A RESPONSABILIDADE CIVIL DO PODER JUDICIÁRIO FRENTE AOS VAZAMENTO DE DADOS DOS TRIBUNAIS SOB A ÓPTICA DA LEI GERAL DE PROTEÇÃO DE DADOS

THE CIVIL LIABILITY OF THE JUDICIARY WITH REGARD TO COURT DATA LEAKS UNDER THE GENERAL DATA PROTECTION LAW

Artigo recebido em 30/03/2023
Artigo aceito em 27/04/2023
Artigo publicado em 23/10/2023

Luan Berci
Graduando em Direito na Faculdade de Direito de Franca – FDF. E-mail: luanberci@hotmail.com.

Yuri Nathan da Costa Lannes
Fez estágio de Pós-Doutorado na Universidade de Brasília (UNB), Doutor em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie, Mestre em Justiça, Empresa e Sustentabilidade pela Universidade Nove de Julho, Professor e Coordenador de Pesquisa da Faculdade de Direito de Franca – FDF, Diretor CONPEDI. E-mail: yurinathanlannes@gmail.com.

Stefania Stefanelli
Professora associada do núcleo de Direito Privado, do departamento de Direito da Universidade de Perugia, Pró-reitora de internacionalização da Universidade de Perugia. E-mail: stefania.stefanelli@unipg.it.

RESUMO: Partindo dos episódios de vazamento de dados dos tribunais identifica-se a problemática da adequação do Poder Judiciário à Lei Geral de Proteção de Dados, observa-se os principais pontos da legislação e inspeciona-se no âmbito da responsabilidade civil qual modalidade deve ser adotada e se os danos morais devem ser provados ou presumidos. Para tanto, adota-se da perspectiva metodológica o método dedutivo na construção de uma pesquisa exploratória utilizando de procedimentos técnicos bibliográficos e documental.
PALAVRAS-CHAVE: vazamento de dados; proteção de dados; responsabilidade civil.

ABSTRACT: Starting from the episodes of data leakage from the courts, the problem of the adequacy of the Judiciary to the General Law of Data Protection is identified, the main points of the legislation are observed and it is inspected in the scope of civil liability which modality should be adopted and if the moral damages should be proved or presumed. For this, the deductive method is adopted from the methodological perspective in the construction of an exploratory research using bibliographic and documental technical procedures.
KEYWORDS: data leakage; data protection; liability.

1 INTRODUÇÃO

O Poder Judiciário é parte integrante da administração pública e sua estrutura está sendo informatizada, com isso, intensifica-se problemas em relação à segurança, tratamento e exposição de dados. Nesse espectro, a governança de adequação à Lei Geral de Proteção de Dados - LGPD faz-se necessária. Logo, é preciso identificar quais são as situações práticas, qual o papel desenvolvido pelos tribunais no tratamento de dados, o que caracteriza a atividade de tratamento de dados, como estes dados devem ser coletados, se existe diferenciação entre os dados e como os tribunais têm se organizado.

A partir disso, a pesquisa busca compreender especificamente o que a LGPD estabelece para as pessoas jurídicas de direito público. Questiona-se: a Lei Geral de Proteção de Dados caracteriza a responsabilidade civil a ser atribuída ao Poder Judiciário e aduz à indenização por danos morais do titular dos dados nos casos de vazamento de dados?

O objetivo geral da pesquisa é identificar na legislação e nos institutos da responsabilidade civil a possibilidade de responsabilização do Poder Judiciário pelos incidentes envolvendo a proteção aos dados pessoais, ao passo que objetiva-se especificamente analisar e compreender a dinâmica dos ativos judiciais, os mandamentos da Lei Geral de Proteção de Dados e o instituto da Responsabilidade por danos em decorrência da reação com os dados pessoais.

A pesquisa se justifica pela dimensão e pela quantidade de dados que o poder judiciário veicula nos processos, de caráter público e que podem acarretar danos aos particulares que se veem envoltos na dinâmica de funcionamento das estruturas do Poder Judiciário.

Para responder às perguntas utiliza-se do método dedutivo, de inspeções bibliográficas, mas majoritariamente documentais, ou seja, em materiais que não receberam o devido tratamento analítico por se tratar de uma temática recente.

Sendo assim, a abordagem da problemática será qualitativa, aproximando-se da hermenêutica jurídica para buscar a interpretação das normas. Outrossim, adota-se referencial teórico mais funcionalista por admitir que o Poder Judiciário exerce um papel específico enquanto instituição e o seu funcionamento desencadeia ações e reações nos indivíduos de acordo com as suas ações e reações institucionais.

2 ATIVOS JUDICIAIS

A estrutura do Poder Judiciário na dinâmica contemporânea utiliza-se de sites, sistemas e uma rede de ferramentas tecnológicas, grande parte pela rede mundial de computadores com a utilização da internet. Partindo do pressuposto de um judiciário informatizado, ataques *hackers* aos sistemas dos tribunais evidenciam a fragilidade na atuação do Poder Judiciário em proteger os dados em seus sistemas operacionais e garantir a segurança de seus usuários.

Nesse espectro, em 1º de abril de 2019, o Conselho Nacional de Justiça - CNJ foi alvo de ataque *hacker* que resultou na exposição de dados de pessoas que já utilizaram a plataforma do CNJ, como nomes, informações de contato, contas bancárias, credenciais de juízes, funcionários e senhas diversas. No entanto, o Processo Judicial Eletrônico (PJe), o Banco de Monitoramento de Prisões (BNMP) e o Sistema Eletrônico de Execução Unificado (SEEU) não foram acessados. Os responsáveis deixaram uma mensagem em indonésio, o que indica a possibilidade de uma ação de ciberativismo como se observa:

> Uma criança nascida hoje crescerá sem uma concepção de privacidade. Eles nunca saberão o que significa ter um certo momento para si pensamentos que não são registrados e não analisados. E isso é um problema porque a privacidade é importante; a privacidade é o que é possível devemos determinar quem somos e quem queremos ser. [1]

Em 3 de novembro de 2020 um ataque cibernético ao Superior Tribunal de Justiça - STJ ocasionou o bloqueio do sistema e dos e-mails. Consequentemente, interrupção no andamento dos processos e nos prazos processuais. A fim de evitar danos ainda maiores, o sistema foi retirado do ar. Somente depois de 15 dias o tribunal, em nota, informou que a Secretaria de Tecnologia e Informação e Comunicação havia restabelecido por completo o sistema do tribunal. No entanto, não houve nenhum pronunciamento a respeito de pedido de eventual resgate dos dados, nem a modalidade específica do ataque cibernético ou ainda como ocorreu a invasão.

Em primeira análise, sabe-se que o STJ possuía um *backup* que foi fundamental para restabelecer o sistema e os acessos a ele. Porém, em razão de um e-mail oficial do STJ, enviado no dia 18 de novembro, pelos inscritos no curso "A Eficiência dos Precedentes Judiciais no STJ", informando que não foram recuperados os dados relativos à essa atividade e que por este

[1] MARTINES, Fernando; COELHO, Gabriela. **CNJ sofre ataque de hacker e dados de milhares de pessoas são vazados**. Consultor Jurídico, 1 abr. 2019. Disponível em: https://www.conjur.com.br/2019-abr-01/cnj-sofre-ataque-hacker-dados-milhares-pessoas-vazam. Acesso em: 26 nov. 2022.

motivo não seria possível a emissão dos certificados, observa-se que o *backup* do tribunal não corresponde à integralidade dos dados, apesar da declaração do Presidente do STJ, Ministro Humberto Martins, de que "os dados do acervo do STJ estão integralmente preservados no backup"[2].

Sem o intuito de abordar a temática, provoca-se o questionamento se em eventual oferta de pagamento de resgate dos dados o Poder Judiciário poderia realizar o pagamento mediante a inexistência de previsão legal. Afinal, episódios como esse podem provocar a destruição de dados processuais imprescindíveis, o que resultaria em grande perda para a sociedade.

Retornando ao episódio, apesar do restabelecimento do sistema do tribunal, o ataque *hacker* obteve acesso a dados de processos sigilosos e dados sensíveis dos cursos on-line que são oferecidos pela Escola Corporativa do STJ (Ecorp). Nesse contexto, o Presidente do STJ solicitou à Polícia Federal a instauração de inquérito para a devida investigação do ataque. A abertura do inquérito também verifica se há alguma ligação desse ataque com o Ministério da Saúde e a Secretaria da Economia do Distrito Federal.

As tentativas de acesso indevida a dados nos sistemas dos tribunais são barradas com frequência, no entanto algumas vezes o sistema é sobrecarregado impossibilitando a sua utilização. Em 30 de março de 2022, o Tribunal Regional Federal da 3ª Região sofreu ataque *hacker* e o sistema ficou fora do ar.[3] Também foi alvo a Justiça Federal de Pernambuco (TJ-PE), em 6 de abril de 2022, em que o único sistema que ficou disponível, segundo nota do Tribunal Regional Federal da 5ª Região, foi o Processo Judicial Eletrônico (PJe) 2.X, utilizado nas ações das turmas que julgam recursos de decisões dos Juizados Especiais Federais. Além do atendimento ser interrompido por tempo indeterminado, a telefonia da Justiça Federal em Pernambuco foi afetada.[4]

Nesse contexto, de forma simplificada, as principais modalidades de ciberataques são por *Malware,* DoS (Denial of Service) ou DDoS (Distributed Denial of Service), *Phishing* e *Advanced Persistent Threats* (APTs). A denominação de *Malware* refere-se genericamente a software nocivo que se instala no sistema sem ser facilmente detectado e com o propósito de

[2] Correio Brasiliense. **Presidente do STJ diz que foi alertado sobre possibilidade de novo ataque hacker**. Publicado em: 11 nov. 2020. Disponível em: https://www.correiobraziliense.com.br/politica/2020/11/4888154-presidente-do-stj-diz-que-foi-alertado-sobre-possibilidade-de-novo-ataque-hacker.html. Acesso em: 26 nov. 2022.

[3] Consultor Jurídico. **TRF-3 suspende prazos processuais e adia transmissão de precatórios**. Publicado em: 1 abr. 2022. Disponível em: https://www.conjur.com.br/2022-abr-01/trf-suspende-prazos-processuais-adia-transmissao-precatorios. Acesso em: 18 nov. 2022.

[4] Consultor Jurídico. **Ataque hacker deixa sistemas da Justiça Federal em PE fora do ar**. Publicado em: 6 abr. 2022. Disponível em: https://www.conjur.com.br/2022-abr-06/ataque-hacker-deixa-sistemas-justica-federal-pe-fora-ar. Acesso em: 19 nov. 2022.

danificar o programa. Os principais tipos de *malware* são: Cavalo de Troia, caracterizado por uma instalação que parece legítima e pode facilitar a entrada de outros *malwares*; *Ransomware*, que trava o sistema até que o resgate seja pago; *Spyware*, que transmite informações de um sistema para outro como as senhas bancárias; e *Worms*, que infecta múltiplos aparelhos e facilita a entrada de outros *malwares*.

O ataque DoS (Denial of Service) e DDoS (Distributed Denial of Service) azáfama o fluxo na internet dificultando o desenvolvimento habitual dos servidores e da própria rede. Já o Phishing, consiste na apreensão de dados, podendo inclusive se difundir pelos outros usuários ou lista de contatos do sistema. Ademais, o *Advanced Persistent Threats* (APTs) consiste em operação semelhante, no entanto, além de coletar dados, realiza o monitoramento dos sistemas sem ser detectado, geralmente empregado em setores específicos como a defesa de um país. Não só dos ataques hackers aos sistemas centrais dos tribunais podem ocorrer vazamentos de dados, práticas cotidianas adotadas pelos tribunais também podem ser alvo de ataques.

Com o advento da pandemia do vírus SARS-CoV-2 a utilização de plataformas eletrônicas pelo Poder Judiciário teve de ser implementada e estimulada ao máximo para que o andamento processual pudesse ocorrer resguardando assim a saúde dos sujeitos do processo. Passado o caráter emergencial uma revisão dos protocolos adotados precisa ser feita, assim como a devida regulação das práticas adotadas para garantir o direito à segurança, privacidade e intimidade.

A adoção de aplicativos de troca de mensagem instantânea é um exemplo de prática que precisa ser revista, visto que apesar de acelerar a comunicação entre tribunais e advogados, seja para a obtenção de informações ou ainda o agendamento de audiências. Inexiste um compromisso público e formal dessas plataformas com a confidencialidade, segurança e tratamento dos dados, que na maioria das vezes são de terceiros, ou seja, as partes envolvidas em determinado processo, que ali são compartilhados.

O vazamento de dados consiste no acesso indevido de terceiros a informações as quais não possuem autorização. Na presente temática os sistemas armazenam senhas, credenciais, e-mails, ferramentas de contagem de prazos e penas, números de processos, informações das partes envolvidas, quais sejam: CPF, RG, telefone, endereço, a depender do processo contas bancárias, balanço patrimonial, imposto de renda, número de benefício previdenciário, informações da rotina das pessoas, e até identidade de gênero, orientação sexual e orientação religiosa, entre muitos outros dados. Portanto, o acesso a essas informações pode desencadear tanto prejuízos diretos, como fraudes bancárias e assaltos como indiretos na venda ilegal desses dados, afinal, na contemporaneidade informação é um valioso ativo.

3 MANDAMENTOS DA LGPD

A Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD) estabeleceu como deve ser realizado o tratamento de dados pessoais, assim como medidas para garantir a proteção dos direitos fundamentais: liberdade (Art. 5º, caput, da CF), privacidade (Art. 5º, inciso X, da CF), e o livre desenvolvimento da personalidade da pessoa natural (Art.5º da CF). Após o advento dessa lei, em 2022, a Emenda Constitucional nº 115 incluiu o inciso LXXIX, assegurando o direito à proteção dos dados pessoais como direito fundamental na República Federativa do Brasil.

Além disso, a LGPD estabelece que seus regramentos devem ser seguidos no ambiente analógico como no digital, também determina no Art. 1° que deve ser atendido por pessoas naturais e jurídicas sejam de direito público ou privado. A partir do tema em tela destaca-se:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
>
> I - a operação de tratamento seja realizada no território nacional;
>
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
>
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Sendo assim, os tribunais, enquanto instituições de direito público e sua operação se enquadrando nos incisos acima elencados, estão submetidas à lei e devem se adequar. Isto posto, parte-se a inspecionar as funções desempenhadas pelos tribunais em relação aos dados. Conforme já mencionado, os sistemas dos tribunais operam com muitas informações que são coletadas pelo próprio tribunal, essas informações são acessadas, classificadas, arquivadas e até destruídas. O Poder Judiciário funciona então, pela perspectiva da lei, atua como agente de tratamento de dados (Art. 5º, X) seja enquanto controlador (Art.5º, VI) ou operador (Art.5º, VII), uma vez que:

> Art. 5º Para os fins desta Lei, considera-se:
>
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Para que o tratamento ocorra é preciso que o dado seja coletado e a LGPD estabelece no art. 7º os requisitos para que isso ocorra. É certo que o fornecimento do dado deve ser consentido pelo titular para atender requisito legal ou regulatório; no âmbito da administração pública é permitido o tratamento e compartilhamento para efetividade de políticas públicas, obedecendo requisitos específicos; também pode ser utilizado para a realização de estudos por órgãos de pesquisa, que não seria o caso; para a execução de contrato do qual seja parte o próprio titular de dados; no âmbito processual, o "exercício regular do processo judicial, administrativo ou arbitral"; para a proteção da vida do titular ou terceiro, para salvaguardar a vida de profissionais da saúde; quando for interesse legítimo do controlador ou terceiro desde que não confronte direitos fundamentais do titular que se sobrepõe, devendo ser garantida a proteção dos dados pessoais; e por fim para garantir a proteção do crédito.

Muito embora os parágrafos deste artigo dispensem a exigência do consentimento para dados tornados públicos pelo titular, por outro lado exigem o consentimento para que ocorra o compartilhamento de dados pessoais entre controladores, ressalvadas as hipóteses dispensadas pela lei como na hipótese mencionada anteriormente. No entanto, a dispensa do consentimento não desobriga os agentes de tratamento a descumprirem as demais responsabilidades impostas pela lei, principalmente os direitos do titular, com destaque para a segurança de seus dados.

Ainda em relação aos dados, a lei faz distinção entre dado pessoal, aquela informação capaz de identificar a pessoa natural, e dado pessoal sensível, a informação que traduz características da pessoa natural, tais como origem racial ou étnica, posicionamento político, filiação sindical, orientação sexual, religiosa, informações genéticas entre outros. Em um processo, instrumento principal do Poder Judiciário, conforme já demonstrado, pode-se conter informações puramente pessoais, mas também pessoais sensíveis e estas demandam tratamento e segurança reforçada, pois a simples exposição dessa informação fornece publicidade indesejada pelo titular, ferindo o seu direito de privacidade, intimidade, vida privada, honra e imagem, o que conforme assegura o art. 5º, inciso X da Constituição Federal "o direito a indenização pelo dano material ou moral decorrente de sua violação".

As atividades que envolvam o tratamento de dados pessoais, como nos processos judiciais, devem obedecer os princípios da boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, prevenção, não discriminação, responsabilização, prestação de contas, transparência e segurança. Este último definido no art. 6º como "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".

Nesse sentido, o Conselho Nacional de Justiça - CNJ publicou a Recomendação nº 73 de 20 de agosto de 2020, 6 dias após a LGPD entrar em vigor, sugerindo a adoção de "medidas preparatórias e ações iniciais para adequação às disposições na Lei Geral de Proteção de Dados - LGPD", resolvendo que os tribunais, com exceção do Supremo Tribunal Federal, realizassem adequações na construção de um plano nacional de proteção de dados no âmbito do Poder Judiciário.

Solicitou-se aos órgãos do judiciário a criação de plano de ação que contivesse especificamente: organização e comunicação, direitos do titular, gestão de consentimento, retenção de dados e cópia de segurança, contratos, plano de respostas de incidentes de segurança com dados. Outras medidas foram recomendadas e na ocasião ainda se solicitou a criação de Grupo de Trabalho voltado para as questões de proteção de dados e adequação do tribunal à Lei, e a coleta desses trabalhos auxiliaria o CNJ a desenvolver a política nacional para esse segmento.

Na sequência, a Resolução nº 363, de 12 de janeiro de 2021, portanto antes da entrada em vigor das sanções da LGPD, estabelecidas para 1º de agosto de 2021, o CNJ "Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais" com exceção do Supremo Tribunal Federal. Cria-se o Comitê Gestor de Proteção de Dados Pessoais (CGPD) com o objetivo de ser o responsável pela implementação da Lei nos tribunais, a designação do encarregado pelo tratamento dos dados pessoais, requisito mencionado anteriormente, formação de Grupo de Trabalho Técnico multidisciplinar, elaboração dos atendimentos dos titulares dos dados, criação de endereço eletrônico com informações sobre a aplicação da LGPD aos tribunais, a disponibilização de informação sobre o tratamento de dados para o titular.

Como também, que os tribunais se preocupem com as ações relacionadas à LGPD, com reforço para os procedimentos extrajudiciais que devem estar sob supervisão da Corregedoria Geral da Justiça; fornecer treinamento aos funcionários da justiça, magistrados, servidores, terceirizados, estagiários e outros, a fim de capacitá-los para trabalhar nos moldes da lei; revisão dos contratos com terceirizados; adoção de segurança técnica e administrativa para proteção dos dados; o registro do tratamento dos dados; e informar o Comitê Gestor de Proteção de Dados - CGDP sobre as operações com automação e inteligência artificial.

É evidente que, ao menos em teoria, o CNJ estabeleceu parâmetros para o desenvolvimento de uma governança nacional no Poder Judiciário de adequação dos tribunais, com exceção do STF aos dispositivos da Lei nº 13.709 de 14 de agosto. Entretanto, não há

qualquer menção às próprias sanções que a LGPD estabelece e quais os limites pré-estabelecidos para a atuação dos tribunais.

Na problemática da pesquisa, partindo dos pressupostos elencados, questiona-se, qual a responsabilidade civil dos tribunais, ou melhor, do Poder Judiciário enquanto instituição pública na reparação dos danos causados pela própria ineficiência na guarda dos dados. Além disso, como deve ser caracterizada a configuração de danos morais nesse caso, trata-se de dano presumido ou deve-se provar a efetividade do dano?

4 RESPONSABILIDADE E DANOS MORAIS

A LGPD disciplina no art. 42 que os agentes de tratamento no exercício de suas atividades de tratamento de dados pessoais respondem pelos danos, patrimonial, moral, individual ou coletivo, obrigando-se, portanto, a reparar as violações que causarem à legislação. No entanto, no art. 43 a Lei elenca as exceções para a responsabilidade quando restar provado que não se realizou o tratamento dos dados da discussão; que realizado o tratamento não houve violação da proteção; ou ainda, que o dano pleiteado é consequência de culpa exclusiva do titular ou terceiro. Ademais, no âmbito do Poder Público, existe a indicação no art. 31 que, em casos de infração a proteção de dados, a autoridade nacional possui a liberalidade de encaminhar informes com medidas para cessar a violação e também poderá pedir a produção de relatórios de impacto e sugerir boas práticas.

Desta forma, não há a indicação precisa na lei da modalidade de responsabilidade civil, se subjetiva ou objetiva, do Poder Público na reparação de danos. Neste ponto, é preciso admitir que a LGPD não cria um universo próprio de sanções, é preciso retomar o pensamento kelseniano de hierarquia de normas na construção de um sistema unificado e harmônico. Isto posto, em um exercício de hermenêutica jurídica chega-se à conclusão de que a modalidade de responsabilidade civil que o art. 42 da LGPD não apresenta é a responsabilidade civil objetiva. Porque, desta forma, obedece ao disposto no art. 37 §6º da Constituição Federal que configura a responsabilidade objetiva.

> Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:

> § 6º As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.

Isso significa que, não há necessidade da vítima provar o dolo ou culpa do agente para configurar a responsabilidade, basta provar o nexo causal entre o fato e o dano pleiteado. Trata-se de uma exceção prevista também no Código Civil no art. 927 em contraponto à regra que é a responsabilidade subjetiva presente nos arts. 186 e 187. A modalidade objetiva também é adotada pelo Código de Defesa do Consumidor nos arts. 12,13 e 14. Ademais, a LGPD se inspira nessa lei, CDC, para facultar ao magistrado a inversão do ônus da prova (art. 42, § 2º) em favor do titular, sanando a onerosidade excessiva e hipossuficiência na produção das provas.

Retomando as questões de responsabilidade civil, o Poder Judiciário deve reparar o dano desde que provado o nexo causal, ou seja, a ligação entre a sua conduta e o resultado danoso. Entretanto, existe o dano real e o presumido, e a LGPD também não dispõe sobre essa questão. Configura-se, portanto, inseguranças jurídicas sobre o tema com a interpretação antagônica dos magistrados e magistradas em casos semelhantes pelo Brasil.

Identifica-se duas correntes sobre a temática, a primeira entende que a simples exposição de dados não configura incidente que enseje reparação de danos morais ao se basear no fato da LGPD não discriminar possibilidade contrária no art. 42. Defendem a proximidade deste artigo com o art. 186 do Código Civil para fundamentar que em ambos não há a anunciação específica de um direito moral presumido e que ele é uma exceção de natureza estritamente particular. Outrossim, apontam que a diferença entre eles está na possibilidade de dano moral coletivo do art. 42, elemento que não seria suficiente para superar a regra do Código Civil; o que se fosse, significaria onerosidade excessiva para as empresas e o próprio poder público ao arcar com as demandas por reparação de danos e banalizaria os reais incidentes de violação.

Já a segunda corrente entende que a exposição de dados configura incidente de reparação de danos, não sendo necessária a prova do dano efetivo pois este seria modalidade *in re ipsa*, pois o prejuízo seria presumido sem a necessidade de provas ao se basear no mesmo art. 42 da LGPD com o dever de indenizar em razão do dano gerado com o tratamento de dados. Essa exposição viola os direitos fundamentais da personalidade e privacidade. Além disso, como a lei determina as dispensas de responsabilização no art. 43, trata-se de rol taxativo e os casos práticos que não se enquadrarem nessas dispensas ensejam reparação. Logo, caso o dano tenha de ser provado haverá um empecilho para a responsabilização, consequentemente, criar-

se-á uma situação em que ocorrerá a exposição de dados sensíveis que não se enquadram no rol de dispensas do art. 42 e os agentes de tratamento não serão responsabilizados em se tratando do poder público, pois para o privado existe as sanções das vias administrativas.

Essa matéria controversa não possui jurisprudência específica para o vazamento de dados oriundos do Poder Judiciário, no entanto, outros casos práticos iniciam a discussão do tema e a criação de jurisprudências. Para exemplificar uma decisão contrária, toma-se o processo 1001311-34.2021.8.26.0564 da 13ª Câmara de Direito Privado do TJ/SP reformou a sentença, de recolhimento dos dados pessoais do autor que foram compartilhados sem autorização deste e ao pagamento de dez mil reais a título de danos morais, sob a justificativa de que a obrigação de fazer não possuía viabilidade e não restou comprovado nos autos a violação da dignidade da pessoa humana, honra ou imagem. Para exemplificar uma decisão favorável observa-se o processo 1003122-23.2020.8.26.0157 da 26ª Câmara de Direito Privado do TJ/SP em que a exposição dos dados do cliente no site da empresa ainda que por curto período ensejou indenização de danos morais de dois mil reais ao cliente.

Em relação a dano moral coletivo no processo 0418456-71.2013.8.19.0001 da 1ª Câmara Cível do Rio de Janeiro, o Ministério Público do Rio de Janeiro em apelação em ação civil pública, conseguiu a decisão de indenização por danos morais de quinhentos mil reais e mais mil reais por danos materiais e morais individual aos consumidores afetados pela exposição de ao menos três meses de suas movimentações financeiras na BV Financeira, sob a justificativa de que as empresas ré não adotaram as medidas de segurança cabíveis, não obedeceram cláusulas contratuais e demoraram para perceber o vazamento e adotar medidas de contenção.

Segundo entendimentos do Superior Tribunal de Justiça a respeito do dano *in re ipsa* a excepcionalidade da presunção de dano segue enquanto regra, no entanto, abarca de contaminação de alimento com corpo estranho (REsp 1.899.304), o uso indevido de marca (REsp 1.507.920), violência doméstica (REsp 1.675.3874), recusa do plano de saúde em autorizar tratamento médico emergencial (REsp 1.839.506), agressão a criança (REsp 1.642.318), até comercialização de dados pessoais em banco de dados (REsp 1.758.799). É evidente que o STJ beneficia situações em que há evidente abalo psicológico da vítima para conceder o dano presumido.

Partindo dessa dinâmica, um meio termo pode ser estabelecido nos pedidos de danos morais em casos vazamentos de dados dos tribunais. Em regra, adequando a LGPD ao ordenamento jurídico, e sem a previsão expressa de dano presumido, deve-se provar o dano para configurar a responsabilização. Todavia, nos casos práticos em que fica explícito o abalo

psicológico da vítima, pode-se admitir o dano in re ipsa, de acordo com o demonstrado entendimento do STJ. Dessa maneira não se onera as empresas e o poder público, prestigia-se os casos de efetivo dano.

A controvérsia também existe no direito europeu na General Data Protection Regulation - GDPR, em que a LGPD é inspirada. Assim, em 2021 as cortes da Áustria e Alemanha encaminharam consultas à Corte Europeia de Justiça sobre a temática dos danos morais em casos envolvendo proteção de dados. Contudo, estas perguntas seguem sob análise, espera-se que a partir do posicionamento da corte resultados práticos possam ser produzidos na legislação brasileira.[5]

6 CONCLUSÃO

A Lei Geral de Proteção de Dados apesar de não trazer expressamente a modalidade de responsabilidade civil que o poder público, no caso em tela o Poder Judiciário, deva responder, em adequação ao ordenamento jurídico, deve-se admitir que a responsabilidade seja objetiva. Assim, não há que se provar o dolo ou a culpa do agente de tratamento para a configuração da reparação do dano. Basta que se prove o nexo causal entre o evento/ação e o dano.

Nesse espectro, apesar de garantir a possibilidade de reparação de danos morais em decorrência do tratamento de dados inadequados, a LGPD também não delimita se o dano moral deve ser provado ou presumido. Em razão disso, os tribunais têm decidido em casos semelhantes, visto que não há decisões que envolvam ações contra vazamento dos tribunais, de forma variada, alguns entendendo que o dano tem de ser presumido e outros que deve ser provado.

Mais uma vez deve-se recorrer à adequação ao ordenamento jurídico, e sem a previsão expressa da exceção de dano in re ipsa, deve-se priorizar a regra de provar a efetividade do dano. Entretanto, na variedade dos casos práticos, situações que resultem efetivo dano psicológico à vítima podem admitir a exceção da presunção de dano, possibilidade já pacificada nos entendimentos do Superior Tribunal de Justiça.

Essa controvérsia também existe na legislação europeia, que serviu de inspiração para a criação da LGPD. Assim, espera-se que o pronunciamento da Corte Europeia de Justiça sobre a temática venha a sanar as dúvidas, pacificar o entendimento e produzir efeitos na legislação pátria. A partir dos elementos acima relacionados, observa-se que a legislação de proteção de

[5] Case C-300/21: Request for a preliminary ruling from the Oberster Gerichtshof, Áustria, lodged on 12.5.2021.

dados ainda está em desenvolvimento e os tribunais precisam implementar de forma efetiva programas de governança para atender essas necessidades e garantir o direito constitucional de proteção dos dados pessoais.

REFERÊNCIAS

BISSO, Rodrigo et al. Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados. **Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação**, [S.l.], v. 3, n. 1, mar. 2020. ISSN 2446-7634. Disponível em: https://revistas.setrem.com.br/index.php/reabtic/article/view/378. Acesso em: 2 dez. 2022.

BLUM, Renato Opice; LÓPEZ, Nuria. **Lei Geral de Proteção de Dados no setor público**: transparência e fortalecimento do Estado Democrático de Direito. Cadernos Jurídicos, São Paulo, v. 21, n. 53, p. 171-177, jan./mar. 2020. Disponível em https://bdjur.stj.jus.br/jspui/bitstream/2011/142294/lei_geral_protecao_blum.pdf . Acesso em 20 set. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm . Acesso em: 21 set. 2022.

Case C-300/21: Request for a preliminary ruling from the Oberster Gerichtshof, Áustria, lodged on 12.5.2021.

Consultor Jurídico. **Ataque hacker deixa sistemas da Justiça Federal em PE fora do ar**. Publicado em: 6 abr. 2022. Disponível em: https://www.conjur.com.br/2022-abr-06/ataque-hacker-deixa-sistemas-justica-federal-pe-fora-ar. Acesso em: 19 nov. 2022.

Consultor Jurídico. **TRF-3 suspende prazos processuais e adia transmissão de precatórios**. Publicado em: 1 abr. 2022. Disponível em: https://www.conjur.com.br/2022-abr-01/trf-suspende-prazos-processuais-adia-transmissao-precatorios. Acesso em: 18 nov. 2022.

Correio Brasiliense. **Presidente do STJ diz que foi alertado sobre possibilidade de novo ataque hacker**. Publicado em: 11 nov. 2020. Disponível em: https://www.correiobraziliense.com.br/politica/2020/11/4888154-presidente-do-stj-diz-que-foi-alertado-sobre-possibilidade-de-novo-ataque-hacker.html. Acesso em: 26 nov. 2022.

CNJ. **Privacidade e proteção de dados do cidadão mobilizam Poder Judiciário**. Disponível em: https://www.cnj.jus.br/privacidade-e-protecao-de-dados-do-cidadao-mobilizam-poder-judiciario/#:~:text=Ao%20estabelecer%20as%20medidas%20para,nos%20atos%20processuais%20e%20administrativos. Acesso em: 10 nov. 2022.

FRANÇA, L. A.; COELHO, L. A. **A responsabilidade civil do poder público à luz da lei geral de proteção de dados**: uma análise acerda da divulgação de dados previdenciários. Revista Ibero-Americana de Humanidades, Ciências e Educação, [S. l.], v. 8, n. 5, p. 3030–

3049, 2022. DOI: 10.51891/rease.v8i5.5925. Disponível em: https://periodicorease.pro.br/rease/article/view/5925 . Acesso em: 24 set. 2022.

HIRATA, Alessandro; LIMA, Cintia Rosa Pereira de. Migalhas, Franca, 11 dez. 2020. **39 dias após o ataque cibernético ao STJ**: reflexões e desafios. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/337701/39-dias-apos-o-ataque-cibernetico-ao-stj--reflexoes-e-desafios. Acesso em: 20 nov. 2022.

LIMA, P. R. S.; MARQUES FERREIRA, L. M.; ALBUQUERQUE PEIXOTO, A. L. V. de. **Gestão da segurança da informação**: análise de políticas de defesa cibernética e estratégias para a proteção de dados e informações da administração pública brasileira. P2P E INOVAÇÃO, [S. l.], v. 9, n. 1, p. 206–221, 2022. DOI: 10.21721/p2p.2022v9n1.p206-221. Disponível em: https://revista.ibict.br/p2p/article/view/5993. Acesso em: 19 dez. 2022.

MARTINES, Fernando; COELHO, Gabriela. **CNJ sofre ataque de hacker e dados de milhares de pessoas são vazados**. Consultor Jurídico, 1 abr. 2019. Disponível em: https://www.conjur.com.br/2019-abr-01/cnj-sofre-ataque-hacker-dados-milhares-pessoas-vazam. Acesso em: 26 nov. 2022.

MARTINS, Ricardo Maffeis; GUARIENTO, Daniel Bittencourt. **TJ/SP limita indenização por dano moral no vazamento de dados pessoais**. Migalhas, 18 mar. 2022. Disponível em: https://www.migalhas.com.br/coluna/impressoes-digitais/361788/tj-sp-limita-indenizacao-por-dano-moral-no-vazamento-de-dados-pessoais. Acesso em: 15 nov. 2022.

OLIVEIRA, J. V. de. **Vazamento de dados pessoais e responsabilização civil**: compatibilidades e conflitos entre o Código de Defesa do Consumidor e a lei geral de proteção de dados. Revista Brasileira de Direito Civil, *[S. l.]*, v. 31, n. 01, p. 17, 2022. Disponível em: https://rbdcivil.emnuvens.com.br/rbdc/article/view/478. Acesso em: 5 dez. 2022.

SILVA, Marcos Vinicius Viana; SCHERF, Erick da Luz; SILVA, José Everton da. **The Right to Data Protection versus "Security"**: Contradictions of the Rights-discourse in the Brazilian General Personal Data Protection Act (LGPD). Revista Direitos Culturais (Cultural Rights Review), Vol. 15. No. 36 (2020). , Disponível: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3569928. Acesso em: 23 set. 2022.

STJ. **In re ipsa**: os entendimentos mais recentes do STJ sobre a configuração do dano presumido. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2022/11092022-In-re-ipsa-os-entendimentos-mais-recentes-do-STJ-sobre-a-configuracao-do-dano-presumido.aspx. Acesso em: 10 nov. 2022.

STOCO, Rui. **Tratado de responsabilidade civil**: doutrina e jurisprudência. 7 ed. São Paulo: Editora Revista dos Tribunais, 2007.

WARREN, Samuel Dennis; BRANDEIS, Louis Dembitz. **The right to privacy**. Harvard Law Review, v.4, n.5, dez. 1890. Disponível em: http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html . Acesso em: 20 set. 2022.

WIMMER, Miriam. **O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público**. In: Tratado de proteção de dados pessoais. Coordenadores: Danilo Doneda, Laura S. Mendes, Ingo W. Sarlet, Otavio Luiz R. Jr, Bruno Bioni, Rio de Janeiro, Forense, 2021, p. 271 e seguintes. Disponível em: https://sollicita.com.br/Noticia/?p_idNoticia=18643&n=a-lgpd-e-o-tratamento-de-dados-pessoais-pelo-poder-p%C3%BAblico. Acesso em: 26 nov. 2022.