



QUALIS
A2



A RESPONSABILIZAÇÃO CIVIL DAS PLATAFORMAS DIGITAIS POR DANOS PRATICADOS POR USUÁRIOS¹

THE CIVIL LIABILITY OF DIGITAL PLATFORMS FOR DAMAGES CAUSED BY USERS

Robson Júnior Fernandes RODRIGUES

Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)

E-mail: denafl155@gmail.com

ORCID: <http://orcid.org/0009-0002-8297-314X>

Arthur Artiaga MALUF

Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)

E-mail: arthuratiagam@gmail.com

ORCID: <http://orcid.org/0009-0006-9010-6109>

73

RESUMO

O presente artigo analisa a responsabilização civil das plataformas digitais por danos decorrentes do tratamento inadequado de dados pessoais e de condutas praticadas por usuários no ambiente digital, à luz da Constituição Federal de 1988, da Lei Geral de Proteção de Dados Pessoais — LGPD, do Marco Civil da Internet e das diretrizes da Autoridade Nacional de Proteção de Dados — ANPD. A pesquisa adota metodologia bibliográfica, explicativa e dedutiva, com exame da evolução legislativa da proteção de dados no Brasil, desde os debates iniciais do anteprojeto da LGPD até a consolidação da proteção de dados pessoais como direito fundamental pela Emenda Constitucional nº 115/2022. O estudo demonstra que o tratamento de dados pessoais envolve agentes específicos, como titular, controlador, operador e encarregado, bem como etapas próprias, como coleta, retenção, processamento, compartilhamento e eliminação. A partir dessa estrutura, discute-se o regime de responsabilidade civil previsto na LGPD, especialmente nos artigos 42 e 43, evidenciando que a responsabilização dos agentes de tratamento não se limita à lógica objetiva tradicional, mas exige análise da conduta, do dano, do nexo causal, da violação à legislação e da adoção ou não de medidas de segurança, prevenção e governança. Conclui-se que a responsabilidade civil das plataformas digitais deve ser compreendida como instrumento de tutela dos direitos fundamentais, de equilíbrio das relações digitais e de proteção da dignidade da pessoa humana na sociedade

¹ COMO CITAR: (ABNT): RODRIGUES, R. J. F.; MALUF, A. A. A Responsabilização Civil das Plataformas Digitais por Danos Praticados por Usuários. **JNT Facit Business and Technology Journal**. Qualis A2. ISSN: 2526-4281, Mês de Junho de 2026 - Ed. 75. VOL. 01. Págs. 73-88. Disponível: <http://revistas.faculdadefacit.edu.br>. Acesso em: __/__/__.

informacional e da seguridade das relações de mercado com fins para proteção da equidade e manutenção do bem-estar, haja vista que os dados pessoais é um ativo importante que deve ter sua proteção e responsabilização adequadas.

Palavras-chave: Responsabilidade civil. Plataformas digitais. Proteção de dados. LGPD. Danos digitais. ANPD.

ABSTRACT

This article analyzes the civil liability of digital platforms for damages arising from the improper processing of personal data and from harmful conduct carried out by users in digital environments, based on the Brazilian Federal Constitution of 1988, the General Personal Data Protection Law — LGPD, the Brazilian Civil Rights Framework for the Internet, and the guidelines issued by the National Data Protection Authority — ANPD. The research adopts a bibliographic, explanatory, and deductive methodology, examining the legislative evolution of personal data protection in Brazil, from the preliminary debates surrounding the LGPD draft bill to the recognition of personal data protection as a fundamental right through Constitutional Amendment No. 115/2022. The study demonstrates that personal data processing involves specific agents, such as the data subject, controller, processor, and data protection officer, as well as distinct stages, including collection, retention, processing, sharing, and deletion. Based on this structure, the article discusses the civil liability regime established by the LGPD, especially Articles 42 and 43, highlighting that the liability of data processing agents cannot be understood solely through a traditional strict liability approach, but rather requires an assessment of conduct, damage, causal link, violation of data protection legislation, and the adoption or omission of security, prevention, and governance measures. It is concluded that the civil liability of digital platforms must be understood as a legal mechanism for safeguarding fundamental rights, balancing digital relations, and protecting human dignity in the information society.

Keywords: Civil liability. Digital platforms. Data protection. LGPD. Digital damages. ANPD.

INTRODUÇÃO

Em decorrência das constantes mudanças na sociedade, é necessário a intervenção do Direito para dirimir melhor as relações sociais em todas as esferas.

Por oportuno, os meios digitais, promoveram uma mudança significativa na estrutura societária, e a proteção dos direitos das relações derivadas dos meios digitais é essencial para manutenção e promoção do Estado democrático de Direito nas esferas nacional e internacional. Posto que, as novas fronteiras se alargaram, e os limites supranacionais se flexibilizaram. Nesse sentido, trataremos sob âmbito brasileiro, a responsabilização civil das plataformas digitais por danos praticados por usuários, perpassando pelo entendimento da aplicação da Lei Geral de Proteção de Dados (LGPD) e legislações conexas na construção das tratativas governamentais para consolidação dos direitos e garantias fundamentais abarcados pela Constituição vigente. Veja que a referida lei retromencionada entrou em vigor em agosto de 2020 no Brasil, com significativas alterações nas regras de tratamentos pessoais de dados dentro das plataformas digitais. Não obstante, as empresas que faziam a coleta de dados pessoais tiveram que se adaptar e cumprir as determinações da LGPD, utilizando-se das bases legais que justifiquem não somente a coleta, mas também o tratamento desses dados. Dessa forma as plataformas digitais devem seguir o regramento da Lei Geral de Proteção de Dados, para uso desse novo meio de tratativas sociais e individuais que é o meio digital.

Em breve esboço histórico, foi promulgado a Emenda Constitucional 115/2022, na qual fez da proteção de dados pessoais partícipe do rol de direitos e garantias fundamentais do Artigo 5º da Constituição Federal. Assim, tal proteção como garantia constitucional traz em seu bojo uma responsabilização para aqueles que usurpam do poder frente a manutenção dos dados pessoais sejam pessoais físicas ou jurídicas, pois devem ser garantidos tais direitos para promoção da dignidade da pessoa humana e a proteção do cidadão.

O artigo está dividido em 4 partes, **a primeira parte** se trata do histórico legislativo das proteções digitais no Brasil, discussão do anteprojeto da Lei e a participação de integrantes da sociedade civil naquela que veio a se tornar a Lei Geral de Proteção de Dados, **a segunda parte** trataremos acerca de alguns termos e limites do usuário e das regulamentações da LGPD para compreensão de todo quadro em que se dá a adequação dos usuários dentro da legislação brasileira vigente, a terceira parte trataremos acerca do conceito de responsabilização tanto dentro do âmbito civil e abordagens dela decorrentes dentro das plataformas digitais, Por fim, passaremos as considerações finais, acerca de todo o tema desenvolvido e as como a sociedade se comportará dentro da adequação legal dos casos em concreto e a forma como a responsabilização pode ser entendida.

DESENVOLVIMENTO

Metodologia

O presente artigo aborda acerca Responsabilização Civil das Plataformas Digitais por Danos Causados aos usuários.

Para atingir esse objetivo, realizou-se uma revisão bibliográfica, com a coleta de informações em artigos científicos e sítios disponíveis na rede mundial de computadores.

Nessa senda, insta relatar que para Cervo e Bervian (2002) a pesquisa bibliográfica procura explicitar um problema utilizando como base referências teóricas publicadas em documento.

Assim quando, analisando a proteção de dados pessoais, as determinações legislativas e tratativas acerca dos usuários, adotou-se a pesquisa explicativa, por meio da exposição de pensamentos acerca da temática.

Por fim, para que a pesquisa se tornasse mais técnica, o método dedutivo se fez presente, haja vista que na ótica de Cervo e Bervian (2002) a explanação de verdades particulares contidas em verdades universais, perpassa uma argumentação lógica em estruturas lógicas, por meio de relacionamento entre antecedente e consequente, entre hipótese e tese, entre premissa e conclusões, com o fito de ressaltar o surgimento de normas que prevejam a responsabilização civil das plataformas digitais por danos causados aos usuários.

Discussão sobre a Proteção de Dados no Brasil

No Brasil, há muito se discutiu sobre o anteprojeto de lei de proteção de dados pessoais resultantes de uma parceria do Ministério da Justiça com o Observatório Brasileiro de Políticas Digitais da Fundação Getúlio Vargas do Rio de Janeiro FGV (2011). Veja que outras nações da América do Sul já tinham um histórico breve acerca da normativas ainda que primitivas referente a temática consoante aponta Angarita Remolina (2014), por exemplo, a Argentina em seu Artigo 43, da Constituição de 1994, cria em 2000 a Lei 25.326 que traz em seu bojo lampejos de proteção aos dados pessoais, bem como a Colômbia em seu Artigo 15 da Constituição de 1991, trouxe na Lei 1581/2012 assunto importante acerca da mesma temática da lei Argentina.

Diante desse quadro na qual a evidência global do uso de tecnologia na qual não necessariamente possui barreiras, ao menos até definir os contornos desse meandro digital, é evidente que as relações ficam a mercê de serem violadas,

conquanto outros países já tinham ao menos um resquício de jurisdição dentro de seus direitos fundamentais, vale acrescentar que:

Sozinha, a tecnologia não dá conta de imunizar cidadãos contra violações e abusos. Novos mecanismos para burlar eventuais barreiras tecnológicas sempre podem ser criados. É nesse sentido que o uso da tecnologia deve se aliar ao direito nacional ou internacional. Limites devem impor não só deveres aos Estados - como o respeito à vida privada, mas também assegurar ao cidadão mecanismos de controle sobre suas informações pessoais. Democracias devem usar o direito como ferramenta de regulação, servindo de escudo para a tutela do direito à privacidade em detrimento de modelos de negócio que possibilitem o acúmulo desse enorme volume de dados pessoais (...). A possibilidade de formação desses bancos de dados expõe o usuário às mesmas lentes nefastas da “teletela orwelliana”. O fato é que os modelos de negócio que imperam na rede hoje propiciam campo livre para a vigilância governamental. Deixar de regulamentar a coleta de dados (privadas e estatais) por meio da criação de barreiras tecnológicas ou jurídicas é negar uma ferramenta preciosa à autonomia do indivíduo e à sociedade democrática (Antonialli & Brito Cruz, 2013, p. 19).

É essencial encontrar um equilíbrio entre o uso responsável dos dados e a proteção dos direitos e privacidade dos indivíduos para garantir que essas mudanças não resultem em injustiças ou exclusões indevidas. Nesse sentido, nos explicam Bioni e Dias

A Lei Geral de Proteção de Dados (LGPD-Lei n.13.709/2018), estabeleceu, pela primeira vez no ordenamento jurídico brasileiro, um conjunto de normas – regras e princípios – vocacionados a regular o tratamento de dados pessoais em todas as atividades do cotidiano do cidadão, abarcando, assim, todos os setores da economia. O impacto desse tipo de reconfiguração do sistema jurídico tem sido comparado à repactuação do próprio contrato social. Afinal, atualmente, as pessoas são julgadas e avaliadas com base no que seus dados pessoais dizem em todos os âmbitos da sua vida. Do acesso a programa de transferência de renda ao de linha de crédito, essas oportunidades sociais são filtradas pelo processamento de seus dados (Zanatta, 2019, p. 11 *apud* Bioni; Dias, 2020, p. 2)

Ponto que merece destaque é o Comitê Gestor da Internet que já discutira antes do anteprojeto de lei, temas sobre a tutela do cidadão frente aos seus dados pessoais. Na esteira desse raciocínio, cumpre o relatado por Danilo Doneda, acerca dos debates travados no Mercosul em 2005, na qual tempos depois resultou na elaboração de um documento denominado “ Medidas para proteção de dados pessoais e sua livre circulação”, documento inclusive que teve aceite dos países-membros do Mercosul no ano de 2010. Em decorrência dessas tratativas, o Ministério da Justiça no mesmo ano da ratificação, promoveu um debate público para contribuir com a elaboração de um projeto de lei destinado a discussão sobre o tratamento de dados pessoais no Brasil. Veja que o Ministério da Justiça teve participação para que a temática fosse considerada relevante dado o impacto na defesa de direitos pessoais.

Nesse ínterim, foi realizada outra audiência pública, e assim, consolidada a versão final do anteprojeto, que foi protocolado no Congresso Nacional em 13 de Maio de 2016, com a participação do Ministério da Justiça e do Ministério de Planejamento na PL 5.276/2016.

O tema começa a ganhar repercussão em outras esferas, antes da plena discussão do referido projeto, vejamos o disposto na Câmara dos Deputados a propositura da PL 4.060/2012, do Deputado Milton Monti, que acabou apensado ao PL de 5.276 sob relatoria de Orlando Silva. Após diversos embates e audiências públicas acerca da temática o PL apensado foi aprovado em 29 de Maio de 2018 e encaminhado ao Senado Federal sob a identificação de PLC 53/2018.

No âmbito do Senado Federal, já tinham sido proposto ao menos outros projetos de lei com a mesma temática, à título de exemplo, constam o PLS 330/2013, PLS 131/2014 e PLS 181/2014. Devido a reincidência do assunto na casa legislativa as iniciativas passaram a tramitar em conjunto sob a relatoria do senador Aloysio Nunes Ferreira com a PL 53/2018 com a referência para os devidos tratamentos. Em sequência, o projeto recebera aprovação do Plenário da casa em 5 de Julho de 2018, quando então após a sanção presidencial, transformou na Lei nº 13.709 (Lei Geral de Proteção de Dados).

Veja que a participação de integrantes da sociedade civil, foi importante, para a confecção da redação da referida lei, como o destacado na publicação do “ Manifesto sobre a Futura Lei de Proteção de Dados”, assinado por diversas associações como a Associação Brasileira de Marketing Direto (ABEMO); Associação Brasileira de Empresas de Software (ABES); Associação Brasileira de Internet (ABRANET); Associação Nacional de Dados de Crédito (ANBC); Associação das Empresas Brasileiras de Tecnologia da Informação (ASSESPRO) e a Associação das Empresas de Tecnologia da Informação e Comunicação e de Tecnologias Digitais (BRASSCOM) ligadas a empresas do setor de tecnologia. A redação do documento, em tópico próprio cita a questão da responsabilidade civil, na qual as entidades solicitam à imputação da obrigação da reparação pelos danos causados uma apuração individualizada, pois acham um entrave a responsabilidade solidária e objetiva. Nesse sentido, caso houvesse uma responsabilização objetiva e solidária esses órgãos gestores, poderiam acabar sendo penalizados por terem que manusear ainda que de forma indireta os dados dos usuários. Essa discussão dessas associações é importante para poder infirmar o modo como a responsabilização ficou quando da vigência da Lei Geral de Proteção de Dados.

Definições Legais sobre os Agentes de Tratamento e o Ciclo dos Dados

Insta relatar alguns esclarecimentos sobre os termos que devemos utilizar ao longo do artigo, em conformidade com as normas vigentes no Brasil, quais sejam Lei 13.709/2018 (LGPD), a Lei de Acesso à Informação (Lei nº 12.527/2011) e a Política Nacional de Arquivos Públicos e Privados (Lei nº 8.159/91) e que estão bem esculpidos no Guia de Boas Práticas da Lei Geral de Proteção de Dados. Quanto ao agentes de tratamento de dados, temos:

1. **Titular:** pessoa natural a quem os dados pessoais se referem. Pode ser criança, adolescente, adulto ou idoso.
2. **Controlador:** pessoa natural ou jurídica, de direito público ou privado, responsável por decisões referentes ao tratamento de dados pessoais como: a aplicação de hipótese legal⁷, a finalidade e a conduta do tratamento de dados pessoais. Conforme a lei, pode executar o tratamento ou designar responsável(is) para a sua realização.
3. **Operador:** pessoa natural ou jurídica de direito público ou privado, ou pessoa física que realiza o tratamento de dados pessoais em nome do controlador.
4. **Encarregador:** pessoa natural indicada pelo controlador ou operador para atuar como moderador entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Também possui, como uma de suas atividades, orientar os funcionários e os contratados do controlador a respeito das práticas relativas à proteção de dados pessoais.

Nesse sentido, passaremos a referendar como o controlador dos dados que é o responsável pela manutenção dos dados deve cumprir com essa gestão dos dados, a qualquer tempo mediante a solicitação de:

- I. Confirmação da existência de tratamento;
- II. Acesso aos dados;
- III. Correção de dados incompletos, inexatos ou desatualizados;
- IV. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta lei;
- V. Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante a requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853/2019)
- VI. Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

- VII. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- VIII. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- IX. Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei (Brasil, 2018, Art.18)

Posto as informações dos agentes e o campo atuarial que devem aqueles realizar dentro da legislação atinente para configuração de uma responsabilização civil que será tratada em tópico próprio, é salutar a importância de que o tratamento dos dados tem um ciclo de vida, porquanto, a utilização dos dados tem um determinado objetivo a ser cumprido e não pode ficar os dados a mercê de uma captação indevida. Conforme consta no Guia de Boas Práticas cada fase do ciclo de vida tem correspondência com operações de tratamento definições na LGPD. Vejamos as seguintes fases:

1. **Coleta** - obtenção, recepção ou produção de dados pessoais independente do meio utilizado.
2. **Retenção** - arquivamento ou armazenamento de dados pessoais independente do meio utilizado
3. **Processamento** - qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.
4. **Compartilhamento** - qualquer operação que envolva transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais.
5. **Eliminação** - qualquer operação que visa apagar ou eliminar dados pessoais (Brasil, 2020, p. 45).

Assim, decorridos os aspectos mais fundamentais acerca da temática, podemos nos aprofundar no quesito de como explicar da melhor forma a gestão dos dados pessoais. Veja que o titular dos dados pessoais, pode ser qualquer pessoa, de qualquer local, uma vez que se está pautado como indivíduo, esse merece proteção quanto as suas próprias informações. Ainda que tal persona, não saiba do que se trate, o acesso as plataformas digitais promovem a circulação dos seus dados e nesse ponto que se discute quem deva ser o possível responsável.

Os termos de consentimento, disponibilizados pelos sites, aplicativos e programas, tem a sua importância para a manutenção dos dados conforme a Agência Reguladora no Brasil, no caso a ANPD que dita as diretrizes em como as empresas

publicitárias, marketing e de tráfego podem se valer dentro do regimento legal das informações que são obtidas. Vejamos que se um titular de dados, não autoriza o acesso a determinada informação pessoal sua e posteriormente essa informação acaba sendo vazada, quem teria de fato a responsabilidade, o veículo que divulgou a informação, a gestora dos dados que fornecera a informação para outro veículo de comunicação, ou ao segurança do sistema informacional na defesa e manutenção da proteção ao site violado.

Nesse ínterim, os dados pessoais podem ser classificados em 3 categorias dentro da normativa brasileira, quais sejam: dados pessoais, sensíveis e anonimizados. A primeira categoria são informações relacionadas a pessoa natural identificada ou identificável, comumente se encontra o nome, profissão, CPF, endereço, telefone, são dados basicamente identificatórios. Na segunda categoria, os dados pessoais sensíveis são aqueles de cunho discriminatório, como origem racial ou étnica, de convicção religiosa, filiação a sindicato, dado referente à saúde ou vida sexual, dado genético ou biométrico. Na última e terceira categoria, os dados anonimizados envolvem informações sobre o titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento.

Ponto importante, ressalvado no artigo 4º da Lei Geral de Proteção de Dados é que a normativa não se aplica ao tratamento de dados realizados por pessoa natural com fins exclusivamente particulares e sem finalidade econômica, por oportuno, estão excluídos também os dados que possuem finalidade exclusivamente jornalísticas, artísticas e acadêmicas. Essa aparente distinção é necessário para não coibir a atuação dessas profissões e nem a liberdade dada aos indivíduos pela Carta Magna. O que se busca, na verdade é a regulação adequada do mercado, com a liberdade fundamental resguardada e exercida em respeito a imagem e proteção garantidas constitucionalmente e internacionalmente, pois a gestão dos dados tem barreiras que superam as físicas e a instantaneidade.

Nesse sentido, não é tão simples definir se o controlador dos dados se valha de toda a culpa do usuário, sendo que existem etapas definidas pela ANPD, conforme exposto acima. Cada gestão de dados pode ser responsabilizada ou contratada para realizar uma etapa no tratamento de dados, e definir em qual etapa houve a determinada violação dentro da fase de tratamento dos dados é essencial para definir quem de fato é o responsável pela violação.

Assim, para que se possa atingir o corolário fundante da lei as situações mais corriqueiras em que a lei deve atuar são referentes ao compartilhamento de dados de

clientes com: terceiros, fornecedores e indústria, representantes comerciais, empresas e-commerce, fornecedores de serviços, empresas de cobrança, transportadoras, dados de cobrança de sistemas bancários, compra e situação financeira de clientes com os órgãos de proteção ao crédito, prestadores de serviços de cobrança, empresas que desenvolvem software, dados de monitoramento de câmera, informações de convênios médicos, cartão de benefícios, convênios em farmácias e lojas, postos de gasolina, supermercados

Vale ressaltar algumas operações de marketing em que a LGPD deverá atuar com maior frequência: envio de e-mail marketing para eleição; envio de folders promocionais/eleitorais; plataforma de envio de email marketing. Não obstante o compartilhamento de informações da empresa e de clientes e colaboradores por Whatsapp ou canais de comunicação externos à empresa. Como se pode deduzir dos casos apresentados, qualquer meio informacional que gere vantagem competitiva de empresas com fins lucrativos sofrerá a intervenção da LGPD para regular a circulação de informação, pois se tem os dados para direcionar toda a estrutura comercial e logística tal informação pode prejudicar sumariamente, não somente o titular de dados, mas as outras empresas concorrentes e afetar o mercado de tal maneira que pode desencadear desequilíbrios que afetam toda a sociedade.

Dessa forma, os fundamentos jurídicos da proteção de dados no Brasil, alicerçados, principalmente, na Constituição Federal de 1988, no Marco Civil da Internet e na Lei Geral de Proteção de Dados (LGPD), estabelecem uma base normativa robusta na garantia do direito à proteção de dados pessoais. Contudo, para que tais direitos sejam efetivamente garantidos, é essencial analisar como o ordenamento jurídico brasileiro estrutura a responsabilidade civil aplicável em casos de violação à Lei Geral de Proteção de Dados (Batistela,2026).

Responsabilidade Civil na Proteção de Dados Pessoais

Insta relatar que é o modelo de responsabilização civil desde a edição do anteprojeto da Lei Geral de Proteção de Dados teve nuances importantes que devem ser consideradas para podermos enquadrar, para fins teóricos quais são os limites atinentes, quanto a responsabilidade do agente que realiza a manutenção dos dados pessoais.

Na primeira versão do anteprojeto da lei geral de proteção de dados pessoais adotou-se a ideia de uma responsabilidade objetiva, e ainda assim quanto da proposta legislativa do Senado Federal houve a continuidade dessa mesma teoria acerca da

responsabilidade objetiva na qual haveria a responderiam, “independentemente da existência de culpa”, pela reparação dos danos.

Ocorre que durante a Comissão Especial PL 4060/12, houve discussão na Câmara acerca de uma responsabilidade objetiva e solidária, fundando-se nas tratativas com as demais fontes legislativas existentes no Brasil, na vulnerabilidade dos consumidores, bem como a segurança jurídica e a confiabilidade dos usuários. Em contraponto, a segunda versão do anteprojeto de lei teve mais força quanto a opção por um regime de responsabilidade subjetiva, veja que as críticas ao modelo foram criticadas diante da consulta pública, sendo a segunda opção, no caso a responsabilidade subjetiva a escolha dominante no Congresso Nacional.

Abaixo traremos uma relação dos textos legais para comparativo para elucidação do caso em comento. Na 1ª versão do anteprojeto o artigo 6º assim tratava:

O tratamento de dados pessoais é atividade de risco e todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a ressarcir-lo, nos termos da lei (Brasil, 2018, artigo 6º)

A redação do artigo torna evidente a responsabilização civil objetiva, haja vista o cumprimento legal dos requisitos, semelhante ao que se encontra no Código de Defesa do Consumidor. Nesse ínterim, a 2ª versão do anteprojeto no artigo 31 traz em seu bojo:

“O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa.” Deste feito, não há que se falar necessariamente em objetividade, mas já se começa a colocar o elemento da culpabilidade pelo menos em discussão, o que se abrangiu o tema. Ao colocar esse ponto da culpabilidade, inicia-se a discussão dos casos de excludente da culpabilidade, pois, nem sempre em todos os casos haverá a intenção dolosa de lesão aos dados pessoais, sejam pelo controlador ou pelo operador de dados pessoais.

Na esteira desse raciocínio, o PLC 53/2018, em sua redação no artigo 42 e incisos já demonstra uma evolução e uma delimitação maior quanto a tema da responsabilidade, além de mais tecnicidade ao se referir aos agentes de dados pessoais. Vejamos:

Art. 42. O responsável ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I – o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de

dados ou quando não tiver seguido as instruções lícitas do responsável, hipótese em que o operador equipara-se a responsável, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II – os responsáveis que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto no Título III da Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso. (Brasil, 2018, art.42)

Vemos nesse ponto que não somente o operador de dados pessoais, mas os responsáveis envolvidos diretamente responderam solidariamente, respeitados a exclusão dos casos previstos em lei, e as provas poderão ter os ônus invertidos a favor do titular quando a prova for excessiva onerosa, abarcando os casos em que temos a hipossuficiência de provas, pois quem possui poucos recursos de gestão dos dados, não deverá ter essa incumbência de comprovar os reais danos e também estabelece o direito de regresso dentro da cadeia da responsabilização tanto da gestão dos dados quanto do armazenamento.

Diante do caso em questão o texto da LGPD a única diferença foi a alteração do termo responsáveis para controladores no inciso II, do §1º do artigo 42. O termo “responsáveis” é genérico, conquanto o controlador é um termo mais delimitado e que tem definição própria dentro da interpretação legislativa da LGPD, o que facilita a identificação do agente na responsabilização civil, ainda que de forma solidária, em tese.

Então, se vê que a responsabilidade civil não é um espelho do CDC, pois no artigo 43, inciso II da LGPD, que a responsabilização dos agentes de tratamento de dados caso comprovem que tenha realizado toda a diligência necessária em seu campo atuarial é eximida e não haverá a violação à legislação de proteção de dados. Em suma, só será responsabilizado se não tiver tomado todas as medidas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação.

Assim, esse ponto da lei, praticamente mitiga a responsabilização civil objetiva. Para manutenção da comprovação da forma como os agentes de tratamentos de dados realizam suas atividades, houve instrumento para facilitar as boas práticas do uso desses dados, quais sejam, os relatórios de impacto à proteção de dados pessoais que funcionam como meio de alerta para os referidos uso de dados e se tomadas todas

as medidas pelos agentes de tratamento, esse instrumento pode evitar a responsabilização, haja vista ter sido demonstrado o risco desses dados, o artigo 55-J da LGPD cria um órgão gestor para recepcionar esses relatórios e a forma dele ser conduzido, vejamos:

Art. 55-J. Compete à ANPD: [...] XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; [...] § 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório (Brasil, 2018, art. 55-J).

Logo, a responsabilidade civil que soubesse ser objetiva passa pelas regras adotadas pela ANPD - Agência Nacional de Proteção de Dados. Uma vez que a responsabilização só será de fato concretizada se não forem adotadas todas as medidas pelos agentes de tratamento de dados pessoais.

O relatório de impacto e a manutenção constante dos dados e a adequação das normas da ANPD por meio da edição de regulamentos e seus procedimentos tornam dinâmica a responsabilização civil, pois no meio digital, a circulação de informações é elevada, e a fluidez dessas informações, necessita de uma legislação que não seja estanque, e que se adapte de forma segura para melhor proteção dos usuários. Deste feito, a responsabilização subjetiva se adequa as constantes mudanças, ainda mais com um órgão regulador que tem flexibilidade e autonomia na edição de regulamentos referentes a proteção de dados pessoais. A responsabilização objetiva, recaindo sempre para o gestor dos dados, nos moldes do CDC, foge o escopo da proteção da relevância dos dados pessoais, afinal, apesar de se usar os dados pessoais como algo mercantilizado, alguns dados são sensíveis e é necessária uma maior proteção, pois tratam-se de direitos personalíssimos resguardados pela Constituição.

Para elucidar a questão dessa modalidade de responsabilidade civil, temos que entender que o tratamento de dados é atividade de risco (Bodin,2019), e a gestão dos dados pelo controlador é fundamental no quesito para comprovar a responsabilização diante do dano apresentado, por oportuno, consta que algum incidente dessa natureza há um volume muito grande de dados a ser exposto para quantificação de qualquer fronteira. Pois, o alcance a que se destina no âmbito da internet é ilimitado, pode ser todo o globo, bem como informações sem precedentes para análise de um banco de dados. Tal medida de proteção dos dados sensíveis é essencial para proteção não só do titular de dados como para a proteção do próprio mercado, o poder lesivo do tratamento de dados fora discutido no Brasil na ADI 6387 e 6388 em decorrência da Medida Provisória nº 954/2018.

Assim, tal atividade de coleta necessita da percepção de vulnerabilidade de todos os usuários, para configuração de uma maior isonomia no tratamento de informações que podem desbalancear todo o sistema, qualquer que seja, financeiro, mercadológico, estatístico.

Conquanto, a fluidez das sociedades que tem que se conectado com mais frequência torna o titular de dados um sujeito cada vez mais dinâmico, pois ao participar dessa gestão, tende-se a moldar a um padrão que se altera constantemente as mudanças do mercado e dos governos e a proteção de todos os usuários é corolário dos princípios humanitários ainda que o sujeito da guarda não tenha nem ideia de que se discute em âmbito global à proteção de dados pessoais, haja vista todo potencial que qualquer usuário possa ter de acessibilidade a informação em qualquer lugar do globo e assim aquele que era inerte ao saber da manutenção de dados, pode usar de informações em caso de não proteção para objetivos escusos aos insculpidos na legislação nacional e internacional de maneira célere. Então, quando se versa sobre a responsabilização, não é apenas sobre o Direito em si, mas a garantia da isonomia entre os pares, na harmonização das relações sociais e o equilíbrio entre os poderes para a devida aplicação da legislação em cada sociedade.

CONSIDERAÇÕES FINAIS

A responsabilização civil das plataformas digitais por danos praticados por usuários revela-se tema de elevada relevância jurídica, social e econômica, especialmente diante da centralidade dos dados pessoais nas relações contemporâneas. A expansão dos meios digitais alterou profundamente a forma como indivíduos, empresas e instituições se relacionam, tornando indispensável a atuação do Direito para estabelecer limites, deveres e mecanismos efetivos de proteção aos titulares de dados.

O estudo demonstrou que a proteção de dados pessoais no Brasil passou por um processo de amadurecimento legislativo, influenciado por debates nacionais e internacionais, pela participação da sociedade civil, pelo desenvolvimento tecnológico e pela necessidade de tutela da privacidade, da intimidade, da liberdade e da dignidade da pessoa humana. A promulgação da Lei Geral de Proteção de Dados e, posteriormente, a inclusão da proteção de dados pessoais no rol de direitos fundamentais pela Emenda Constitucional nº 115/2022 consolidaram um novo paradigma normativo, no qual os dados pessoais deixam de ser tratados apenas como insumo econômico e passam a ser compreendidos como extensão da própria personalidade do indivíduo.

Verificou-se, ainda, que a LGPD estruturou um sistema próprio de governança e responsabilização, delimitando os papéis do titular, controlador, operador e encarregado, bem como estabelecendo deveres relacionados à coleta, retenção, processamento, compartilhamento e eliminação dos dados. Essa organização normativa permite identificar com maior precisão a atuação de cada agente no ciclo de vida dos dados pessoais, evitando responsabilizações genéricas e exigindo análise concreta da conduta praticada, da etapa em que ocorreu a falha e da extensão do dano causado.

No campo da responsabilidade civil, constatou-se que a LGPD não reproduz integralmente o modelo clássico de responsabilidade objetiva previsto em outras legislações, como o Código de Defesa do Consumidor. Embora reconheça a vulnerabilidade do titular e admita mecanismos como solidariedade entre agentes e inversão do ônus da prova, a lei também prevê hipóteses de exclusão de responsabilidade quando demonstrado que o agente não realizou o tratamento de dados, que não houve violação à legislação ou que o dano decorreu de culpa exclusiva do titular ou de terceiro. Dessa forma, a responsabilização civil no âmbito da proteção de dados assume feição técnica, dinâmica e proativa, exigindo não apenas a reparação posterior do dano, mas também a adoção prévia de medidas de segurança, prevenção, transparência e conformidade regulatória.

Nesse contexto, a atuação da ANPD assume papel essencial, pois a autoridade reguladora orienta, fiscaliza e estabelece parâmetros para a proteção de dados pessoais, especialmente nos casos de tratamento de alto risco. Instrumentos como relatórios de impacto, políticas internas de governança, mecanismos de segurança da informação e boas práticas empresariais tornam-se fundamentais para avaliar a diligência dos agentes de tratamento e para definir a eventual responsabilidade civil das plataformas digitais.

Conclui-se, portanto, que a responsabilização civil das plataformas digitais deve ser interpretada como mecanismo de equilíbrio entre inovação tecnológica, livre iniciativa, segurança jurídica e proteção dos direitos fundamentais. A sociedade digital exige plataformas mais responsáveis, transparentes e preventivas, capazes de assegurar que o tratamento de dados pessoais seja realizado de forma legítima, proporcional e segura. Assim, a reparação de danos no ambiente digital não representa apenas resposta individual a uma lesão, mas instrumento de preservação da confiança, da democracia informacional e da dignidade humana nas relações mediadas pela tecnologia.

REFERÊNCIAS

- ANGARITA REMOLINA, Nelson. **Latin America and Protection of Personal Data: Facts and Figures (1985-2014)**. University of Los Andes Working Paper, 2014. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412091. Acesso em: 23 jun. 2026.
- ANTONIALLI, Dennys; BRITO CRUZ, Francisco. Por que a privacidade importa. **O Estado de S. Paulo**, São Paulo, 16 jun. 2013, página 19.
- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Perguntas frequentes**. Brasília, DF, 2021. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/201105-faq-anpd-finalrev.pdf>. Acesso em: 18 abr. 2026.
- BATISTELLA, A. R.; ARAÚJO, J. D. A responsabilidade civil pelo vazamento de dados nas plataformas digitais. **Revista Rede de Direito Digital, Intelectual & Sociedade**, [s. l.], v. 5, n. 10, p. 213-238, 2026. DOI: <https://doi.org/10.5380/rrddis.v5i10101030>.
- BIONI, B.; DIAS, D. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, Rio de Janeiro, v. 9, n. 3, 2020.
- BODIN DE MORAES, Maria Celina. LGPD: um novo regime de responsabilização civil dito “proativo”. **Civilistica.com**, Rio de Janeiro, a. 8, n. 3, 2019.
- 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 (Marco Civil da Internet). **Diário Oficial da União**: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 mar. 2026.
- BRASIL. Ministério da Economia. Comitê Central de Governança de Dados. **Lei Geral de Proteção de Dados (LGPD): Guia de Boas Práticas para Implementação na Administração Pública Federal**. Brasília, DF, 2020.
- CERVO, A. L.; BERVIAN, P. A. **Metodologia**. São Paulo: Prentice Hall, 2002.
- DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo et al. (org.). **Tratado de proteção de dados pessoais**. 1. ed. Rio de Janeiro: Forense, 2021. p. 3-20.
- FUNDAÇÃO GETULIO VARGAS (FGV-CTS). **Relatório de políticas de internet: Brasil 2011**. São Paulo: Comitê Gestor da Internet no Brasil, 2012.
- ZANATTA, Rafael A. F. **Agentes de tratamento de dados, atribuições e diálogo com o Código de Defesa do Consumidor**. In: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coords.). Lei Geral de Proteção de Dados — LGPD: caderno especial. São Paulo: Thomson Reuters/Revista dos Tribunais, 2019. p. 183-198.