CENTRO UNIVERSITÁRIO SÃO JOSÉ
CURSO DE DIREITO

FRANCINE MAGALHÃES
INGRID DOS SANTOS CRUZ
JÚLIA DA SILVEIRA GIBSON

A LEI DE PROTEÇÃO DE DADOS À LUZ DO AGRAVO EM RECURSO ESPECIAL Nº 2.130.619-SP

Rio de Janeiro
2023.2

FRANCINE MAGALHÃES
INGRID DOS SANTOS CRUZ
JULIA DA SILVEIRA GIBSON

A LEI DE PROTEÇÃO DE DADOS À LUZ DO AGRAVO EM RECURSO ESPECIAL Nº 2.130.619-SP

Trabalho de Conclusão de Curso apresentado para a Disciplina de TCC II, sob a orientação da Professora Mestre Leilane Lima de Paula.

Rio de Janeiro
2023.2

DEDICATÓRIA

Dedicamos este trabalho a todas as pessoas que possibilitaram a realização deste estudo e que caminharam ao nosso lado durante esta jornada acadêmica.À nossa família, pelo amor incondicional, incentivo e apoio constante. Cada conquista é também a de vocês.Aos meus amigos, que foram fontes de inspiração e motivação, e que estiveram ao nosso lado nos momentos de desafio. Aos nossos professores e orientadores, pela orientação sábia, paciência e ensinamentos valiosos.Aos nossos colegas de curso, pelas trocas enriquecedoras de conhecimento e experiências. Este trabalho é dedicado a todos vocês, com profunda gratidão.

AGRADECIMENTO

Gostaríamos de expressar nossa sincera gratidão a todas as pessoas que permitiram a realização deste sonho.

Primeiramente, gostaríamos de agradecer a Deus, por toda nossa conquista. Se chegamos até aqui com certeza foi graças a ele.

Agradecemos a nossa orientadora, Mestre Leilane Lima, pela paciência ao longo deste processo. Seu apoio foi fundamental para o nosso sucesso.

Também somos gratas à nossa família por todo apoio, encorajamento e compreensão durante esses cinco anos intensos. O apoio de vocês foi essencial para que pudéssemos superar todos os desafios.

Não podemos deixar de mencionar nossos amigos de turma, por toda troca diária, por dividir conosco momentos tão difíceis, tornando esse processo menos difícil e auxiliando a não desistir.

Por fim, agradecemos a todos que de alguma forma contribuíram para este trabalho, mesmo que não estejam mencionados aqui. Cada pequeno gesto de apoio e encorajamento desempenhou um papel significativo na nossa formação.

RESUMO

Este trabalho tem por objetivo analisar a decisão proferida em sede recursal, especificamente o teor do Agravo em Recurso Especial de nº 2.130-619 — SP, oriundo dos autos de nº 1003203-67.2021.8.26.0405, que estabelece que o dano moral decorrente do vazamento de dados não é presumido. Tal decisão contradiz o entendimento específico e as disposições gerais da Lei Geral de Proteção de Dados (LGPD), uma vez que traz em voga questionamentos cruciais sobre a proteção da privacidade e responsabilidade de terceiros no tratamento de informações personalíssimas.Nesse contexto, este estudo remete à discussão sobre o papel da Lei Geral de Proteção de dados (LGPD) na regulação do vazamento de dados e a posição adotada pelo mencionado recurso, sendo certo que a referida decisão dispõe que o dano moral não deve ser presumido, indicando a necessidade de comprovação efetiva do prejuízo sofrido pelo titular dos dados.Nesse ínterim, a pesquisa aborda os fundamentos jurídicos que embasam a decisão, considerando princípios constitucionais, legislação específica e precedentes judiciais relevantes, bem como analisa a Lei Geral de Proteção de Dados (LGPD), destacando suas disposições sobre responsabilidade, segurança e tratamento de dados pessoais.Por fim, o artigo analisa a interação da Lei específica e o entendimento pátrio sobre o tema, explorando criticamente a decisão do Superior Tribunal de Justiça, considerando as implicações para a proteção da privacidade e a responsabilização das partes envolvidas no vazamento de dados. O trabalho também investiga possíveis lacunas na legislação e sugere reflexões sobre a necessidade de ajustes normativos para lidar com os desafios contemporâneos relacionados a esse Direito Fundamental.

Palavra-Chave: Lei Geral de Proteção de dados (LGPD). Vazamento de dados. Informações personalíssimas. Responsabilidade de terceiros. Poder Judiciário. Direito Fundamental.

ABSTRACT

This work aims to analyze the decision handed down on appeal, specifically the content of the Appeal in Special Appeal No. 2.130-619 — SP, originating from case No. 1003203-67.2021.8.26.0405, which establishes that the moral damage resulting from the Data leakage is not assumed. This decision contradicts the specific understanding and general provisions of the General Data Protection Law (LGPD), as it raises crucial questions about the protection of privacy and the responsibility of third parties in the processing of very personal information. In this context, this study refers to the discussion on the role of the General Data Protection Law (LGPD) in regulating data leaks and the position adopted by the aforementioned appeal, given that the aforementioned decision provides that moral damage should not be presumed , indicating the need for effective proof of the loss suffered by the data subject. In the meantime, the research addresses the legal foundations that support the decision, considering constitutional principles, specific legislation and relevant judicial precedents, as well as analyzing the General Data Protection Law (LGPD), highlighting its provisions on responsibility, security and data processing. personal. Finally, the article analyzes the interaction of the specific Law and the national understanding on the topic, critically exploring the decision of the Supreme Court of Justice, taking into account the implications for the protection of privacy and the accountability of the parties involved in the data leak. The work also investigates possible gaps in legislation and suggests reflections on the need for regulatory adjustments to deal with contemporary challenges related to this Fundamental Right.

Keyword: General Data Protection Law (LGPD). Data leak. Very personal information. Third party liability. Judicial power. Fundamental right.

SUMÁRIO

INTRODUÇÃO

O presente prefácio, busca, de maneira simplória, desvender uma análise axiológica e cronológica dos eventos e das mudanças sociais necessárias para que a privacidade, direito de 1ª geração[1], evolua e ganhe novos contornos para que se seja possível a plena discussão sobre o direito fundamental à proteção de dados[2]. Nesse introito, pode-se afirmar que o ponto de partida é a Constituição.

O grande escritor franco-argelino Albert Camus inicia seu Magnum Opus diz que "(…)uma forma conveniente de travar conhecimento com uma cidade é procurar saber como se trabalha, como se ama e como se morre.[3]".

Se transportássemos essa afirmação para o nosso ordenamento jurídico e, ao invés de cidade, buscássemos conhecer o Estado de Direito, veríamos que do amor, se inicia a família, à morte, que ela não faz cessar, ou seja, tudo perpassa pela nossa Constituição de 1988, logo, não seria diferente com a privacidade e suas novas perspectivas.

Antes de adentrar a análise da Carta Magna, é preciso analisar a gênese das ideias que contribuíram para a sua formação e, consequentemente, para todos os valores que ela transmitiria.

A Constituição brasileira de 1988 sofre inúmeras influências, mas duas se reputam imprescindíveis, são elas: (i) do ponto de vista filosófico, é influenciada pelo Neoconstitucionalismo do pós-segunda guerra e, ainda, (ii) do ponto de vista fático, alumia-se num processo de redemocratização após o fim da ditadura militar (1964-1985) no Brasil.

O peso do Neoconstitucionalismo garante uma Carta principiológica e erguida sob a premissa de construção de uma normatividade inerente à Constituição, que nela mesmo ganha força, e, somado a isso, o peso do contexto fático, faz nascer um rol de inúmeros direitos e garantias fundamentais ao longo de todo o texto constitucional[4].

O impacto disso chacoalharia as instituições civilistas e, a melhor doutrina, viria então a consagrar a necessidade de uma filtragem constitucional e aquilo que se convencionou denominar de Direito Civil-Constitucional ou Constitucionalização do Direito Civil.

---

1 RAMOS, André de Carvalho. Curso de Direitos Humanos – 8ª ed. – São Paulo: Saraiva Educação, 2021, p.60.
2 BRASIL, Constituição (1988), Emenda Constitucional nº155/2022 – 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 pessoais. Art. 5, LXXIX. Disponível em: https: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 15 ago. 2023.
3 CAMUS, Albert. A Peste. 38ªed. – Rio de Janeiro: Record, 2022, p.09.
4 BARROSO, Luís Roberto. Efetividade das normas constitucionais por que não uma constituição para valer? Revista de direito da Procuradoria Geral do Estado do Rio de Janeiro, n. 39,1987, p. 27-61.

Como era de se esperar, com novos ares democráticos, ajustaram-se as velas do Estado Democrático de Direito ao sabor dos novos ventos, o que, invariavelmente, fez nascer a necessidade de releitura de alguns institutos, de criação de novos direitos fundamentais e, como se buscará demonstrar nesse artigo científico, a ampliação de proteção e do espaço da privacidade no ordenamento jurídico nacional.

Com isso, num primeiro momento, será abordada a Lei Geral de Proteção de Dados de nº 13.709/18. Posteriormente será discutido brevementea respeito do conceito de privacidade e intimidade na era digital, conceitos estes que por vezes se confundem. Ato contínuo, será analisado o caso do Facebook, que exemplifica como as empresas de tecnologia podem enfrentar desafios em relação à privacidade dos dados, em seguida serão explorados os desafios que envolvem a regulação de dados pessoais. Por fim, será analisado o acórdão do Agravoem Recurso Especial (RESP) 2.130.619-SP, uma recente decisãodo Superior Tribunal de Justiça (STJ) e será examinado como o referido julgado impactará a vida dos consumidores.

1 A LEI GERAL DE PROTEÇÃO DE DADOS N° 13.709/18

O advento da era digital revolucionou a troca de dados, proporcionando uma velocidade sem precedentes. No entanto, mesmo diante dos inegáveis benefícios desse avanço, é natural vir uma preocupação inerente às informações e dados compartilhados na rede.

Por essa razão, foram levantadas as preocupações sobre a privacidade e o uso adequado das informações pessoais. Nesse contexto, surgiua Lei Geral de Proteção de dados (Lei n° 13.709), aprovada em 2018, a lei tem o objetivo de regulamentar o tratamento de dados pessoais no Brasil, tanto por entidades públicas quanto privadas. Inspirada no Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, a LGPD (Lei Geral de Proteção de dados) visa criar um ambiente legal que proteja os direitos dos cidadãos em relação às suas informações pessoais, estabelecendo diretrizes claras para a coleta, armazenamento, processamento e compartilhamento desses dados.

Além disso, a LGPD (Lei Geral de Proteção de Dados) é embasada por uma série de princípios delineados no artigo 6º da referida legislação:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de

> tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas conforme o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, segundo a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.[5]

Primeiramente, da finalidade, esta que exige que o tratamento de dados ocorra para propósitos legítimos, específicos, explícitos e previamente informados ao titular, sem a possibilidade de modificação.

Em seguida, é mencionada a adequação, que define que apenas determinados dados podem ser utilizados, conforme apresentado ao titular.

Outro princípio relevante é a necessidade, que dispõe que o tratamento de dados pessoais deve estar relacionado a finalidades específicas e legítimas, com a coleta de dados limitada ao mínimo necessário para atingir essas finalidades.

Além dos supracitados, há o princípio do livre acesso, que garante aos titulares o direito de acessar os dados pessoais coletados e processados por uma organização. Há também o princípio da qualidade dos dados, que visa assegurar ao titular a exatidão, clareza, pertinência e atualização dos dados conforme necessário para atingir a finalidade do tratamento.

Para a Lei Geral de Proteção de Dados (LGPD), transparência é a obrigação das organizações em informar aos titulares dos dados como suas informações serão tratadas, incluindo os propósitos do tratamento, os tipos de dados coletados e os direitos dos titulares; segurança são medidas técnicas e organizacionais que devem ser implementadas para proteger os dados pessoais contra acesso não autorizado, vazamentos e outros incidentes de segurança;

---

[5]BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Art.6. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 06 out. 2023.

prevenção são as medidas que possam prevenir danos em caso de necessidade; a não discriminação garanteo não tratamento de dados para fins discriminatórios ilícitos ou abusivos.

Por fim, o princípio da a responsabilização e prestação de contas, visa a garantir a observância e a adoção de medidas eficazes para comprovar o efetivo cumprimento das normas da lei.

Após a apresentação dos princípios, pode-se notar que todos eles desempenham um papel fundamental na implementação da Lei, auxiliando a legalidade do tratamento de dados pessoais, sendo regidos pelo princípio da boa-fé.

Dito isso, é possível observar, umatransformação significativa, não apenas no âmbito jurídico, mas também na maneira como grandes empresas tratam os dados de colaboradores e titulares. A aprovação da Lei Geral de Proteção de Dados (LGPD), exigiu a implementação de novas medidas de segurança, ajustes nas políticas de privacidade e segurança, bem como a inclusão de cláusulas pertinentes em contratos.

A Lei Geral de Proteção de Dados (LGPD) é um marco importante na história da proteção de dados no Brasil, estabelecendo regras claras e princípios éticos para o tratamento de dados pessoais, protegendo os direitos fundamentais dos cidadãos em um mundo cada vez mais digital.

A implementação bem-sucedida da Lei Geral de Proteção de Dados (LGPD), não apenas reforça a privacidade, mas também promove um ambiente de confiança entre as organizações e os indivíduos, pavimentando o caminho para um futuro em que a inovação e a segurança caminham juntas.

1.1 O CONCEITO DE PRIVACIDADE E INTIMIDADE NA ERA DIGITAL

Inicialmente, é de extrema relevância estabelecer distinção entre os conceitos de privacidade e intimidade, uma vez que frequentemente acabam sendo confundidos, especialmente devido à crescente divulgação da vida pessoal nas redes sociais.

Entretanto, apesar de diversas vezes consideradas sinônimos, intimidade e privacidade, na verdade, possuem conceitos distintos, mesmo que seja uma distinção sutil e dependente de contexto e interpretação. Em termos gerais, a privacidade engloba o direito de controlar o acesso a informações pessoais, podendo abranger várias áreas da vida, como dados pessoais e correspondência. Por outro lado, a intimidade se concentra em aspectos mais profundos e pessoais, abordando pensamentos íntimos, sentimentos profundos e relacionamentos afetivos.

A intimidade é frequentemente vista como o núcleo mais interno da privacidade, englobando informações extremamente pessoais que uma pessoa pode preferir não compartilhar com a maioria das pessoas. Tanto a privacidade quanto a intimidade desempenham papéis fundamentais na proteção dos direitos individuais, embora a interpretação e aplicação desses conceitos possam variar conforme a legislação e as normas culturais.

Gabriel Rigoldi Vidal,[6] em seu artigo, no meio acadêmico, aduz que há divergências significativas na utilização dos termos mencionados. Por vezes, os conceitos de "vida privada" e "intimidade" são usados de maneira intercambiável, enquanto em outras instâncias, o termo "privacidade" é preferido. Com o intuito de esclarecer esta questão e evitar ambiguidades na nomenclatura, será feita uma análise concisa dos significados associados a esses termos.

Apesar de existirem pequenas controvérsias e debates sobre o assunto, a compreensão predominante é que a "intimidade" é considerada o núcleo essencial da "vida privada", representando o espaço interno e pessoal desta última.

Nessa perspectiva, Ferreira Filho[7] sustenta a ideia de que a intimidade constitui o cerne da vida privada, representando o seu espaço mais interno. Ele aborda a desafiante questão de distinguir entre vida privada e intimidade, argumentando que a última é um componente fundamental da primeira, constituindo seu aspecto mais íntimo, porém não se confundindo com ela.

Mateucci[8] por sua vez, utiliza uma metáfora de círculos concêntricos para ilustrar esses conceitos. No centro, o círculo de menor raio representa a "intimidade", caracterizada pelo recato, isolamento e o indivíduo voltado para si, em um espaço inviolável. O círculo de maior raio, englobando o interior, abrange situações que, embora compartilhadas com algumas pessoas, o indivíduo não deseja que se tornem de conhecimento público.

As palavras e a interpretação de José Afonso da Silva, conforme seu comentário sobre o artigo 5º, inciso X, da Constituição Federal de 1988,[9] são consideradas relevantes e significativas no cenário brasileiro:

---

[6]VIDAL, Gabriel Rigoldi. Conceituação do direito à privacidade em face das novas tecnologias. **Orientador: Professora Doutora Riva Sobrado de Freitas**, 2014.
[7]FERREIRA FILHO, M. G. *Curso de direito constitucional*. 33.ed. rev. e atual. São Paulo: Saraiva, 2007. p. 296
[8]MATEUCCI, C. R. F. *Privacidade e internet. Revista de Direito Privado,* São Paulo, ano 5, p.46-55, jul.-set. 2004.
[9]BRASIL, Constituição (1988), Capítulo I – Dos Direitos Individuais e Coletivos. Art.5, X. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm Acesso em: 15 ago. 2023.

> O dispositivo põe, desde logo, uma questão, a de que a intimidade foi considerada um direito diverso dos direitos à vida privada, à honra, à imagem das pessoas, quando a doutrina os reputava com outros, manifestação daquela. De fato, a terminologia não é precisa. Por isso preferimos usar a expressão direito à privacidade, num sentido genérico e amplo, de modo a abarcar todas as manifestações da esfera íntima, privada e da personalidade que o texto constitucional em exame consagrou.[10]

Enquanto Matos Pereira procura conceituar a privacidade como:

> O conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidido a quem, quando, onde e em que condições, sem a isso pode ser legalmente sujeito.[11]

Relevante que, conforme os pensadores supracitados, as expressões não são idênticas, mas sim relacionadas de uma maneira em que a intimidade é vista como uma categoria mais específica dentro do conceito de vida privada, assim optamos por empregar o conceito de "privacidade" de maneira ampla, de modo a englobar tanto a "intimidade" quanto a "vida privada" como componentes integrados. Essa abordagem evita potenciais discrepâncias que poderiam surgir de uma separação rígida entre esses termos. Além disso, permite-se abordar, em nossas discussões, as questões relacionadas a esse direito no contexto das novas tecnologias.

Analisando a questão sob uma perspectiva tecnológica, Maria Eduarda Gonçalves preceitua[12]o ciberespaço, como o principal vetor da Internet, caracterizado por sua invisibilidade, intangibilidade e intercomunicabilidade. O avanço do processamento de informações por meio de computadores deu origem a esforços legislativos e judiciais para proteger os direitos relacionados à informação e regulamentar o acesso e uso desses recursos.

Nas palavras de Gonçalves, a Internet é notável por ser um espaço de comunicação direta, organizado com base em uma "relação todos-todos". É nesse contexto que as pessoas interagem com a rede mundial de computadores, a qual armazena uma ampla variedade de conteúdos, sejam eles compartilhados pelos próprios usuários sobre suas preferências e vida privada, ou os dados fornecidos pelos servidores.

Entretanto, a interação na rede apresenta um desafio considerável: a distinção entre as esferas pública e privada de cada indivíduo no ambiente virtual. Torna-se uma tarefa complexa discernir o que deve ou não estar disponível para acesso público na internet. Isso

---

[10] AFONSO DA SILVA, José. Curso de Direito Constitucional Positivo. 25ª ed. São Paulo: Malheiros, 2005, p. 206

[11]PEREIRA, J. Matos. Direito de informação. Dicionário de História de Portugal, v. 7, p. 15, 1980.

[12]GONÇALVES, Maria Eduarda. Direito da Informação: novos desafios e formas de regulação na sociedade da informação. Coimbra: Almedina, 2003.

ocorre porque a interação e o armazenamento de conteúdo na rede tornam praticamente impossível a remoção de informações uma vez que são publicadas online.

Nesse ínterim, a informática é considerada uma ameaça significativa à privacidade, uma vez que possibilita uma vigilância constante, a criação de enormes bancos de dados e a rápida distribuição de informações em escala global.

Segundo Nissenbaum, "la informática se considera una gran amenaza para la privacidad porque permite una vigilância omnipresente, bases de datos gigantescas y una veloz distribución de información en El globo entero"[13].

Ressalta-se que acesso à internet se estabeleceu como o principal meio de comunicação no século XXI, permitindo com que as pessoas se conectem a qualquer lugar do mundo. No entanto, à medida que a tecnologia avança e a internet cresce de forma descontrolada, o conceito de privacidade acaba se misturando com intimidade e enfrenta desafios significativos.

É de suma importância destacar que a privacidade é um direito fundamental, devidamente garantido em nossa legislação, em no art. 5, inciso X, da Constituição da República Federativa do Brasil de 1988[14] e no art. 21 do Código Civil[15] e a sua preservação desempenha um papel essencial na proteção das informações pessoais, dados sensíveis e assuntos pessoais contra acesso, uso ou divulgação por parte de pessoas, ou meios não autorizados.

O avanço tecnológico e a crescente tendência à autoexposição têm impactado consideravelmente a privacidade e intimidade das pessoas.

Segundo o Massachusetts Institute of Technology (MIT), no Brasil, em 2018 e 2019, foram registrados um aumento de, 493% de dados expostos e no ano de 2021, foi considerado o sexto país com mais vazamentos de dados no mundo[16].

Isso decorre da coleta constante de dados pessoais em larga escala, impulsionada pela disseminação das redes sociais e pela partilha de informações, o que tornou a fronteira entre o mundo online e a vida privada mais difusa.

---

[13]NISSENBAUM, Helen. Privacidad amenazada. Tecnología, política y la integridade de la vida social. México:Oceano, 2010, p. 21.

[14]BRASIL, Constituição (1988), Capítulo I – Dos Direitos Individuais e Coletivos. Art.5, X. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 ago. 2023.

[15]BRASIL, Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: https://www.jusbrasil.com.br/topicos/10729483/artigo-21-da-lei-n-10406-de-10-de-janeiro-de-2002. Acesso em: 15 ago. 2023.

[16]NETO, Nelson Novaes et al. Desenvolvimento de um banco de dados global sobre violação de dados e os desafios encontrados. **Revista de Qualidade de Dados e Informação (JDIQ)**, v. 1, pág. 1-33, 2021.

Além das redes sociais, é pertinente mencionar as plataformas de compras e os sistemas de pagamentos eletrônicos, nos quais uma quantidade exorbitante de dados pessoais é diariamente inserida. Muitas vezes, os titulares desses dados não demonstram preocupação com sua segurança, confiando frequentemente suas informações a essas plataformas digitais e, dessa forma, expondo seu direito à privacidade a riscos potenciais.

O vazamento de dados, se utilizado de forma maliciosa, pode comprometer substancialmente a tutela dos direitos individuais.

Isso porque, a exposição de informações que deveriam ser mantidas em sigilo representa uma ameaça significativa tanto a privacidade quanto a intimidade, uma vez que, quando tais informações, se em lugares errados, podem ser exploradas de maneirai licita, resultando em sérias consequências à vida, a segurança e a integridade das pessoas. Isso ocorre por várias razões, que incluem abertura de contas fraudulentas, o uso de informações pessoais para fins de assédio e extorsão, bem como a prática de crimes digitais.

2 O CASO DO FACEBOOK

O Facebook, foi criado por Mark Zuckerberg no ano de 2004 e cresceu para se tornar uma das maiores redes sociais do mundo. Com bilhões de usuários, a plataforma digital, coleta uma enorme quantidade de dados pessoais, com informações de perfil, interações diárias, localização, preferências, entre outros.

Sendo assim, o vazamento de dados do Facebook torna-se um assunto de grande importância, uma vez que a proteção dessas informações é essencial para a privacidade dos usuários.

O caso do Facebook na proteção de dados é um dos marcos mais emblemáticos no debate sobre privacidade e segurança na era digital, isso porque, a plataforma enfrentou inúmeras críticas e controvérsias ao longo dos anos, destacando a importância da regulamentação e fiscalização, eficazes em um cenário onde os dados pessoais dos usuários são coletados em grande escala.

Diversos incidentes ocorreram ao longo desses anos de atividade, expondo a vulnerabilidade na proteção de dados da plataforma, contudo, destaca-se o incidente da Cambridge Analytica, em 2018, onde 87 milhões de dados de usuários do Facebook foram compartilhados com uma empresa de análise de dados, levantando preocupações significativas sobre a manipulação de informações para fins políticos. O Brasil aparece na

lista, como o oitavo país mais atingido do mundo, com 443.117 usuários.[17]

Nesse contexto, o vazamento desencadeou investigações, ações judiciais e, eventualmente, resultou em mudanças nas políticas de privacidade do Facebook e em regulamentações mais rigorosas em todo o mundo, fazendo com que a condenação do Facebook entrasse para o marco da maior multa já aplicada pela Comissão Federal de Comércio dos Estados Unidos (FTC), no valor de US$ 5 bilhões (dólares).[18]

Além do referido vazamento, o Facebook também foi condenado por uma série de descumprimentos, incluindo a lei Children's Online Privacy Protection Actda (FDC) de 2012, que visava proteger a integridade e imagem de crianças com menos de 13 anos na internet. Ainda, segundo a referida Lei, houve uma conferência em que a empresa informou que não haveria mais permissão para terceiros armazenarem dados dos usuários e de suas conexões, porém, em outra ocasião, informou que a coleta de dados das conexões dos usuários se manteria por mais um ano.

O caso destacou a necessidade de as empresas de tecnologia serem responsáveis pela proteção dos dados pessoais de seus usuários e levou a um aumento na conscientização sobre os direitos à privacidade. Além disso, incentivou discussões sobre a necessidade de regulamentações mais robustas para proteger as informações pessoais em um ambiente digital em constante evolução. Esse caso ilustra o desafio contínuo de equilibrar a inovação tecnológica com a preservação da privacidade e segurança dos indivíduos.

Segundo o Autor Ronaldo Lemos, que trata sobre o assunto, não há nada que possamos fazer hoje para evitar sermos monitorados – pelas empresas, pelo governo ou por qualquer outro indivíduo na rede. Pelo menos não sob uma perspectiva individual. A privacidade já é uma exigência do passado.[19]

Com todo esse cenário, para lidar com os vazamentos de dados, o Facebook e outras empresas implementaram medidas de segurança, como auditorias e políticas de proteção de dados mais rigorosas.

No entanto, essas medidas continuam sendo alvo de debate em relação à sua eficácia. Sendo assim, legisladores estão trabalhando para estabelecer diretrizes mais rígidas para proteger a privacidade dos usuários.

---

[17]GAUCHAZH. Vazamento de dados do Facebook atinge 443 mil usuários no Brasil. Disponível em: https://gauchazh.clicrbs.com.br/mundo/noticia/2018/04/vazamento-de-dados-do-facebook-atinge-443-mil-usuarios-no-brasil-cjfmg3kqh06de01phlwlsy4be.html. Acesso em: 15 out. 2023.

[18]LESLIE, Fair.FTC impõe multa de US$ 5 bilhões e novas restrições de privacidade no Facebook. Disponível em: https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook. Acesso em: 10 nov.2023.

[19]RONALDO LEMOS, *A batalha pela privacidade na internet já está perdida*. *Época Negócios,2014.*

Analisando casos jurídicos e decisões judiciais relacionadas aos vazamentos de dados, é possível identificar grandes preocupações com a questão entre os legisladores. Uma delas é a necessidade de punições eficazes para garantir a conformidade com as leis de proteção de dados e assim conscientizar a população sobre a relevância da privacidade nos negócios digitais.

Os casos de vazamento de dados do Facebook servem como um lembrete das responsabilidades das empresas na era digital e da necessidade de regulamentações rigorosas para garantir a privacidade dos usuários.

3 DESAFIOS ENVOLVENDO A REGULAÇÃO DE DADOS PESSOAIS

A regulação de dados pessoais tornou-se um tópico de crescente relevância em um mundo cada vez mais digital e interconectado. Com a proliferação de tecnologias de coleta, armazenamento e processamento de informações pessoais, surgiram uma série de desafios que requerem atenção especial, principalmente no âmbito do direito.

A proteção da privacidade e a garantia dos direitos individuais em um ambiente de dados em constante expansão são questões cruciais.

Neste tópico, serão explorados os principais desafios que envolvem a regulação de dados pessoais, abordando questões de segurança, consentimento, transferência internacional e responsabilidade das empresas.

À medida que a sociedade avança em direção a um futuro cada vez mais orientado por dados, compreender esses desafios e trabalhar para resolvê-los torna-se imperativo para proteger os direitos e a privacidade das pessoas em todo o mundo, mas especificamente aqui, trata-se de um direito protegido pela Constituição Federal.

Os desafios mencionados a seguir enfatizam a necessidade de regulamentações eficazes para a proteção de dados pessoais, bem como o papel das empresas na garantia de conformidade e no respeito à privacidade dos indivíduos.

Além disso, a colaboração entre governos, empresas e sociedade civil é essencial para abordar esses desafios de maneira eficaz. Esses desafios incluem a proteção da privacidade, para garantir que os dados pessoais sejam protegidos contra acessos não autorizados. Vazamentos e uso indevido é um desafio fundamental. Isso envolve uma definição de padrões de segurança, como criptografia, para proteger os dados; A coleta adequada de consentimento é essencial, exigindo que as empresas obtenham assinaturas claras, específicas e informadas antes de coletar e processar dados; A transferência de dados

internacionais enfrenta desafios em garantir a conformidade com as regras de proteção de dados de diferentes jurisdições; A complexidade da regulamentação em muitos países, com várias leis e regulamentos, torna desafiador o entendimento e cumprimento por parte das empresas; A definição da responsabilidade das empresas em relação à proteção de dados pessoais requer investimento em infraestrutura, treinamento e conformidade; O direito de exclusão, que permite que os indivíduos solicitem a exclusão de seus dados, representa desafios de implementação e implicações técnicas; A proteção de dados sensíveis, como informações médicas ou religiosas, exige medidas adicionais para garantir sua segurança; A fiscalização e aplicação das regulamentações enfrentam desafios, especialmente no caso de empresas internacionais; A educação e conscientização sobre os direitos dos indivíduos e a importância da proteção de dados pessoais são fundamentais; A evolução constante da tecnologia, incluindo inteligência artificial, aprendizado de máquina e Internet, exige que os regulamentos se mantenham atualizados para abordar novos desafios.

Nesse contexto, ressalta-se que enfrentar esses desafios requer uma abordagem múltipla que envolva reguladores, legisladores, empresas, tecnólogos, acadêmicos e a sociedade civil.

À medida que a tecnologia e as ameaças à privacidade evoluem, a regulamentação de dados pessoais deve ser flexível e adaptável para proteger efetivamente os direitos e a privacidade das pessoas.

3.1 ENTENDIMENTO DO STJ SOBRE O AGRAVO EM RESP 2.130.619-SP

Neste capítulo, será explorado a decisão recente do Superior Tribunal de Justiça e de como há influência desse entendimento na discussão sobre a regulamentação de dados pessoais.

Antes de mais nada, é de suma importância contextualizar o julgamento do Agravo em Recurso Especial de nº 2.130.619 – SP, e após será desdobrado uma análise sobre como a decisão vem influenciando a discussão no cenário jurídico contemporâneo.

Nesse contexto, cumpre elucidar que o presente julgado teve como origem, o processo de nº 1003203-67.2021.8.26.0405, ação de indenizatória, distribuída em 17.02.2021, em face da empresa Eletropaulo Metropolitana Eletricidade de São Paulo S.A (Enel Brasil S.A.), pleiteando indenização de R$ 15.000,00 (quinze mil reais), a título de danos morais.

A ação proposta pela parte autora, Maria Edite de Souza, questionava o vazamento de dados pessoais, relativos ao contrato estabelecido entre as partes, uma vez que as informações

personalíssimas foram compartilhadas para um número indeterminado de pessoas, resultando em apropriaçãoindevida de identidade, fraudes, importunações e afins.

Apesar, da primeira instância, ter julgado improcedente os pleitos autorais, o Tribunal de Justiça, em sua 27ª Câmara de Direito Privada, de maneira acertada e escorreita, deu provimento ao recurso da autora, condenando, assim, o apelado ao pagamento de danos morais, no montante de R$ 5.000,00 (cinco mil reais), com juros moratórios desde a citação e a correção monetária desde o arbitramento, nos termos da Súmula 362 do Superior Tribunal de Justiça[20].

Sendo assim, a empresa, opôs embargos de declaração, sob fundamento de que a decisão foi omissa em analisar normas jurídica da Lei Geral de Proteção de Dados Pessoais. Os embargos foram acolhidos, porém, o mérito se manteve.

Nesse ínterim, a Enel, inconformada com o acórdão proferido em segunda instância, interpôs Recurso Especial, fundamentandoque o vazamento de dados não foi culpa da empresa, requerendo exclusão de responsabilidade, contudo, o Recurso, acertadamente, foi inadmitido.

Diante dessa situação, a Enel, Agravou da referida decisão e foi nesse momento que o Superior Tribunal de Justiça, em sua segunda Turma, dispôs que o dano moral não tem condão, por si só, de gerar indenização, sendo necessário, portanto, que o titular dos dados comprove eventual dano decorrente da exposição de suas informações personalíssimas.

> PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL.VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO. I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais. II - A sentença julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa. III - A tese de culpa exclusiva de terceiro não foi, em nenhum momento, abordada pelo Tribunal Estadual, mesmo após a oposição de embargos de declaração apontando a suposta omissão. Nesse contexto, incide, na hipótese, a Súmula n. 211/STJ. In casu, não há falar em pré-questionamento ficto, previsão do art. 1.025 do CPC/2015, isso porque, em conformidade com a jurisprudência do STJ, para sua incidência deve a parte ter alegado devidamente em suas razões recursais ofensa ao art. 1022 do CPC/2015, de modo a permitir sanar eventual omissão através de novo julgamento

[20]BRASIL. **Supremo Tribunal de Justiça** - Agravo REsp.: 1728093 RJ 2020/0172673-3, Relator: Ministro Raul Araújo, Data de Julgamento: 23/02/2021.T4 - QUARTA TURMA, Data de Publicação: Dje 23/02/2021. O tribunal por unanimidade, conhecer do agravo para conhecer em parte do recurso especial e, nessa parte, dar-lhe provimento,. Disponível em: https: https://www.jusbrasil.com.br/jurisprudencia/stj/1172223467. Acesso: 10 set. 2023.

> dos embargos de declaração, ou a análise da matéria tida por omissa diretamente por esta Corte. Tal não se verificou no presente feito. Precedente: AgInt no REsp 1737467/SC, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 8/6/2020, DJe 17/6/2020. IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis. V - O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações. VI - Agravo conhecido e recurso especial parcialmente conhecido e, nessa parte, provido.[21]

Durante o processo de elaboração da Lei Geral de Proteção de Dados (LGPD), o legislador optou por uma abordagem bifurcada em relação aos dados pessoais. Por um lado, são dados pessoais não sensíveis, conforme definidos pelo art. 5º, I, da Lei Geral de Proteção de Dados (LGPD)[22], que são aqueles relacionados a um indivíduo natural identificado ou identificável. Exemplos de dados pessoais não sensíveis, conforme destacado por Gediel e Côrrea[23], incluem "o nome, o endereço, o telefone e os números dos documentos de identificação."

Por outro lado, evidenciam os dados sensíveis, que, em sua maioria, apresentam maior potencialidade para causar danos aos titulares e estão enumerados no art. 5º, II, da Lei Geral de Proteção de Dados (LGPD)[24].

No entanto, com uma análise aprofundada, evidencia que dados pessoais, independente da sua natureza, podem potencialmente causar danos aos titulares e como ilustração, pode-se citar o nazismo, momento este que os alemães perseguiram judeus com base em informações encontradas, como endereços, destacando que o domicílio, visto individualmente, pode não ser considerado um dado sensível, mas o contexto pode torná-lo

---

[21]BRASIL. **Supremo Tribunal de Justiça** - Agravo REsp.: 2130619 RJ 2022/0152262-2, Relator: Ministro Francisco Falcão, Data de Julgamento: 07/03/2023.T2 - SEGUNDA TURMA, Data de Publicação: Dje 10/03/2023. O tribunal por unanimidade, conhecer do agravo para conhecer em parte do recurso especial e, nessa parte, dar-lhe provimento,. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/1780119718. Acesso: 10 set. 2023.

[22]BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Institui Lei Geral de Dados Pessoais. Disponível em: https: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 ago. 2023.

[23] GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade sitiada entre o Estado e o mercado. Revista da Faculdade de Direito UFPR, n. 47, 2008, p. 144. Disponível em: https://revistas.ufpr.br/direito/article/view/15738. Acesso em: 17 mar. 2023

[24] BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Institui Lei Geral de Dados Pessoais. Disponível em: https: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 ago. 2023.

sensível[25].

Rodotà enfatiza que a sensibilidade dos dados é determinada pelo caso concreto e deve ser analisada conforme a concretude ontológica, não possuindo um valor ontológico individualmente, mas sim em virtude do contexto em que está inserido ou das finalidades para as quais é utilizado.[26]

O julgado do Superior Tribunal de Justiça (STJ) não considerou que o caso concreto é responsável por definir a natureza jurídica de um dado pessoal como sensível, portanto, a parte afetada é encarregada do ônus probatório, seja ele moral, material, ou eventualmente estético, decorrente do vazamento de dados pessoais não sensíveis.

A discussão acerca do dano moral, concebido como uma dor subjetiva ou uma violação à dignidade, permeia o universo jurídico, tornando-se especialmente o contexto contemporâneo marcado pelos crescentes desafios relacionados à proteção de dados.

Ao explorar a teia que envolve o dano moral, surge a necessidade de compreender não apenas sua definição jurídica, mas também sua manifestação como uma afronta à esfera subjetiva do indivíduo.

Neste contexto, destaca-se a relevância dessa perspectiva subjetiva ao analisar casos de vazamentos de dados. A disseminação não autorizada de informações pessoais pode transcender a mera violação de normas legais que atinge a esfera íntima e pessoal, provocando danos que muitas vezes escapam às métricas tradicionais de reparação.

A dimensão subjetiva do dano moral, entendida como uma dor que transcende o tangível, influencia o ônus probatório para a busca de indenização em situações de vazamentos de dados. Adentraremos nas nuances dessa influência, examinando como a experiência subjetiva do titular dos dados afeta a comprovação do dano, destacando desafios e reflexões pertinentes no campo jurídico.

Carlos Roberto Gonçalves destaca de maneira precisa que “o dano moral não é propriamente a dor, a angústia, o desgosto, a aflição espiritual, a humilhação, o complexo que sofre a vítima do evento danoso, pois esses estados”[27]. Para Gonçalves, esses estados emocionais configuram, na realidade, o resultado da violação a algum interesse existencial. Essa distinção é fundamental para compreender que o dano moral não se limita às

---

[25] EPSTEIN, Eric J.; ROSEN, Filipe. **Dicionário do Holocausto: biografia, geografia e terminologia** . Bloomsbury Publishing EUA, 1997.

[26] RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2018, p. 77.

[27] GONÇALVES, Carlos Roberto. Direito Civil Brasileiro: Responsabilidade Civil. São Paulo: Saraiva, 2007, p. 359.

manifestações subjetivas, mas reside na lesão a aspectos fundamentais da vida e da dignidade do indivíduo, transcendendo a esfera emocional e alcançando a integridade de seus valores e direitos existenciais.

Ao analisar a postura adotada pelo Superior Tribunal de Justiça (STJ) no julgamento em voga, torna-se evidente que o conceito de dano moral não foi aplicado como uma violação direta a um interesse existencial. O entendimento pátrio, inclinou-se à perspectiva de que o dano moral decorrente do vazamento de dados não sensíveis, por si só, não resulta automaticamente em danos morais. Esta abordagem indica que cabe ao autor a responsabilidade de demonstrar efetivamente a ocorrência do dano.

Insta salientar, que este julgamento não se deu por meio do rito repetitivo ou outro procedimento capaz de estabelecer um precedente vinculante. No entanto, é crucial reconhecer que toda decisão judicial, mesmo quando não vinculante, assume a forma de um precedente, refletindo a posição de uma turma ou órgão em relação à matéria em questão. É importante notar que, em situações de demandas idênticas, é provável que o julgamento anterior sirva como orientação, indicando a tendência de uma decisão semelhante.

Diante de um vazamento de dados pessoais não sensíveis, a obtenção do mérito pode depender da consideração do Superior Tribunal de Justiça (STJ) sobre se o dano moral é in re ipsa ou não. Essa possibilidade, no entanto, não é assegurada, pois, como observado, o julgamento do agravo em recurso especial 2.130.619.

Não demanda grande esforço intelectual compreender que a comprovação da culpa, requisito para a configuração da responsabilidade civil, tem sido historicamente desafiadora para o autor, especialmente quando este assume a posição de consumidor.

Até os dias atuais, o consumidor, parte mais vulnerável da relação, enfrenta obstáculos significativos ao tentar evidenciar o dano moral, especialmente em situações que não se enquadram como danos in re ipsa, como a dos autos em questão.

Os dados pessoais são categorizados como sensíveis ou não pela Lei Geral de Proteção de Dados (LGPD). Entretanto, em uma realidade concreta que caracteriza uma sociedade do risco, do conhecimento, da inovação e da globalização, com conexões globais e diversas possibilidades de tratamento e emergências relacionadas a ameaças ou lesões aos titulares, torna-se imperativo superar essa bifurcação.

Nessa perspectiva, a natureza de um dado pessoal, seja sensível ou não, deve ser analisada à luz do caso concreto. Isso requer uma avaliação do titular, do contexto, do grau de lesão, do potencial risco e do conjunto de medidas para mitigar ou neutralizar quaisquer danos resultantes do tratamento; em última análise, o caso concreto deve demonstrar a natureza do

dado pessoal.

O Superior Tribunal de Justiça (STJ), no entanto, aborda os dados pessoais sob a ótica da pela Lei Geral de Proteção de Dados (LGPD) e, portanto, sustenta que o vazamento de dados pessoais, por si só, não gera danos à pessoa.

Isso marca uma mudança que se assemelha à concepção de dano moral do século XIX, em que este não é caracterizado pela lesão ao interesse jurídico da pessoa, mas sim pela lesão ao ser humano, exigindo comprovação.

Apesar disso, o consumidor pode buscar reparação por dano moral em casos de vazamento de dados pessoais. No entanto, para isso, deve empregar todos os meios de prova disponíveis, especialmente aqueles previstos legalmente, para demonstrar de maneira efetiva que algum atributo inerente à sua pessoa foi afetado, resultando em prejuízo, diminuição do bem-estar emocional, lesão na psique ou abalo emocional.

CONCLUSÃO

Em conclusão, a análise do recente julgamento do Superior Tribunal de Justiça (STJ) no Agravo em Recurso Especial de nº 2.130.619 – SP, revela uma significativa influência na discussão sobre a regulamentação de dados pessoais.

Originado de uma ação indenizatória contra a Enel Brasil S.A., o caso envolveu o vazamento de dados pessoais não sensíveis, desencadeando uma série de questionamentos sobre a natureza do dano moral e a responsabilidade das empresas em relação a isso.

A discussão em torno da natureza dos dados pessoais, se sensíveis ou não, ganha relevância no contexto da Lei Geral de Proteção de Dados (LGPD). O STJ, ao abordar os dados sob a ótica da Lei Geral de Proteção de dados (LGPD), destaca que a mera violação do sigilo não configura, por si só, dano moral. Essa posição, embora não estabeleça um precedente vinculante, oferece uma orientação que pode influenciar futuras decisões judiciais sobre casos semelhantes.

E nesse contexto, é visível que o consumidor, parte mais afetada da relação, ao buscar reparação em casos de vazamento de dados, enfrenta desafios significativos na comprovação do dano, especialmente quando não se trata de danos *in re ipsa*.

Portanto, diante dessa complexa relação entre a proteção de dados, a concepção do dano moral e a responsabilidade das empresas, o cenário jurídico contemporâneo enfrenta o desafio de equilibrar a necessidade de proteção dos titulares de dados personalíssimos com a exigência de uma prova efetiva dos danos sofridos.

A discussão sobre a regulamentação de dados pessoais segue em evolução e a Lei

Geral de Proteção de dados, continua desempenhando um papel primordial para a elaboração de uma abordagem jurídica equilibrada e adaptada aos desafios do mundo digital.

REFERÊNCIAS

AFONSO DA SILVA, *José. Curso de Direito Constitucional Positivo. 25ª ed. São Paulo: Malheiros, 2005, p. 206.*

BARROSO, Luís Roberto. Efetividade das normas constitucionais por que não uma constituição para valer? Revista de direito da Procuradoria Geral do Estado do Rio de Janeiro, n. 39, p. 27-61 1987.

BRASIL, Constituição (1988), Capítulo I – Dos Direitos Individuais e Coletivos. Art.5, X. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm Acesso em: 15 ago. 2023.

BRASIL, Constituição (1988), Emenda Constitucional nº155/2022 – 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 pessoais. Art. 5, LXXIX. Disponível em: https: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 15 ago. 2023.

BRASIL, Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: https://www.jusbrasil.com.br/topicos/10729483/artigo-21-da-lei-n-10406-de-10-de-janeiro-de-2002. Acesso em: 15 ago. 2023.

BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Institui Lei Geral de Dados Pessoais. Disponível em: https: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 ago. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Art.6. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 06 out. 2023.

BRASIL. **Supremo Tribunal de Justiça** - Agravo REsp.: 1728093 RJ 2020/0172673-3, Relator: Ministro Raul Araújo, Data de Julgamento: 23/02/2021.T4 - QUARTA TURMA, Data de Publicação: Dje 23/02/2021. O tribunal por unanimidade, conhecer do agravo para conhecer em parte do recurso especial e, nessa parte, dar-lhe provimento,. Disponível em: https: https://www.jusbrasil.com.br/jurisprudencia/stj/1172223467. Acesso: 10 set. 2023.

BRASIL. **Supremo Tribunal de Justiça** - Agravo REsp.: 2130619 RJ 2022/0152262-2, Relator: Ministro Francisco Falcão, Data de Julgamento: 07/03/2023.T2 - SEGUNDA TURMA, Data de Publicação: Dje 10/03/2023. O tribunal por unanimidade, conhecer do agravo para conhecer em parte do recurso especial e, nessa parte, dar-lhe provimento,. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/1780119718. Acesso: 10 set. 2023.

CAMUS, Albert. A Peste. 38ªed. – Rio de Janeiro: Record, 2022, p. 09.

COUTO, José Henrique de Oliveira. Vazamentos de dados e dano moral in re ipsa: comentários ao Agravo em Recurso Especial nº 2.130.619/SP. Revista IBERC, Belo Horizonte.

EPSTEIN, Eric J.; ROSEN, Filipe. **Dicionário do Holocausto: biografia, geografia e terminologia** . Bloomsbury Publishing EUA, 1997.

FERREIRA FILHO, M. G. *Curso de direito constitucional*. 33.ed. rev. e atual. São Paulo: Saraiva, 2007. p. 296.

GAUCHAZH. Vazamento de dados do Facebook atinge 443 mil usuários no Brasil. Disponível em: https://gauchazh.clicrbs.com.br/mundo/noticia/2018/04/vazamento-de-dados-do-facebook-atinge-443-mil-usuarios-no-brasil-cjfmg3kqh06de01phlwlsy4be.html. Acesso em: 15 out. 2023.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade sitiada entre o Estado e o mercado. Revista da Faculdade de Direito UFPR, n. 47, 2008, p. 144. Disponível em: https://revistas.ufpr.br/direito/article/view/15738. Acesso em: 17 mar. 2023

GONÇALVES, Carlos Roberto. Direito Civil Brasileiro: Responsabilidade Civil. São Paulo: Saraiva, 2007, p. 359.

GONÇALVES, Maria Eduarda. Direito da Informação: novos desafios e formas de regulação na sociedade da informação. Coimbra: Almedina, 2003.

LESLIE, Fair.FTC impõe multa de US$ 5 bilhões e novas restrições de privacidade no Facebook. Disponível em: https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook. Acesso em: 10 nov.2023.

MATEUCCI, C. R. F. *Privacidade e internet. Revista de Direito Privado*, São Paulo, ano 5, p.46-55, jul.-set. 2004.

NETO, Nelson Novaes et al. Desenvolvimento de um banco de dados global sobre violação de dados e os desafios encontrados. **Revista de Qualidade de Dados e Informação (JDIQ)**, v. 1, pág. 1-33, 2021.

NISSENBAUM, Helen. Privacidad amenazada. Tecnología, política y la integridade de la vida social. México:Oceano, 2010, p. 21.

PEREIRA, J. Matos. Direito de informação. Dicionário de História de Portugal, v. 7, p. 15, 1980.

RAMOS, André de Carvalho. Curso de Direitos Humanos – 8ª ed. – São Paulo: Saraiva Educação, 2021, p. 60.

RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2018, p. 77.

VIDAL, Gabriel Rigoldi. Conceituação do direito à privacidade em face das novas tecnologias. **Orientador: Professora Doutora Riva Sobrado de Freitas**, 2014.