dever de segurança, este trabalho dará atenção especial à confidencialidade. Quando um tratamento de dados não atender a esse requisito, podem ocorrer situações em que a informação pessoal seja acessada por quem não tenha autorização para tanto.

Resta, nesses casos, caracterizado um incidente de segurança da informação, denominado "violação de dados pessoais".

2.3.2 Acesso não autorizado – violação do direito à proteção de dados

A concretização do direito à proteção de dados pessoais depende, portanto, do adimplemento do dever de segurança por parte dos agentes de tratamento de dados. A ausência de medidas técnicas, administrativas e físicas de controle de acessos a essas informações facilita a ocorrência de incidentes de acessos não autorizados. Caracterizam-se, como tais, todos aqueles acessos realizados por pessoas, sistemas ou processos não autorizados ou com desvio da finalidade para a qual os dados foram coletados. Ou seja, se determinado dado foi coletado para uma finalidade específica, ele somente pode ser utilizado para concretizá-la. Essa conclusão deriva do expresso no art. 6º, I, da LGPD, que dispõe como princípio basilar do tratamento de dados a "finalidade: realização do tratamento para propósitos legítimos, específicos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades".

É comum o pensamento de que o acesso não autorizado ocorreria somente em eventos de invasões ou de furto dessas informações. Contudo, o acesso indevido pode ocorrer de forma ainda mais sutil quando os dados são compartilhados ilegitimamente com terceiros que a princípio não deveriam ter acesso.

Os eventos de furtos – conceito penalmente discutível - de dados são, contudo, os que têm potencial para produzir maior impacto ao sujeito de dados. Isso porque as consequências desses eventos são, em regra, não rastreáveis e expõem o titular dos dados à fraude e ao furto de identidade (LAMBERT, 2018). Nesses casos, é possível, por exemplo, fazer movimentações financeiras ou se fazer passar pela própria pessoa proprietária dos dados.

Para Tanner (2017), ainda mais grave é a situação em que dados sensíveis, de saúde, sexuais, biométricos, entre outros, sejam indevidamente acessados e expostos. Perseguição política em regimes totalitários, discriminação em caso de consumo de medicamentos controlados, entre tantas outras situações. O risco de que essa pessoa seja submetida à discriminação é alto, e o dano é permanente.

Pode-se afirmar, portanto, que só é devido e autorizado o acesso aos dados pessoais quando respeitadas as bases legais e finalidades previstas na lei.

3 A CONFIGURAÇÃO DO DANO MORAL

Enquanto a configuração do dano material é de fácil verificação e valoração na seara civilista, o mesmo não se pode dizer quanto ao dano moral. A aceitação da existência do dano moral foi construída ao longo da história legislativa, doutrinária e jurisprudencial.

A Constituição da República de 1988 pacificou a existência do dano moral indenizável em seu artigo 5º, inciso X, assegurando o direito de indenização no caso de violação do direito à intimidade, à vida privada, à honra e à imagem. Na seara infraconstitucional, merecem destaque o art. 186 do Código Civil e o art. 6º, inciso VI, do Código de Defesa do Consumidor, que consolidam a existência do dano moral.

De forma preponderante, a doutrina associa o dano moral a "lesões aos direitos da personalidade", ou seja, "que restaria configurado sempre que houvesse uma lesão a "elementos essenciais da individualidade" (TARTUCE, 2018, p. 292). Conforme Gagliano e Stolze (2017, p. 115 e 135), o "conteúdo não é pecuniário nem comercialmente redutível a dinheiro" onde "a certeza do dano decorre da efetiva violação do direito na esfera extrapatrimonial". Tais entendimentos podem ser resumidos na definição de Gonçalves (2015, *apud* TARTUCE, 2018, p. 292): "dano moral é o que atinge o ofendido como pessoa, não lesando seu patrimônio. É lesão de bem que integra os direitos da personalidade, como a honra, a dignidade, a intimidade, a imagem e o bom nome".

Diante da posição doutrinária, o simples acesso não autorizado aos dados pessoais se configuraria como uma violação a um direito fundamental, independentemente de se entender a proteção de dados como um direito da personalidade autônomo ou decorrente do direito à privacidade. Ou seja, independentemente do produto da violação ao direito, existirá o dano moral. Ressalte-se, contudo, que em alguns casos as consequências são desastrosas, como no caso Ashley Madison, em que pessoas tiveram suas vidas abaladas de tal forma, diante da revelação de suas informações pessoais (as quais estavam em posse do site de relacionamentos extraconjugais, sob promessa de sigilo), que não suportaram a exposição e cometeram suicídio (LAMONT, 2016).

Para Gagliano e Stolze (2017), existem situações em que verificar a existência do dano moral pode não ser simples, mas nesses casos a dificuldade estaria na seara probatória e não deve ser entendida como óbice para a reparação diante da existência da lesão.

Dessa forma, no caso Ashley Madison, o dano foi nítido, todavia, na maior parte dos incidentes envolvendo dados pessoais, a concretização da ofensa que conduziria à configuração do dano é latente, futura, senão hipotética. É o caso, por exemplo, da falha de segurança existente nos sistemas de uma companhia telefônica, que tornou possível acessar, via portal da internet, dados

pessoais existentes no cadastro de clientes, tais como nome, nome da mãe, entre outros (SCHAEFFER, 2019); ou ainda da exposição de dados pessoais, inclusive endereço de possuidores de carteira nacional de habilitação por falha existente no site do Detran do Rio Grande do Norte (NAKAGAWA, 2019).

Aferir objetivamente se houve dano extrapatrimonial ou simples aborrecimento é a questão que se coloca quando se leva a ofensa para a apreciação do Judiciário. Determinar se é dano ou mero dissabor é essencial, uma vez que não há possibilidade de reparação para o segundo, conforme entendimento pacificado do STJ:

> AGRAVO INTERNO NO RECURSO ESPECIAL. AÇÃO DE INDENIZAÇÃO. ENVIO DE CARTÃO DE CRÉDITO SEM SOLICITAÇÃO DO CONSUMIDOR. AUSÊNCIA DE NEGATIVAÇÃO OU COBRANÇA INDEVIDA. DANOS MORAIS NÃO CONFIGURADOS. MERO ABORRECIMENTO. ABRAVO DESPROVIDO.
> 1. É pacífica a jurisprudência desta Corte no sentido de que os aborrecimentos comuns do dia a dia, os meros dissabores normais e próprios do convívio social não são suficientes para originar danos morais indenizáveis. (STJ – AgInt no REsp: 1655212 SP 2017/0035891-1, Relator: Ministro Raul Araújo, data de julgamento: 19/02/2019, T4 – Quarta Turma, data de publicação: DJe 01/03/2019)

Doutrinadores de proteção de dados defendem que o mero conhecimento do acesso indevido às informações pessoais pode causar ansiedade e temor no titular dos dados diante do risco iminente da revelação de informações íntimas que poderiam dar causa a grandes desgastes sociais e emocionais (SOLOVE, 2017). Dessa forma, a violação das informações pessoais, ainda que não resulte em consequências aferíveis, ensejaria a configuração do dano.

Para Tartuce (2018, p.292), “a reparação do dano moral não requer a determinação de um preço para a dor ou o sofrimento, mas sim um meio para atenuar as consequências do dano imaterial”. Esse entendimento encontra respaldo no Enunciado 445 da V Jornada de Direito Civil, que afirma ser desnecessário aferir a existência de sentimentos negativos para configuração da existência do dano moral. Tal entendimento é consolidado pelo Tribunal da Cidadania no Recurso Especial n. 1.245.550-MG de 2015, que coloca os sentimentos desagradáveis vivenciados como resultado da lesão que, por sua vez, é fato anterior que prescinde de associação com alguma reação do afetado (BRASIL, 2015).

No tocante à proteção de dados, a dificuldade reside em caracterizar o que seria considerado ato lesivo ou não, acessar indevidamente a informação pessoal, seja por meio de invasão ou qualquer outra modalidade de acesso não autorizado bastaria para concretizar a lesão? Responder a essa questão é fundamental, visto que o dano não se configura diante da mera hipótese de

ocorrência de um fato lesivo, sendo necessário que se evidencie seu acontecimento. Caso "provado o fato lesivo a bem patrimonial ou moral, o dano está ínsito na própria ofensa, decorre da gravidade do ilícito em si" (CAVALIERI, 2014 p.116).

Nesse sentido, destaca Pereira (2018, p.64) que, embora não haja óbice ao reconhecimento de dano futuro, existem requisitos de "certeza, atualidade e subsistência", que devem estar presentes para que se configure a existência de dano ressarcível. Em que pese não exista a necessidade de concretização completa da lesão, é preciso que seja certa sua ocorrência, ou seja, "o que se exclui de reparação é o dano meramente hipotético, eventual ou conjuntural, isto é, aquele que pode não vir a concretizar-se".

3.1 O DANO MORAL PRESUMIDO

Diante do entendimento prevalente na doutrina e na jurisprudência, de que basta a ocorrência do fato lesivo a um direito extrapatrimonial para a configuração do dano moral, é preciso que se discuta se esse dano é presumido ou se sua comprovação depende de construção probatória.

O dano moral objetivo ou presumido não necessita de prova, ocorre *in re ipsa*, a fim de evidenciar um dano que decorre do simples fato ou da simples situação da coisa. Para Gagliano e Stolze (2017, p. 518), o dano *in re ipsa* é aquele que decorre da "força dos próprios fatos. Pela dimensão do fato, é impossível deixar de imaginar em determinados casos que o prejuízo aconteceu" e, continua, "não é necessária a apresentação de provas que demonstração de provas que demonstrem a ofensa moral da pessoa. O próprio fato já configura o dano".

Assim, se ocorreu o acesso não autorizado, o direito já foi violado, existindo desde já a ofensa a um direito fundamental atualmente protegido pelo art. 5º, X da CRFB/88. Analisando sob este prisma, seriam as consequências do acesso indevido do dado mero agravante e restaria configurado desde a efetivação do acesso não autorizado o dano moral presumido (*in re ipsa*). Essa conclusão vai ao encontro do exposto por Garatini e Porto (2017), que defendem que nessa espécie de dano há apenas a necessidade de comprovar a existência de nexo causal entre o fato e o dano.

Para Oliva (2013), a necessidade de existir o dano moral presumido decorre da vinculação do dano extrapatrimonial à existência de sofrimento, em tese, causado pela ofensa que de forma incontestável atingiu a vítima. Assim, como um meio de promover a reparação de forma mais rápida e eficaz, dado que é impossível retornar ao *status quo ante*, assume-se que não há necessidade de comprovação do dano, uma vez que ele seria consequência notória e imediata da ofensa ao direito tutelado. A assunção do dano *in re ipsa* antecipa a compensação pelo prejuízo

imaterial sofrido, uma vez que elimina a fase de produção de provas. Dessa forma, por limitar a possibilidade de defesa do autor da ofensa, não é aplicado de forma genérica, sendo o dano não presumido a regra no ordenamento jurídico.

O Superior Tribunal de Justiça, quando confrontado acerca do tema, tem andado no sentido de confirmar a ocorrência do dano moral presumido nos casos de afronta aos direitos da personalidade. Assim se posicionou no Recurso Especial n. 1.243.699-RJ de 2016 ao se pronunciar sobre o direito à reparação diante da violação do direito à imagem, utilizando como argumento a Súmula 403, emitida pelo próprio Tribunal, que considerou que a veiculação da imagem sem autorização da pessoa retratada configura o dano moral presumido, não exigindo prova da ocorrência de qualquer prejuízo. Nesse mesmo julgamento, considerou como um dos fatores determinantes para o reconhecimento do dado o fato de que a vítima poderia ser facilmente individualizada por meio da imagem (BRASIL, 2016).

Andou no mesmo sentido a Corte no Recurso Especial n. 1.292.141-SP de 2012, ao determinar que quando há ofensa a valores fundamentais previstos na Constituição, como em casos de ofensa à dignidade humana, estará configurado o dano *in re ipsa* (BRASIL, 2012). Esse entendimento foi reafirmado no informativo de jurisprudência n. 513 de 2013 do mesmo Tribunal.

O entendimento doutrinário, por sua vez, é o de que, "provado que a vítima teve o seu nome aviltado, ou a sua imagem vilipendiada, nada mais lhe será exigido provar, por isso que o dano moral está *in re ipsa*; decorre inexoravelmente da gravidade do próprio fato ofensivo, de sorte que, provado o fato, provado está o dano moral" (CAVALIERI, 2014, p.116). Em outras palavras, basta que ocorra grave afronta a algum direito da personalidade para que se esteja diante de um dano presumido.

No tocante aos dados pessoais, destaca Solove e Citron (2017) que não se vislumbra outra motivação para o acesso indevido, no caso de invasões a bases de dados, por exemplo, que não seja o seu uso para fraudar ou para assumir a identidade de outra pessoa.

Tanner (2017), ao tratar da utilização não autorizada dos dados pessoais pela indústria farmacêutica, destaca o potencial ofensivo de tal conduta. Para representar a densidade da agressão aos direitos do sujeito de dados, o autor apresenta como exemplo a situação de acesso indevido aos dados de pacientes portadores de enfermidades mentais e o quão discriminatório pode ser o tratamento destinado a esses indivíduos, caso essas informações se tornem públicas.

A Lei nº 13.709/2018 deixa clara a existência da preocupação em relação ao potencial discriminatório conferido a alguns tipos de tratamentos de dados pessoais. Tanto é assim que a não discriminação é princípio expresso no corpo da lei. Portanto, nenhum tratamento de dados que

possa levar à discriminação do indivíduo será lícito e por isso não pode ser admitido (BRASIL, 2018). Não obstante, o tratamento de dados com fins discriminatórios, por si só, violaria a boa-fé, princípio geral do Código Civil.

Na medida em que acessos não autorizados aos dados pessoais ensejam tratamento indevido, há grande potencial lesivo da dignidade humana, visto que os dados pessoais poderiam ser utilizados para causar prejuízo ao seu titular. Nesses casos, além da violação do direito fundamental à privacidade e do direito à proteção de dados, também restaria violada a dignidade humana. Indo ao encontro da teoria defendida por Solove e Citron (2017), de que não há no acesso não autorizado aos dados pessoais outra intenção que não seja a de sua utilização para fins não benéficos ao seu titular.

A partir do pressuposto de que o acesso indevido aos dados pessoais viola fundamento constitucional e, considerando o entendimento já exarado pelo Superior Tribunal de Justiça, ao julgar o já citado Recurso Especial n. 1.292.141-SP de 2012, segundo o qual, para a configuração do dano moral presumido, basta demonstrar que existiu ofensa injusta à dignidade humana (BRASIL, 2012), parece ser coerente defender a existência dessa espécie de dano moral em situações de acesso não autorizado aos dados pessoais.

3.2 A LIMITAÇÃO TÉCNICA DA SEGURANÇA DA INFORMAÇÃO COMO CAUSA PARA A DESCARACTERIZAÇÃO DO DANO MORAL PRESUMIDO

Conforme já apresentando no texto, a LGPD traz um dever de segurança que se consubstancia na necessidade de o agente que realizar o tratamento de dados pessoais garantir que o mesmo acontecerá sem interferências não autorizadas, sob pena de responsabilidade.

De forma contundente, Mitnick e Simon (2006, p.3) afirmam nas primeiras linhas de sua obra:

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim a empresa ainda estará vulnerável.

Ou seja, diante da capacidade dos atacantes, não há tecnologia que resista. Ao longo da obra, os autores demonstram como a maior parte das informações é fornecida mediante um simples pedido. Isso é muito comum em ataques denominados de engenharia social, nos quais uma pessoa

amistosa e prestativa, utilizando-se da facilidade de comunicação que lhe é característica, faz com que a vítima entregue a informação que deseja, sem que esta nem se dê conta do que está acontecendo.

Para exemplificar a impossibilidade de construir ambientes tecnológicos e físicos definitivamente seguros, vale mencionar o caso Snowden, envolvendo a retirada de informações sigilosas de dentro da Agência Nacional de Segurança dos EUA – NSA. Embora o caso não trate de dados pessoais, a situação ilustra como um funcionário da mais alta confiança pode burlar qualquer mecanismo de segurança e colocar uma organização em risco. Sobre o caso, posiciona-se Scudere (2015, p. 78): "Snowden não cometeu *hacking*, e sim roubo puro e simples de informações usando suas credenciais de acesso aos sistemas da NSA e tomando posse da identidade de outro usuário com nível de acessos superior ao seu". O caso, vale ressaltar, causou grande comoção mundial, uma vez que atingiu a privacidade de vários governantes, entre eles, pode-se citar a revelação do monitoramento dos e-mails da presidente brasileira à época e da primeira-ministra alemã, tendo sido este um dos motivos que conduziram os governos a editarem leis com vistas a regular a proteção de dados .

Diante desse quadro de vulnerabilidade, parece inviável a caracterização do dano moral presumido diante de qualquer acesso indevido aos dados que caracterize um incidente de segurança à luz da LGPD. Conforme Sombra (2019), para atender aos dispositivos da LGPD acerca da segurança da informação, é preciso que as políticas de segurança da informação sejam construídas com base na prevenção de incidentes que resultem na quebra da confidencialidade, integridade e disponibilidade do dado pessoal, mas também de forma a permitir uma rápida resposta no caso de o incidente ocorrer.

Em face desse fato, cabe analisar se existe razoabilidade na adoção do dano moral presumido em situações de violação da confidencialidade dos dados. Entende a doutrina que, sempre que o legislador quis que a responsabilidade objetiva fosse adotada, ele deixou explícito no texto legal. Dessa forma, de acordo com Tasso (2020, p.106), não há que se falar em dano moral presumido para situações de violação de dados em que o responsável pelo tratamento dos dados seja pessoa jurídica de direito privado ou uma pessoa natural. Assim, "não há na Lei Geral de Proteção de Dados qualquer artigo que se valha da expressão 'independentemente de culpa' ou 'independentemente da existência de culpa', a indicar de modo inequívoco que o regime jurídico adotado fora o da responsabilidade objetiva."

Para o citado autor, a LGPD traz, ao longo de seu texto, várias indicações de que a utilização das melhores práticas voltadas a garantir a segurança dos dados pessoais é causa atenuante para as

sanções prescritas no texto legal, o que não coaduna com a adoção da responsabilidade objetiva, que levaria ao dano moral presumido. Tal entendimento encontra guarida em alguns artigos da referida lei que preveem a possibilidade de o agente de tratamento dos dados pessoais comprovar que agiu de maneira a evitar a ocorrência do ato ilícito, afastando assim a sua responsabilidade.

Dessa forma, o artigo 6º, X, da Lei nº 13.709/18 determina que o agente deve demonstrar que adotou meios adequados para garantir a proteção de dados que, em última instância, correspondem ao dever de cumprir o disposto no ordenamento jurídico. Quanto à responsabilidade do agente de tratamento, a lei traz excludentes especificadas no artigo 43, quais sejam, o agente deve provar que não realizou o tratamento a ele atribuído, que ainda que tenha realizado o tratamento atribuído não violou a legislação sobre proteção de dados ou ainda a culpa exclusiva do titular dos dados ou de terceiros.

Ademais, a lei apresenta, ainda no artigo subsequente, situações que configuram o tratamento irregular que pode se caracterizar pela forma como os dados são tratados, por resultados e riscos razoavelmente esperados e ainda pela técnica disponível ao tempo em que o tratamento foi realizado, e acrescenta como fato gerador da responsabilidade a negligência em utilizar as medidas de segurança especificadas na lei. Chama ainda a atenção o fato de que o rol presente no dispositivo não é taxativo, uma vez que o texto assim dispõe: “entre as quais”.

Outro ponto apresentado por Tasso (2020) é que a LGPD, inclusive pelo seu contexto de criação e pelo sistema econômico altamente dependente da utilização dos dados pessoais, deve ser compreendida como uma lei que fortalece a evolução tecnológica de forma a privilegiar a inovação e a livre iniciativa.

Nesse cenário, deve-se recorrer às premissas da constitucionalização do Direito Civil, de tal forma que o caráter punitivo da lei não pode se sobrepor ao direito à livre iniciativa, sob pena de perder-se a proporcionalidade que deve existir quando se estiver diante de um conflito aparente entre fundamentos constitucionais, quais sejam a dignidade da pessoa humana e a livre iniciativa. Sob esse aspecto, não faz sentido que qualquer acesso indevido aos dados pessoais seja fato gerador de dano moral *in re ipsa*. Nessa linha, faz-se necessário considerar que o desenvolvimento social que permitirá que objetivos fundamentais constitucionalmente previstos, tais como a garantia do desenvolvimento nacional e a cooperação para o progresso da humanidade, passam necessariamente pela evolução tecnológica atualmente calcada no tratamento de dados inerente, ao qual existem riscos.

4 ENTENDIMENTO JUDICIAL

4.1 TRIBUNAIS NO BRASIL

Em se tratando do acesso indevido aos dados pessoais, os tribunais brasileiros têm-se posicionado na medida em que vêm sendo acionados pelos titulares de dados. O Superior Tribunal de Justiça, em julgamento do Recurso Especial n. 1.758.799/MG, relatado pela Ministra Nancy Andrig, adotou importante posicionamento que pode servir como precedente para futuras decisões quando o objeto do processo for a utilização indevida de dados pessoais. O acórdão proferido resolveu uma demanda em que um sujeito de dados questionava e pedia reparação em virtude do dano moral ocorrido pelo compartilhamento não autorizado de seus dados pessoais. No caso, o STJ entendeu que, quando os dados pessoais são acessados indevidamente em uma relação jurídica fundada no Direito consumerista, resta configurado o dano moral presumido:

> RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL *IN RE IPSA*. JULGAMENTO: CPC/15
> 6. O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas.
> 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar imediatamente, a ofensa aos direitos da personalidade.
> [...]
> 9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulga-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais.
> [...]
> 10. Hipótese em que se configura o dano moral *in re ipsa*. (STJ -REsp: 1758799 MG 2017/0006521-9, Relatora: Ministra Nancy Andrighi, data de julgamento: 12/11/2019, T3 Terceira Turma, data de publicação: DJe 19/11/2019).

A decisão do STJ reflete o entendimento adotado por muitos dos tribunais de justiça estaduais. Ainda no ano de 2012, o TJ- SP, no julgamento da apelação 9.000.703-75.2011.8.26.0037, de relatoria do Desembargador Maury Bottesini, manteve a decisão em primeiro grau que condenou uma empresa de telefonia por fornecer os dados da autora ao ex-marido, com

fundamento no Código de Defesa do Consumidor e sob a alegação de violação do já anteriormente mencionado art. 5º, X da CRFB/88. A saber:

> APELAÇÃO. TELEFONIA CELULAR. VIOLAÇÃO DE DADOS SIGILOSOS. FALHA NOS SERVIÇOS PRESTADOS. INDENIZAÇÃO DEVIDA. SENTENÇA CONFIRMADA. RITJSP, ART. 252. RECURSO IMPROVIDO
> 1.“inequívoca a ocorrência de dano moral que, em casos da espécie não depende de demonstração: sua existência é presumida, e decorre da observação daquilo que ordinariamente acontece, sendo devida a indenização pelo sofrimento moral injusto e grave infligido pela divulgação indevida a terceiro de seus dados telefônicos. (TJSP – Apelação: 9000703-75.2011.8.26.0037, Relator: Maury Bottesini, data de julgamento: 05/09/2012, data da publicação: 06/09/2012)

Ainda na esfera consumerista, já decidiu o Tribunal de Justiça do Paraná, no recurso Inominado n. 0023501-13.2014.8.16.0182, de relatoria da Juíza Liana de Oliveira Lueders, que o vazamento de informações pessoais configura dano moral:

> RECURSO INOMINADO. AÇÃO DE REPARAÇÃO DE DANOS MORAIS. ENVIO DE E-MAIL FALSO QUE CONTEMPLA A AUTORA EM DOIS INGRESSOS PARA A COPA DO MUNDO DE 2014. VAZAMENTO DE INFORMAÇÕES PESSOAIS. DANO MORAL CONFIGURADO. FALHA NO SISTEMA DE SEGURANÇA DO SITE DA RÉ. SENTENÇA MANTIDA. Recurso conhecido e desprovido. Decidem os Juízes integrantes da 1ª Turma Recursal do Estado do Paraná, por unanimidade de votos, CONHECER E NEGAR PROVIMENTO ao recurso, mantendo-se a decisão singular por seus próprios fundamento.[...] quanto aos danos morais, evidente a sua ocorrência, uma vez que o consumidor, ao se deparar com seus dados pessoais expostos – ainda que apenas via e-mail – viu-se impotente, já que não sabe em que proporção houve o vazamento das informações, as quais poderiam estar posse de terceiros de má-fé (TJ-PR - RI: 00235011320148160182 0 PR 0023501-13.2014.8.16.0182/0 (Acórdão), Relator: Liana de Oliveira Lueders, Data de Julgamento: 06/06/2015, 1ª Turma Recursal, Data de Publicação: 11/06/2015).

Contudo, a presunção do dano em casos de acesso indevido às informações pessoais não se restringe às relações regidas pelo CDC. O Tribunal de Justiça do Rio de Janeiro ao resolver a apelação n. 0.071.614-40.2012.8.19.0002, de relatoria do Desembargador Juarez Fernandes Folhes, em que se pleiteava o dano moral decorrente de uma falha no sistema em um portal de comércio eletrônico, em que hackers invadiram a conta do autor, tendo alterado sua senha e dados cadastrais. Entenderam os desembargadores da Vigésima Sexta Câmara Cível do Tribunal de Justiça do Estado do Rio de Janeiro por ratificar a sentença exarada em primeiro grau, que declarou que a situação se enquadrava na Teoria do Risco do empreendimento, aplicando a responsabilidade objetiva ao caso, com fundamento no art. 927, parágrafo único, do Código Civil. A afirmação importante retirada dessa decisão, contudo, é de casos em que existam invasões de hackers que acessem indevidamente

dados pessoais de usuários é de que tais situações são consideradas como fortuito interno, não afastando a responsabilidade de indenização à vítima.

Todavia, é possível encontrar também decisões que afastam o dano presumido. O TJ-DF, em sede de apelação, afastou o dano moral pleiteado pelo autor em relação ao vazamento de informações pessoais do banco de dados da ré, por ausência de comprovação de que os dados foram efetivamente acessados. Na apelação julgada sob o n. 20140110578872, o referido tribunal alegou que o consumidor não logrou êxito em comprovar que fora atingido pelos vazamentos de dados noticiados. Alegou o tribunal que a presunção de ocorrência no incidente de segurança não configura prova suficiente para condenar a ré em danos morais.

Também foi afastada a ocorrência do dano moral presumido no Recurso Inominado n. CNJ 0030108-65.2013.8.21.9000 (n. local 71004537700) julgado pela Primeira Turma Recursal Cível do Tribunal de Justiça do Rio Grande do Sul. Na citada ação, alunos de uma universidade pleitearam indenização por danos morais por terem seus dados cadastrais divulgados indevidamente em um grupo de e-mail da instituição de ensino superior. Entendeu a turma recursal pela inexistência de dano *in re ipsa*, uma vez que não houve a comprovação de ofensa aos direitos da personalidade. Referente ao mesmo caso, entendeu a Nona Câmara Cível, na apelação 0296615-34.2018.8.21.7000, que:

> APELAÇÃO CÍVEL. SUBCLASSE RESPONSABILIDADE CIVIL. AÇÃO INDENIZATÓRIA. DIVULGAÇÃO DE DADOS NA INTERNET. UNISINOS. DADOS NÃO SENSÍVEIS. INEXISTÊNCIA, NO CASO, DE VIOLAÇÃO DOS DIREITOS E INTERESSES REFERIDOS NA INICIAL – HONRA, IMAGEM E PRIVACIDADE. AUSÊNCIA DE DANOS COMPENSÁVEIS.
> 1.Em que pese o ato ilícito da ré ao divulgar dados pessoais de alunos na internet, tratava-se, no caso, dos chamados 'dados não sensíveis', e facilmente obteníveis por outras fontes, tais como endereço, CPF, RG, número de telefone, curso em que matriculado, etc. A parte autora não comprovou ter sofrido qualquer lesão à sua honra, imagem ou privacidade – que foram os interesses referidos na inicial [...] não há que se falar em danos morais, no caso. (TJ-RS -Apelação Cível: 70079314035 CNJ: 0296615-34.2018.8.21.7000 (Acórdão), Relator: Eugenio Facchini Neto, Data de Julgamento: 18/12/2018, Nona Câmara Cível, Data de Publicação: 18/01/2019).

Em outra decisão, agora da Terceira Turma Recursal Cível, também do Rio Grande do Sul, no processo n. 0047026-37.2019.8.21.9000 (n. local 71008773855), também foi afastada a ocorrência do dano moral pleiteado pela vítima de vazamento de dados cadastrais. Sob a alegação de que se tratava de mero aborrecimento decorrente da vida em sociedade, no entender da Corte, deferir o dano moral na ausência de comprovação de violação de direitos da personalidade incorreria em mera punição ao réu, modalidade não admitida no Direito brasileiro.

Faz-se necessário ressaltar que as Cortes já enfrentaram o tema fora da esfera consumerista. O Supremo Tribunal Federal, em sede de Recurso Extraordinário n. 675.943, de relatoria do Ministro Dias Toffoli, entendeu que dados pessoais cadastrais (nome completo, CPF e RG) não são sigilosos e que, por isso, a utilização de listagem com essas informações pelo empregador, na seara da justiça trabalhista como forma de defesa, não enseja utilização indevida ou não autorizada, inocorrendo, portanto, dano moral de qualquer espécie.

O Tribunal Regional Federal da 4ª região, diante de uma situação de utilização dos dados pessoais de um indivíduo para a abertura de conta bancária fraudulenta, entendeu ao julgar os Embargos Infringentes n. 5002819-02.2012.404.7000/PR, em que se pleiteava dano moral, que a ansiedade e apreensão sofrida pelo autor não são elementos suficientes para a configuração do dano moral.

4.2 TRIBUNAIS NO DIREITO COMPARADO: ESTADOS UNIDOS E EUROPA

Devido ao momento incipiente de construção da jurisprudência nacional, ainda sobre os danos decorrentes do acesso indevido aos dados pessoais, sejam eles causados por mau uso ou por atividades de cibercriminosos, é importante olhar para o Direito Comparado, em que as Cortes judiciais já têm posicionamentos de certa forma mais consolidados. Estados Unidos e Europa, além de adotarem sistemas jurídicos distintos, o primeiro adepto da *common law* e do sistema de precedentes, enquanto a segunda fortemente calcada no *civil law*, com decisões judiciais baseadas na força da lei, também têm culturas muito distantes relacionadas à proteção da privacidade o que se reflete na construção legislativa de cada um e consequentemente na atividade judicial.

Fortemente baseado no sistema de precedentes, o Judiciário americano não pacificou ainda entendimento a respeito da ocorrência de dano moral presumido nos casos de violação de dados pessoais. Em um levantamento acerca dos litígios promovidos entre os anos de 2004 e 2014, em que se pleiteava o reconhecimento de dano moral em situações de violação de dados pessoais, Solove e Citron (2017) identificaram que os pedidos geralmente foram construídos a partir do risco de prejuízo futuro sob a alegação de que o acesso indevido aos dados aumentava a probabilidade de ocorrência de fraudes e de roubo de identidade. Nesses casos, os tribunais em regra afastam a existência do dano, com o fundamento de que ele não é concreto e atual e que o pedido se subsumia em especulação.

Outra tese utilizada pelos demandantes norte-americanos utilizava a necessidade de adotar medidas preventivas para evitar prejuízos futuros. A tese, construída sob a alegação de que as

vítimas gastavam tempo e dinheiro para garantirem que a utilização das informações pessoais acessadas indevidamente não lhes causaria prejuízo, também não encontra respaldo nas decisões judiciais.

O terceiro argumento pleiteado diante das Cortes americanas trata dos danos causados ao indivíduo pela ansiedade. Sob a alegação de que o indivíduo que tivesse seus dados violados passaria por situações de sofrimento emocional, pedia-se o reconhecimento do dano moral. Contudo, para o Judiciário americano, tal alegação é insuficiente para concretizar o dano.

O autor destaca que, de forma geral, o reconhecimento do dano nos EUA somente ocorre quando existe prova ou risco eminente de prejuízo físico ou de perdas financeiras. Desse modo, por não serem de cognição fácil, os danos que podem vir a ser causados pelo acesso indevido aos dados pessoais raramente tem seus pedidos de reparação reconhecidos.

Vale ressaltar que, nos Estados Unidos, grande parte dos casos em que há muitas vítimas é resolvida via acordos entre os réus e a *Federal Trade Commission*, entidade responsável por proteger os direitos dos consumidores, como ocorreu no vazamento de dados pessoais de que foram vítimas os clientes da Equifax, um dos maiores *bureaus* de crédito norte-americano. Nesse caso em específico, dados financeiros dos titulares foram indevidamente expostos. Para não ser demandada individualmente por todas as vítimas, a empresa fez um acordo com a FTC, de forma que os titulares dos dados dividiram o valor do acordo conforme os danos sofridos. Embora não exista óbice ao litígio individual pleiteando a reparação de danos extrapatrimoniais, Schwartz (2018) reafirma a já relatada ausência de condenação dos réus. As Cortes norte-americanas têm resistido ao dano imaterial.

A posição assumida pelos julgadores dos EUA tem refletido o entendimento da Suprema Corte, é essa a conclusão de Yenouskas e Swank (2018) em um artigo publicado pela Associação Americana de Advogados. Os autores destacam que, no julgamento *Clapper v Amnesty International USA*, em 2013, a Corte Suprema estabeleceu que o temor de vigilância causado por possível monitoramento de comunicações privadas por programas do governo e que alegações da existência de possibilidade de problemas futuros oriundos do acesso indevido a dados pessoais são especulativos, não podendo ser considerados como ofensas a justificarem a existência de algum dano.

Na Europa, a pesquisa se resume a algumas decisões tomadas em países membros da União Europeia, que estão sob a égide do Regulamento Geral de Proteção de Dados, apenas como ilustração do que vem ocorrendo onde a proteção de dados é entendida como um direito fundamental. Faz-se necessário salientar que o entendimento dos tribunais europeus vem passando

por mudanças após a entrada em vigor do regulamento em maio de 2018. Se antes as ações judiciais pleiteando reparação de danos estavam restritas à esfera consumerista, atualmente o artigo 82 do Regulamento Europeu, autoriza expressamente a condenação à reparação em danos extrapatrimoniais quando houver qualquer violação da proteção de dados de algum titular. Assim, os tribunais têm atuado no sentido de condenar quem, por ação ou omissão, der causa ao uso não autorizado das informações pessoais.

De acordo com Orlic (2019) na Holanda um ex-empregador foi condenado por danos extrapatrimoniais por revelar os registros médicos de uma funcionária para o novo empregador por meio de uma carta gerada automaticamente. As leis do país europeu não exigem que o empregado revele ao empregador sua situação de saúde. Embora a comunicação enviada não revelasse qual o mal que a afetava, ela permitia entender que a empregada em questão fazia jus ao benefício concedido aos trabalhadores que precisam se afastar do trabalho por determinação médica. Ocorre que a funcionária já havia melhorado do problema de saúde, mas o ex-empregador não havia atualizado seus registros. Entendeu a Corte de Amsterdam que o fato dos registros médicos terem sido enviados ao novo empregador sem autorização do titular dos dados caracterizou uma violação dos dados pessoais e que o fato causou ansiedade e sofrimento à vítima, que por isso fez jus a uma indenização por danos morais, em que pese o ocorrido não tenha prejudicado em nada sua posição no novo emprego.

Ainda sob a égide da legislação europeia anterior sobre a proteção de dados pessoais e amparada no *Data Protection Act*, *Halliday vs. Creation Consumer Finance Limited*, foi o primeiro litígio britânico em que o réu foi condenado a reparar o dano moral sofrido pelo autor, por ter revelado dados financeiros incorretos dele a uma agência de crédito (INGLATERRA, 2013). Embora também anterior ao Regulamento, o caso – *Google Inc. vs. Vidal Hall* – tratou do armazenamento e da análise de informações de navegação dos usuários pelo Google, sem o conhecimento e a autorização dos titulares dos dados, que transcorreu no Reino Unido em 2016, merece destaque. Nesse caso, em decisão inédita, o Judiciário britânico considerou que o simples sentimento de angústia é causa suficiente para caracterizar o dano (UNITED KINGDOM, 2015).

Em outra decisão em que se reconheceu o dano *in re ipsa* aplicando entendimento igual ao caso anterior foi pelo vazamento acidental de dados pessoais de pessoas requerentes de asilo (CELERINI e LANG, 2017). O litígio, *TLT v* Secretary *of State for The Home Department*, teve início porque uma planilha contendo dados de mais de mil e quinhentas pessoas que pleiteavam entrar ou permanecer no Reino Unido foi divulgada de forma equivocada. Ao final, a ré foi condenada a reparar danos morais refletidos pelos sentimentos de angústia suportados pelas vítimas.

5 CONSIDERAÇÕES FINAIS

Ao longo do trabalho, construiu-se um estudo acerca da existência ou não de dano presumido em situações envolvendo violação de dados pessoais, que ocorrem quando eles são acessados indevidamente ou de forma não autorizada ou ainda por vazamentos que podem ser ou não causados por atividades criminosas.

Buscou-se esclarecer qual a importância de se promover a proteção dos dados relacionados às pessoas, demonstrando que em muitos países esse já é considerado um direito fundamental, presente de forma expressa nos textos constitucionais. No Brasil, essa discussão está no Congresso Nacional, no texto do Projeto de Emenda Constitucional 17, que já recebeu parecer favorável de algumas comissões gerando a expectativa de que em breve tal direito figure no rol do artigo 5º da Constituição Federal. A discussão acerca da existência do dano presumido ocorre porque a Lei n. 13.709/18, não traz expressamente sequer a modalidade de responsabilidade civil a ser aplicada aos agentes de tratamento em caso de incidentes de segurança que atinjam a proteção de dados. Dessa forma, restará ao Judiciário enfrentar o tema e pacificá-lo como meio de garantir a segurança jurídica tão necessária ao desenvolvimento econômico.

Dentre as hipóteses que surgem como possibilidade de resposta ao problema exposto, duas foram discutidas ao longo do texto. A primeira explora a perspectiva de que o acesso não autorizado aos dados pessoais gera o dano presumido; ela encontra-se amparada pela tese de que a mera expectativa de que qualquer informação pessoal seja utilizada para fins desconhecidos e/ou não esperados pelo titular dos dados é causa de dano. Tal entendimento decorre da impossibilidade de se dimensionar ou precisar as consequências do vazamento de dados. A expectativa de que a informação pessoal seja utilizada como meio de injusta ofensa ao princípio constitucional da dignidade humana, levando em conta que, em virtude de vazamentos de dados, pessoas poderiam sofrer tratamentos discriminatórios, ser vítimas de furto de identidade ou de ataques com objetivos fraudulentos serve de fundamento a esse posicionamento. Some-se a isso a exigência da LGPD de que todo tratamento de dados deve ser realizado a partir de uma finalidade específica que precisa ser informada *a priori* ao sujeito de dados, gerando assim uma relação de confiança calcada na boa-fé entre o agente de tratamento e o titular dos dados, de modo que um acesso não autorizado quebra esse vínculo.

Em contraposição, a segunda hipótese abordada é de que o dano moral não é presumido, precisando, portanto, ser provado pelo titular dos dados atingido. Sustenta essa tese a compreensão

de que em uma economia de dados não se pode compreender a atividade de tratamento de dados como de risco. Além disso, há a reconhecida impossibilidade técnica de garantir ambientes totalmente seguros. Sistemas são todos em maior ou menor grau vulneráveis e sua implementação pode chegar a valores exorbitantes, onerando excessivamente o agente de tratamento de dados o que em último grau inviabilizaria a atividade econômica. Sob essa hipótese, por não existir certeza de que a consequência do acesso indevido ou do vazamento seja danosa ao titular dos dados, estar-se-ia diante de um dano hipotético. Sob esse prisma, exige-se que se prove que o dano ocorreu de fato, não se tratando de simples conjectura.

Conforme demonstrado ao longo do texto, quando confrontado, o Judiciário tem se posicionado de forma divergente. Parte entende que há dano presumido, defendendo que a expectativa de que determinadas informações possam ser utilizadas em prejuízo do titular de dados é motivo suficiente para causar transtornos que ensejam a reparação extrapatrimonial. Há também os que entendem que não existe qualquer certeza da ocorrência do dano, ficando este no plano hipotético, o que impede o reconhecimento do dano *in re ipsa.*

A discordância transcende os tribunais brasileiros, o Judiciário norte-americano, com poucas divergências, tem decidido no sentido de afastar o dano presumido nesses casos, exigindo a prova da efetiva ocorrência do dano para determinar a reparação. Em países pertencentes à União Europeia que estão sob a égide do Regulamento Europeu, em decisões mais recentes, tem se reconhecido a presunção do dano extrapatrimonial em favor do titular de dados.

Há que se ressaltar, contudo, que no Brasil, já há alguma pacificação do Superior Tribunal de Justiça no sentindo da ocorrência do dano *in re ipsa*, quando o acesso indevido aos dados ocorre na esfera consumerista. Entretanto, a LGPD não se circunscreve apenas aos dados pessoais dos consumidores, ela abrange todo e qualquer tratamento de dados realizado em território brasileiro ou de titulares de dados que estejam em território nacional. Dessa forma, informações pessoais de colaboradores, de sócios, de parceiros de negócio, por exemplo, também estão contempladas.

A questão merece ser objeto de maiores debates, uma vez que toda pessoa natural é sujeito de dados pessoais, e todas as organizações utilizam informações pessoais em algum momento no exercício de suas atividades. Agregado a isso há o fato da impossibilidade de ambientes com segurança infalível. Cria-se, então, a perspectiva de um aumento na judicialização de casos envolvendo vazamentos de informações pessoais, uma vez que os conflitos entre organizações e titulares de dados são inevitáveis. Diante dos cenários apresentados, parece ser razoável fazer a discussão sobre a ocorrência do dano extrapatrimonial presumido ante o caso concreto. Não aparenta ser proporcional atribuir o mesmo valor ao dado cadastral, utilizado em larga escala, e ao

dado sensível, que é aquele cuja simples exposição pode implicar grave prejuízo ao titular. Também carece de razoabilidade atribuir o mesmo ônus de reparação do dano para organizações que invistam pesadamente em segurança da informação e outras que negligenciam tal fator, deixando assim as informações que estão sob sua posse expostas.

Assim, o presente trabalho atingiu o seu principal objetivo de realizar uma discussão sobre o tema. Contudo, ao seu final, restam mais perguntas do que respostas e a certeza de que o assunto é digno de ser aprofundado em outros trabalhos. A legislação sobre proteção de dados pessoais no Brasil é recente, contudo, os debates ultrapassam a barreira de uma década. Ao longo dos próximos anos, novas teses surgirão, sejam elas em defesa dos titulares do direito à proteção de dados, sejam em defesa das organizações, que dependem cada vez mais desse ativo para manterem-se competitivas no mercado. A LGPD tem como objetivo equilibrar essa balança entre sujeitos de dados e organizações, entretanto, possui lacunas que, ao que tudo indica, serão fechadas pelo Judiciário, que dependerá de coerência nas fundamentações e profundidade nas argumentações.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT ISO/IEC 27001**: técnicas de segurança – sistemas de gestão de segurança da informação. Rio de Janeiro: ABNT, 2013.

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

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em: 03 set. 2019.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 05 set. 2019.

_____. **Proposta de Emenda Constitucional nº 17.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoa. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>. Acesso em: 05 set. 2019.

_____. Superior Tribunal de Justiça. **Informativo nº 0513**. Direito Civil. Dano moral. Ofensa à dignidade da pessoa humana. Dano *in re ipsa*. Disponível em: < https://ww2.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisar&processo=1292141&operador=mesmo&tipo_visualizacao=RESUMO&b=INFJ&thesaurus=JURIDICO&p=true>. Acesso em: 11 abr. 2020.

_____. Superior Tribunal de Justiça. **Recurso Especial nº 1.292.141** Ação de compensação por danos morais. Acidente em obras do rodoanel Mário Covas. Necessidade de desocupação temporária de residência. Dano moral *in re ipsa*. Relatora: Min. Nancy Andrigui, 21 de maio de 2013. Disponível em: <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201101127241&dt_publicacao=04/06/2013>. Acesso em: 13 set. 2019.

_____. Superior Tribunal de Justiça. **Recurso Especial nº 1.245.550**. Saque indevido em conta-corrente. Falha na prestação do serviço. Responsabilidade da instituição financeira. Sujeito absolutamente incapaz. Ataque direto da personalidade. Configuração do dano moral. Irrelevância quanto ao estado da pessoa. Direito à dignidade. Previsão constitucional. Proteção devida. Relatora: Min. Luis Felipe Salomão, 17 de março de 2015. Disponível em: <https://scon.stj.jus.br/SCON/jurisprudencia/doc.jsp> Acesso em: 11 abr. 2020.

_____. Superior Tribunal de Justiça. **Recurso Especial nº 1.243.699.** Direito de imagem. Publicação de fotografia. Mulher de biquíni na praia. Exata individualização da pessoa. Autorização prévia ou posterior. Inexistência. Revista de conotação erótica. Proveito econômico. Uso indevido da imagem. Dano moral configurado (Súmula 403/STJ). Relator: Min. Raul Araújo, 21 de junho de 2016. Disponível em: <https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?processo=1243699&tipo_visualizacao=RESUMO&b=ACOR&thesaurus=JURIDICO&p=true>. Acesso em: 11 abr. 2020.

_____. Superior Tribunal de Justiça. **Agravo Interno no Recurso Especial nº 1.655.212**. Ação de indenização. Envio de cartão de crédito sem solicitação do consumidor. Ausência de negativação ou cobrança indevida. Danos morais não configurados. Mero aborrecimento. Agravo desprovido. Relator: Min. Raul Araújo, 19 de fevereiro de 2019. Disponível em: <https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=90570121&num_registro=201700358911&data=20190301&tipo=5&formato=PDF>. Acesso em: 13 maio 2020.

_____. Superior Tribunal de Justiça. **Recurso Especial nº 1.758.799.** Ação de compensação de dano moral. Banco de dados. Compartilhamento de informações pessoais. Dever de informação. Violação. Dano moral *in re ipsa*. Relator: Min. Nancy Andrighi. 12 de novembro de 2019. Disponível em: <https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1888267&num_registro=201700065219&data=20191119&formato=PDF>. Acesso em: 13 maio 2020.

_____. Supremo Tribunal Federal. **Recurso Extraordinário nº 675.943.** Recurso cível indenização por dano moral. Utilização de dados pessoais de empregados como prova em defesa em ação trabalhista. Ao direito à intimidade não violado. Dano moral não caracterizado. Relator: Min. Dias Toffoli, 04 de fevereiro de 2013. Disponível em: <http://stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%28%28675943%2ENUME%2E+OU+675943%2EDMS%2E%29%29+NAO+S%2EPRES%2E&base=baseMonocraticas&url=http://tinyurl.com/y86rlkgu>. Acesso em: 13 maio 2020.

BUSSCHE, Axel; VOIGT, Paul. **The EU General Data Protection Regulation (GDPR):** a practical guide. Suíça: Springer, 2017.

CELERINE, Elena J.; LANG, Christian. **Cyber liability: data breach in Europe**. Zurich: Swiss Reinsurance Company Ltd, 2017. Disponível em: <https://www.swissre.com/dam/jcr:b6772437-

1bb4-4555-9ff9-1c55e67b6367/Cyber_Liability_Data_Breach_Europe.pdf> Acesso em: 17 maio 2020.

CANOTILHO, J.J.Gomes. **Direito constitucional e teoria da Constituição**. 7.ed. Coimbra: Edições Almedina, 1941.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11.ed. São Paulo: Atlas, 2014.

CONSELHO DA JUSTIÇA FEDERAL. V Jornada de Direito Civil: **Enunciado 445.** Obrigação de indenizar. Indenização. Ato ilícito. Dano. Reparação. Obrigação. Culpa. Natureza. Risco. Disponível em: < https://www.cjf.jus.br/enunciados/enunciado/366>. Acesso em: 11 abr. 2020.

DISTRITO FEDERAL. Tribunal de Justiça do Distrito Federal. **Acórdão Apelação Cível do Juizado Especial nº 20140110578872**. Consumidor. Vazamento de informações pessoais do banco de dados da ré. Fato não comprovado. Ônus probatório. Art. 333, I, CPC. Recurso conhecido e improvido. Sentença mantida. Relator: Marco Antonio do Amaral. 16 dezembro 2014. Disponível em <https://tj-df.jusbrasil.com.br/jurisprudencia/311516047/apelacao-civel-do-juizado-especial-acj-20140110578872?ref=serp> Acesso em: 16 maio 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2020.

Estados Unidos da América. Federal Trade Comission. **Equifaz to pay $575 Million as part of settlement with FTC, CFPB, and States Related to 2017 Data Breach.** Disponível em: <https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related> Acesso em: 03 maio 2020.

GAGLIANO, Pablo.S.; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil, volume 3:** responsabilidade civil. 15.ed. São Paulo: Saraiva, 2017.

GARATINI, MARIA C.; PORTO, Ana L. F.. A evolução da responsabilidade civil no direito constitucional contemporâneo: do dano moral *in nature* ao dano moral *in re ipsa*. **Cadernos de dereito actual.** São Paulo, n.8, 2017. Disponível em: < http://www.cadernosdedereitoactual.es/ojs/index.php/cadernos/article/view/230 >. Acesso em: 12 maio 2020.

INGLATERRA. England and Wales Court of Appeal (Civil Division) Decisions. **Appeal Halliday and Creation Consumer Finance Limited.** On the assessment of damages Mr. Halliday claimed damages for damage to his reputation and damages for distress. 15 march 2013. Disponível em: <http://www.bailii.org/ew/cases/EWCA/Civ/2013/333.html> Acesso em: 20 maio 2020.

LAMBERT, Paul B. **Understanding the New European Data Protection Rules**. New York: CRC Press, 2018.

LAMONT, Tom. Life after the Ashley Madison affair. **The Guardian**, London, 28 fev. 2016. Disponível em: <https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked>. Acesso em: 20 ago. 2019.

MARMELSTEIN, George. **Curso de direitos fundamentais**. 8. ed. São Paulo: Atlas, 2019. p.15-26.

MARTINS, Leonardo. **Cinquenta anos de jurisprudência do tribunal constitucional federal alemão.** Montevideo: Mastergraf, 2005. p. 233-234.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**: controlando o fator humano na segurança da informação. São Paulo: Pearson Makron Books, 2006.

NAKAGAWA, Liliane. Detran vaza dados pessoais de quase 70 milhões de brasileiros. **Olhar Digital**, São Paulo, 08 out. 2019. Disponível em: < https://olhardigital.com.br/noticia/-exclusivo-detran-vaza-dados-pessoais-de-quase-70-milhoes-de-brasileiros/91308>. Acesso em: 11 abr. 2020.

OLIVA, Milena D. Dano moral e inadimplemento contratual nas relações de consumo. **Revista de Direito do Consumidor.** São Paulo, v. 93, mai-jun 2014. p. 13-28.

ORLIC, Nina. District court grants EUR 250 for immaterial damages suffered due to breach with GDPR. **Loyens&Loeff**, Amsteram, 10 set. 2019. Disponível em: <https://www.loyensloeff.com/nl/en/news/news-articles/district-court-grants-eur-250-for-immaterial-damages-suffered-due-to-breach-with-gdpr-n16691/>. Acesso em: 17 maio 2020.

PARANÁ. Primeira Turma Recursal. **Recurso Inominado nº 0023501-13.2014.8.16.0182**. Ação de reparação de danos morais. Envio de e-mail falso que contempla a autora em dois ingressos para a copa do mundo de 2014. Vazamento de informações pessoais. Dano moral configurado. Falha no sistema de segurança do site da ré. Sentença Mantida. Relatora: Juíza Liana de Oliveira Lueders. 2 de junho de 2015. Disponível em: <http://portal.tjpr.jus.br/jurisprudencia/j/2100000001856341/Ac%C3%B3rd%C3%A3o-0023501-13.2014.8.16.0182>. Acesso em: 15 maio 2020.

PEREIRA, Caio Márcio da Silva. **Responsabilidade civil.** 12. ed. Rio de Janeiro: Forense, 2018. p. 60-87.

PERSILY, Nathaniel. Can democracy survive the internet? **Journal of democracy**, Washington, v. 28, n. 2, abr. 2017. The 2016 U.S. Election. p. 63-76. Disponível em: <https://www.journalofdemocracy.org/articles/the-2016-u-s-election-can-democracy-survive-the-internet/>. Acesso em: 01 set. 2019.

PORTUGAL. **Constituição da República Portuguesa de 1976.** Lisboa: Procuradoria-Geral Distrital de Lisboa [2019]. Disponível em: <http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=4&tabela=leis&so_miolo=>. Acesso em: 10 ago. 2019.

RIO DE JANEIRO. Tribunal de Justiça do Estado do Rio de Janeiro. **Apelação Cível nº 0071614-40.2012.8.19.0002.** Site de comércio eletrônico. Anunciante de produto à venda que alega prejuízos por falha na segurança do serviço administrado pela ré ("Mercado Livre"). Sentença de parcial procedência, deferindo apenas dano moral. Apelação de ambas as partes. Sentença que se mantém. Demanda envolvendo atividade intermediária. Apelações inicialmente distribuídas para a 26ª Câmara Cível do Consumidor, que fez retornar o feito à 1ª. Vice-presidência, por entender não se tratar de relação de consumo. Incidência da súmula 307 TJRJ. Relação não disciplinada pelo Código de Defesa do Consumidor. Relator: Des. Juarez Fernandes Flores. 29 de junho de 2016. Disponível em: <http://www1.tjrj.jus.br/gedcacheweb/default.aspx?UZIP=1&GEDID=00048356A8FEC447DB02BC21BF05115FBB58C5051C340310>. Acesso em: 15 maio 2020.

RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Organização, seleção e apresentação Maria Celina Bodin de Moraes. Tradução: Danilo Doneda, Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Apelação nº 9000703-75.2011.8.26.0037**, Telefonia celular. Violação de dados sigilosos. Falha nos serviços prestados. Indenização devida. Sentença confirmada. RITJSP, art. 252. Recurso improvido. Relator: Maury Bottesini. 05 de setembro de 2012. Disponível em: < Apelação 9.000.703-75.2011.8.26.0037 https://esaj.tjsp.jus.br/cjsg/resultadoSimples.do;jsessionid=26F0EEE6F4C1A74DF7F1F171145879A3.cjsg3?conversationId=&nuProcOrigem=9.000.703-75.2011.8.26.0037&nuRegistro=>. Acesso em: 13 maio 2020.

SCHAEFFER, Cesar. Falha de segurança expõe dados de 24 milhões de usuários da Vivo. **Olhar Digital**, São Paulo, 04 nov. 2019. Disponível em: < https://olhardigital.com.br/fique_seguro/noticia/-exclusivo-falha-de-seguranca-expoe-dados-de-24-milhoes-de-usuarios-da-vivo/92520>. Acesso em: 11 abr. 2020.

SCHREIBER, Anderson. PEC 17/19: Uma análise crítica. **Carta Forense.** Disponível em: <http://cartaforense.com.br/conteudo/colunas/pec-1719-uma-analise-critica/18345>. Acesso em: 04 set. 2019.

SCHWARTZ, Paul. M.; SOLOVE, Daniel J. **Information Privacy Law**. 5. ed. New York: Wolters Kluwer, 2015. p.43-72.

SCHWARTZ, Mathew J. British Airways Faces Class-Action Lawsuit Over Data Breach. **Information Security Media Group**. Princenton, 10 set. 2018. Disponível em: <https://www.bankinfosecurity.com/british-airways-faces-class-action-lawsuit-over-data-breach-a-11478>. Acesso em: 17 maio 2020.

RIO GRANDE DO SUL. Tribunal Regional Federal da 4ª Região. **Embargos Infringentes nº 5002819-02.2012.404.7000.** Indenização por danos morais. Empréstimo consignado. Desconto não autorizado. Dano moral não configurado. Relator: Salise Monteiro Sanchotene, 12 de fevereiro 2015. Disponível em: <https://www2.trf4.jus.br/trf4/controlador.php?acao=consulta_processual_resultado_pesquisa&txtPalavraGerada=qyup&hdnRefId=bd67868a55b4b02ef26fb6a543b005dc&selForma=NU&txtValor=5002819-02.2012.404.7000&chkMostrarBaixados=&todasfases=&todosvalores=&todaspartes=&txtDataFase=&selOrigem=TRF&sistema=&codigoparte=&txtChave=&paginaSubmeteuPesquisa=letras>. Acesso em: 15 maio 2020.

_____. Terceira Turma Recursal Cível dos Juizados Especiais Cíveis do Estado do Rio Grande do Sul. **Recurso Inominado nº 71008773855.** Ação de indenização por danos materiais e morais. Fraude perpetrada. Vazamento de informações cadastrais e negociais do autor. Danos morais não configurados. Ausência de previsão legal para impor danos morais com caráter meramente punitivo. Sentença mantida pelos próprios fundamentos. Recurso improvido. Relator: Fabio Vieira Heerdt, 26 de setembro de 2019. Disponível em: <https://www.tjrs.jus.br/buscas/jurisprudencia/exibe_html.php>. Acesso em: 20 de maio 2020.

_____. Primeira Turma Recursal Cível dos Juizados Especiais do Estado do Rio Grande do Sul. **Recurso Inominado nº 71004537700**. Reparação de danos materiais. Pedido de indenização por

danos morais. Divulgação indevida dos dados cadastras de alunos da universidade. Ausência de comprovação de qualquer violação aos direitos de personalidade da autora. Sentença de improcedência mantida por seus próprios fundamentos. Relator: Roberto José Ludwig. 28 de outubro de 2013. Disponível em: <https://www.tjrs.jus.br/buscas/proc.html?tb=proc>. Acesso em: 20 maio 2020.

_____. Tribunal de Justiça do Rio Grande do Sul Nona Câmara Cível. **Apelação Cível nº 700793140035.** Responsabilidade civil. Ação indenizatória. Divulgação de dados na Internet. Unisinos. Dados não sensíveis. Inexistência, no caso, de violação dos direitos e interesses referidos na inicial: honra, imagem e privacidade. Ausência de danos compensáveis. Eugênio Fachini Neto, 18 de dezembro de 2018. Disponível em: <https://www.tjrs.jus.br/buscas/jurisprudencia/exibe_html.php>Acesso em: 20 de maio 2020.

SCUDERE, Leonardo. **Risco digital na web 3.0**. Rio de Janeiro: Elsevier, 2015.

SOLOVE, Daniel. J.; CITRON, Danielle. K. Risk and anxiety: a theory of data breach harms. **SSRN Electronic Journal**. Washington, n. 2017-2. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885638>. Acesso em: 25 ago. 2019.

SOMBRA, Thiago. L. Brazil Cybersecurity. In: **GDR Insight**: handbook 2020. London: Global Data Review Law Business Research Ltd, 2019. Part 2, p. 121.

TANNER, Adam. **Our bodies, our data:** how companies make billions selling our medical records. Boston: Beacon Press, 2017.

TARTUCE, Flávio. **Manual de responsabilidade civil.** São Paulo: Método, 2018.

TASSO, Fernando. A. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. In: **Cadernos Jurídicos:** Direito Digital e proteção de dados pessoais. Ano 21, nº 53. São Paulo: 2020. Cap. II, p. 97.

UNIÃO EUROPEIA. **Carta dos direitos fundamentais da União Europeia.** Bruxelas: Parlamento Europeu [2000]. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/CARTAFUNDAMENTAL.pdf>. Acesso em: 05 set. 2019.

_____. **Regulamento Geral de Proteção de Dados.** Bruxelas: Parlamento Europeu [2016]. Disponível em: <https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-general-data-protection-regulation>. Acesso em: 12 fev. 2020.

UNITED KINGDOM. High Court of Justice. **Appeal Google Inc. and Judith Vidal-Hall, Robert Hann, Marc Bradshaw and The Information Commissioner.** Cause of action for misuse of private information is a tort; damage in section 13 of the Data Protection Act 1998 (the DPA); whether there can be a claim for compensation without pecuniary loss. 27 march 2015. Disponível em: <https://www.judiciary.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf>. Acesso em: 10 maio 2020.

EUA vão exigir histórico das redes sociais para liberação de visto. **Veja**. São Paulo, 02 abr. 2018. Caderno Economia. Disponível em: <https://veja.abril.com.br/economia/eua-vao-exigir-historico-das-redes-sociais-para-liberacao-de-visto/>. Acesso em: 29 ago. 2019.

YENOUSKAS, Joseph F.; SWANK, Levi W. Emerging Legal Issues in Data Breach Class Actions. **American Bar Asssociation**. Washington, D.C: 17 jul. 2018. Disponível em: < https://www.americanbar.org/groups/business_law/publications/blt/2018/07/data-breach/>. Acesso em: 17 maio 2020.