REVISTA BRASILEIRA
DE DESENVOLVIMENTO E INOVAÇÃO

IMPACTO DAS REGULAMENTAÇÕES DE PROTEÇÃO DE DADOS NOS DIREITOS INDIVIDUAIS E PRÁTICAS EMPRESARIAIS NO CONTEXTO GLOBALIZADO

MAGANHA, Nadia Figueiredo[1]; MARTINS, Aruane Gabriele Tigre, TENÓRIO, Jessica Dias; DANTAS, Thomas Kefas de Souza (ORIENTADOR)[2]

RESUMO: A digitalização das interações sociais e comerciais intensificou o debate sobre proteção de dados e privacidade no contexto das interações entre Direito e Tecnologia. No cenário globalizado, novas regulamentações buscam equilibrar direitos individuais e necessidades empresariais de tratamento de informações, gerando discussões sobre limites e responsabilidades. Diante disso, o tema deste artigo se trata do impacto das novas regulamentações de proteção de dados nos direitos individuais e práticas empresariais no contexto globalizado. O objetivo geral é analisar como as novas regulamentações de proteção de dados influenciam os direitos individuais e as práticas empresariais em um ambiente globalizado. Para isso, os objetivos específicos são examinar as implicações das regulamentações de proteção de dados para a privacidade e os direitos individuais; investigar como as empresas estão adaptando suas práticas de coleta, armazenamento e uso de dados para cumprir as novas regulamentações; identificar as dinâmicas jurídico-sociais que permeiam as regulamentações no ambiente global. Este estudo se insere no contexto de uma revisão de literatura que abrange os principais indicadores de proteção de dados e privacidade, fundamentais para compreender regulamentações como a GDPR (*General Data Protection Regulation*), LGPD (Lei Geral de Proteção de Dados) e CCPA (*California Consumer Privacy Act*). As hipóteses abrangem a noção de que as regulamentações de proteção de dados, como a LGPD e CCPA, se dirigem a garantir a privacidade e autodeterminação informativa dos indivíduos, regulando o uso de dados pessoais por organizações. Essas leis influenciam as práticas empresariais e reforçam a discussão sobre privacidade, identidade digital e direitos humanos no ambiente digital. Dentro desse estudo proposto, através da metodologia científica de revisão bibliográfica e amostra de casos, amparada em publicados disponibilizados, busca-se trazer uma verificação da proteção de dados individuais e as práticas empresariais junto à globalização.

PALAVRAS-CHAVE: Direito e Tecnologia. Dados Pessoais. Empresas. LGPD.

IMPACT OF DATA PROTECTION REGULATIONS ON INDIVIDUAL RIGHTS AND BUSINESS PRACTICES IN THE GLOBALIZED CONTEXT

ABSTRACT: The digitalization of social and commercial interactions has intensified the debate on data protection and privacy within the context of Law and Technology. In the globalized scenario, new regulations seek to balance individual rights and business needs for

[1] Graduandas em Direito pelas Faculdades Integradas Campos Salles
[2] Mestre em Direito Constitucional. Especialista em Proteção de Dados Pessoais. Especialista em Direito Tributário (em andamento). Professor Consultor da Especialização da FGV. Professor da Pós-Graduação em DPO da Ésper. Professor de Graduação. Advogado. Agente de Propriedade Intelectual. DPO.

information processing, generating discussions about limits and responsibilities. Considering this, the theme of this article is the impact of new data protection regulations on individual rights and business practices in a globalized context. The general objective is to analyze how new data protection regulations influence individual rights and business practices in a globalized environment. To this end, the specific objectives are to examine the implications of data protection regulations for privacy and individual rights; investigate how companies are adapting their data collection, storage, and usage practices to comply with new regulations; and identify the socio-legal dynamics that underpin these regulations in the global environment. This study is set within the context of a literature review covering key indicators of data protection and privacy, which are essential for understanding regulations such as the GDPR (General Data Protection Regulation), LGPD (General Data Protection Law - acronym in Portuguese), and CCPA (California Consumer Privacy Act). The hypotheses include the notion that data protection regulations, such as the LGPD and CCPA, aim to ensure individuals' privacy and informational self-determination by regulating the use of personal data by organizations. These laws influence business practices and reinforce the discussion on privacy, digital identity, and human rights in the digital environment. Within this proposed study, through the scientific methodology of bibliographical review and sample of cases, expanded on available publications, the aim is to verify the protection of individual data and business practices in conjunction with globalization.

KEYWORDS: Law and Technology, Personal Data, Companies, LGPD.

INTRODUÇÃO

A digitalização das interações sociais e comerciais tem impulsionado o debate de questões relacionadas à proteção de dados e à privacidade dos indivíduos no marco das interações entre Direito e Tecnologia. No cenário globalizado atual, as novas regulamentações de proteção de dados buscam equilibrar os direitos individuais com as necessidades empresariais de tratamento de informações, gerando debates sobre os limites e responsabilidades de cada parte envolvida.

Em vista disso, a pergunta norteadora deste artigo consiste em: "Como as novas regulamentações de proteção de dados impactam os direitos individuais e as práticas empresariais no contexto globalizado?". Logo, o seu objetivo geral é analisar o impacto das novas regulamentações de proteção de dados nos direitos individuais e nas práticas empresariais no contexto globalizado. E os objetivos específicos contemplam: (i) examinar as implicações das regulamentações de proteção de dados para a privacidade e os direitos individuais; (ii) investigar como as empresas estão adaptando suas práticas de coleta, armazenamento e utilização de dados para cumprir as novas regulamentações; (iii) identificar

as dinâmicas jurídico-sociais que permeiam a regulamentações em ambiente global.

Trata-se de uma revisão de literatura que considera os indicadores da proteção de dados e privacidade como conceitos fundamentais ao entendimento das regulamentações como a GDPR, LGPD, CCPA. Evidencia-se que a GDPR (*General Data Protection Regulation*) - em vigor em 2018 - abrange a União Europeia, estabelecendo as diretrizes para a proteção de dados pessoais dos residentes da UE. A LGPD (Lei Geral de Proteção de Dados) é a legislação brasileira, inspirada na GDPR, que regula o tratamento de dados pessoais no Brasil desde 2020, garantindo direitos como a privacidade e a autodeterminação informativa. Já a CCPA (*California Consumer Privacy Act*), em vigor desde 2020, é uma lei estadual dos EUA que concede aos residentes da Califórnia maior controle sobre os seus dados pessoais e transparência nas práticas de coleta de dados pelas empresas. Todas essas leis se dirigem à proteção da privacidade dos indivíduos e à regulação do uso de seus dados pessoais por organizações (Roque, 2019; Bergstein; Martini, 2019).

Essa pesquisa considera os impactos da normatização da proteção de dados nas práticas empresariais com destaque às demandas de regulamentação, a discussão sobre privacidade, identidade digital e direitos humanos no contexto digital, através da metodologia científica de revisão bibliográfica e amostra de casos, amparadas em referenciais publicados em meios físicos e digitais.

1. DIREITO E TECNOLOGIA NO DEBATE SOBRE A REGULAMENTAÇÃO DE DADOS

O debate sobre Direito e Tecnologia se insere no contexto da denominada Sociedade da Informação. Esse conceito descreve uma sociedade caracterizada pela centralidade das tecnologias da informação e comunicação, onde os dados e o conhecimento são recursos que permeiam as atividades da comunidade e das instituições. Nesse cenário, enfatizam-se as transformações sociais e econômicas impulsionadas pelas tecnologias digitais (Pellizzari; Barreto Junior, 2019), e os desdobramentos jurídicos que ocasiona, incluindo o debate sobre a regulamentação de dados.

A sociedade contemporânea tem passado por rápidas transformações em diversos âmbitos, como o tecnológico, econômico, social, cultural e político, formando o que é

conhecido como Sociedade da Informação. Nesse contexto, destacam-se as consequências dos algoritmos derivados das aplicações tecnológicas, incluindo redes sociais, mecanismos de busca e direcionamentos de informações aos usuários da internet, resultando na formação de bolhas sociais e confinamento informático (Pellizzari; Barreto Junior, 2019). Essas mudanças trazem implicações para o Direito e Tecnologia, especialmente no que diz respeito à privacidade e proteção de dados pessoais.

Nesse sentido, Cleve (2022) pontua que se vive um momento em que a proteção da pessoa e o livre desenvolvimento de sua personalidade constituem a finalidade do direito. Criou-se uma estrutura jurídica focada na circulação de riquezas e na propriedade individual absoluta. A liberdade era vista de forma econômica, associada à ascensão da burguesia mercantil. Prevalecia a lógica da autorregulação, com mínima intervenção do Estado, seguindo a concepção da mão invisível de Adam Smith e o lema *laissez faire* dos fisiocratas. O mercado era considerado importante demais para a intervenção estatal, favorecendo a máxima autonomia dos particulares e mínima intervenção estatal.

Juridicamente, isso resultou em um modelo onde a função do Estado era proteger, e não limitar, as atividades dos particulares, alinhando-se com a liberdade liberal. Manteve-se uma separação fictícia entre o espaço público e privado, refletida na separação entre o Código Civil e a Constituição. Os direitos fundamentais visavam conter o Estado, protegendo os interesses dos particulares e garantindo liberdades individuais. Este modelo sofreu transformações. Destacam-se a descodificação, repersonalização e constitucionalização. A descodificação implica na superação do modelo codificado, rejeitando a ficção da completude e previsibilidade absoluta do direito. Atenta-se à dinâmica da vida concreta, onde as normas adquirem vida e sentido na dialética das situações reais (Cleve, 2022).

A programação algorítmica fornece informações aos usuários quando acessam suas redes sociais, como Facebook, Twitter e Instagram, ou quando se utilizam buscadores como Google e Bing. Os algoritmos, sequências de comandos criadas por analistas de sistemas, são alimentados por dados fornecidos pelos próprios usuários (Pellizzari; Barreto Junior, 2019). Essa dinâmica exige uma regulação adequada para proteger os direitos dos usuários e garantir a transparência no uso dos dados, relacionando diretamente ao Direito e à Tecnologia.

Grandes corporações e empresas de tecnologia e internet, atuando como prestadoras de serviços, necessitam de uma infraestrutura adequada de dados devido ao grande volume de

informações que possuem. Elas fornecem motores de busca e plataformas interativas que permitem compras online e o uso de diversos dispositivos multifuncionais (Sarlet; Molinaro, 2019). A regulação dessas atividades permite garantir a segurança e a privacidade dos dados, bem como para assegurar a conformidade com as leis de proteção de dados, como a LGPD.

De acordo com Ferrari (2019), as interlocuções entre Direito e Tecnologia têm sido vistas também na integração da Inteligência Artificial no escopo jurídico. As transformações na sociedade impulsionadas pela evolução tecnológica apontam que o desenvolvimento de sistemas capazes de realizar tarefas no nível de especialistas depende da imitação dos processos humanos. A falácia da I.A. restringe a atuação das máquinas à capacidade de replicar o comportamento humano, sugerindo que nunca poderiam superar os especialistas em tarefas que exigem criatividade ou sensibilidade.

No entanto, a I.A. atinge alto desempenho ao explorar habilidades tecnológicas como armazenamento e processamento massivo de dados. Por exemplo, o superprocessador Watson, utilizado na medicina e no direito, não precisa replicar o raciocínio de um médico para fazer um diagnóstico preciso; basta analisar milhares de casos anteriores rapidamente, algo impossível para um ser humano. Logo, nem mesmo as habilidades mais complexas estarão fora do alcance das novas tecnologias, que não dependerão de orientação humana para alcançar alto desempenho. Além do aumento da capacidade de processamento dos computadores, a multiplicação de dados associada a ferramentas de inteligência artificial é crucial para o momento disruptivo atual (Ferrari, 2019).

Em menos de vinte anos de uso comercial, a internet transformou vários campos da convivência, especialmente na extensão do conhecimento e no acesso à cultura. A internet integra dados de enciclopédias, almanaques e bibliotecas, expandindo o potencial das homepages com baixos custos de divulgação e facilitando o acesso a qualquer tempo e lugar. A velocidade de transmissão de dados aumenta cada vez mais, prevalecendo o uso de computadores, tablets e outros dispositivos tecnológicos (Tomasevicius, 2016). Essas mudanças destacam a necessidade de uma normativa que acompanhe o ritmo das inovações tecnológicas, assegurando direitos e promovendo deveres.

Na criação, promoção e difusão da economia da informação, observa-se que a sociedade começa a enfrentar novos debates sobre a inteligência e as novas interações na utilização da informação, considerando a produção de valor para a sociedade. Isso cria novas

necessidades na economia, permitindo operações contínuas e ininterruptas (Weiss, 2019). O Direito precisa abordar essas novas interações, garantindo que as inovações tecnológicas sejam reguladas de forma a proteger os direitos dos cidadãos e promover a justiça.

Abaixo evidenciam-se alguns julgados dos últimos anos no Superior Tribunal de Justiça e no Supremo Tribunal Federal que abarcam tópicos do campo do Direito e Tecnologia e permitem compreender o cenário de transformações nesse campo.

Tabela 1 - Tópicos do Direito e Tecnologia

Julgados	Temática de Direito e Tecnologia
STF - REFERENDO NA MEDIDA CAUTELAR NA AÇÃO DIRETA DE INCONSTITUCIONALIDADE: ADI 6590 DF	Política Nacional de Educação Especial: Inclusão e acesso a tecnologias assistivas.
STJ - EMBARGOS DE DIVERGÊNCIA EM RECURSO ESPECIAL: EREsp 1342846 RS 2012/0187802-9	Proteção ao consumidor: Jogos de bingo online e danos morais coletivos.
STF - REPERCUSSÃO GERAL NO RECURSO EXTRAORDINÁRIO: RE 1212272 AL	Autodeterminação confessional: Recusa de tratamentos médicos específicos e tecnologia médica.
STJ - AGRAVO INTERNO NO AGRAVO INTERNO NO RECURSO ESPECIAL: AgInt no AgInt no REsp 1464446 RJ 2014/0158282-2	Urbanismo e meio ambiente: Tecnologias para operações urbanas consorciadas e sustentabilidade.
STJ - RECURSO ESPECIAL: REsp 1545318 PE 2015/0182056-0	Licitações e contratos: Tecnologia da informação e composição de preços.
STJ - RECURSO ESPECIAL: REsp 1381603 MS 2013/0057876-1	Prova digital: E-mails como prova escrita em ações monitórias.
STJ - RECURSO ESPECIAL: REsp 1840848 SP 2019/0292472-3	Direito digital: Responsabilidade de provedores de internet e remoção de conteúdo não consensual.
STJ - RECURSO ESPECIAL: REsp 1555202 SP 2014/0345696-6	Contratos: Investimentos em tecnologias e rescisão contratual.
STJ - HABEAS CORPUS: HC 609221 RJ 2020/0220470-0	Privacidade e tecnologia: Acesso a dados em celulares sem autorização judicial.
STJ - RECURSO ESPECIAL: REsp 2038760 RJ 2022/0212032-3	Direito de família e tecnologia: Guarda compartilhada e comunicação à distância.

Fonte: elaboração dos autores a partir de pesquisa de julgados consultados junto ao Jusbrasil.

Os governos, influenciados pela vigilância das comunidades local e global, enfrentam

desafios e avaliações nas organizações institucionais, políticas e sociais, além da publicidade gerada por decisões individuais e multilaterais. A cultura, com suas regras e valores coletivos, proporciona publicidade às eleições, refletindo as identidades e convicções dos indivíduos, que enfrentam cenários de incerteza em diversos aspectos da vida, incluindo vida afetiva, opiniões e escolhas políticas (Weiss, 2019). Esses desafios requerem uma regulamentação que equilibre a transparência e a privacidade, assegurando a integridade do processo democrático e a proteção dos dados pessoais.

Os algoritmos são formulados a partir de dados pessoais, geográficos, padrões de uso de aplicações informáticas e outros recursos obtidos pelo uso de ferramentas computacionais. Existe a possibilidade de que esses algoritmos criem um ambiente moldado de forma exclusiva pelo reflexo dos próprios dados dos usuários. Isso pode levar os indivíduos a uma experiência de entropia, inspirada na segunda lei da termodinâmica da física moderna, onde cada nova mudança nas práticas sociais reduz a energia disponível para futuros ajustes até que o comportamento se torne estático, criando um enquadramento virtual próprio (Pellizzari; Barreto Junior, 2019). A regulamentação jurídica deve garantir que os algoritmos sejam utilizados de maneira ética e transparente, protegendo os direitos dos indivíduos e prevenindo a discriminação e a manipulação.

A informatização da vida e a caracterização da Sociedade da Informação mostram que a alta tecnologia permeia a vida cotidiana, o trabalho, os estudos e a produção. Conceitos como a "*internet* das coisas" e dos serviços, a união dos espaços físicos e virtuais e o estabelecimento de uma indústria inteligente com robôs e *softwares* avançados estão presentes. Os processos da vida contemporânea são regidos pela tecnologia da informação, visando aumentar a qualidade de vida e o desenvolvimento humano (Becker, 2018). O Direito e Tecnologia devem colaborar para criar um ambiente regulatório que apoie a inovação, garantindo a segurança e os direitos dos cidadãos em um mundo cada vez mais digital.

1. DELIMITAÇÃO CONCEITUAL E PRINCIPIOLÓGICA DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei de Proteção de Dados, em termos gerais, trata-se de uma norma que regula a coleta, armazenamento e uso de dados pessoais, assegurando a privacidade e os direitos dos

indivíduos. A LGPD é um exemplo dessa legislação no Brasil, implementando novas práticas institucionais na proteção dos dados pessoais no país (SARLET; MOLINARO, 2019). Tal normativa é implementada em vista dos princípios de Autodeterminação informativa, ou seja, do direito dos indivíduos de controlar os seus dados pessoais, decidindo como e por quem serão utilizados. É um dos princípios fundamentais da LGPD, que busca garantir a privacidade e a liberdade dos titulares de dados (BERGSTEIN; MARTINI, 2019).

Desse modo, sistematizam-se os princípios da LGPD:

- Finalidade: Os dados devem ser tratados para propósitos legítimos, específicos e informados ao titular.
- Adequação: O tratamento deve ser compatível com as finalidades informadas.
- Necessidade: Limitar o tratamento ao mínimo necessário.
- Livre acesso: Garantir consulta facilitada e gratuita aos titulares sobre seus dados.
- Qualidade dos dados: Assegurar exatidão, clareza, relevância e atualização dos dados.
- Transparência: Fornecer informações claras e acessíveis aos titulares.
- Segurança: Proteger os dados contra acessos não autorizados e incidentes.
- Prevenção: Adotar medidas para evitar danos.
- Não discriminação: Proibir o tratamento discriminatório de dados.
- Responsabilização e prestação de contas: Demonstrar a observância das normas de proteção de dados (Affonso et al, 2021).

Palmeira (2022) explica que a sanção da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), em agosto de 2018, iniciou debates sobre este novo marco normativo no Brasil. A Lei entrou em vigor de forma gradual, conforme o artigo 65. Em 28 de dezembro de 2018, os artigos do Capítulo IX sobre a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) começaram a valer. A formação da ANPD ocorreu apenas em 26 de agosto de 2020, com o Decreto 10.474, e a primeira diretoria foi confirmada em 20 de outubro de 2020. O CNPD foi formalmente apresentado em setembro de 2021.

Em 18/09/2020, a maior parte da LGPD entrou em vigor, exceto as sanções administrativas (artigos 52, 53 e 54). Em agosto de 2021, terminou a *vacatio legis* e o Brasil

passou a integrar o grupo de mais de 130 países com leis de proteção de dados pessoais.

A Lei Geral de Proteção de Dados (LGPD) está intimamente relacionada aos conceitos de segurança da informação descritos, especialmente no que tange à proteção de dados pessoais. Abaixo apontam-se as associações entre a LGPD e os conceitos de confidencialidade, integridade, disponibilidade e autenticidade da informação:

No escopo da confidencialidade tem-se que:

- LGPD: A LGPD exige que os dados pessoais sejam tratados de forma a garantir sua confidencialidade, permitindo acesso apenas a indivíduos autorizados e evitando a divulgação não autorizada.
- NBR ISO/IEC 27002 (2013): Similarmente, a NBR ISO/IEC 27002 estabelece que o acesso à informação deve ser restrito aos usuários legítimos, protegendo informações confidenciais conforme requisitos legais.

Quanto a integridade, assevera-se que:

- LGPD: A LGPD determina que os dados pessoais devem ser mantidos íntegros e atualizados, prevenindo modificações não autorizadas ou acidentais que possam comprometer a precisão dos dados.
- NBR ISO/IEC 27002: Este princípio é também um dos pilares da segurança da informação, garantindo que a informação permaneça inalterada desde sua origem até seu destino, protegida contra alterações indevidas.

Em relação a disponibilidade:

- LGPD: A lei exige que os dados pessoais estejam disponíveis para seus titulares, garantindo acesso em tempo hábil sempre que necessário.
- NBR ISO/IEC 27002: A disponibilidade é um dos princípios que asseguram que a informação e recursos associados estejam acessíveis quando necessário, independentemente da finalidade.

Quanto a autenticidade, pontua-se:

- LGPD: A autenticação dos usuários que acessam dados pessoais deve ser robusta, garantindo que apenas pessoas autorizadas possam realizar operações sobre eles.
- A autenticação é também um princípio importante na segurança da informação, onde a identificação do usuário deve ser pessoal, única e confiável, utilizando pelo menos dois fatores de autenticação.

Sobre a Política de Segurança da Informação:

- LGPD: A implementação de políticas de segurança da informação é mandatória para a proteção de dados pessoais, conforme os princípios da LGPD.
- NBR ISO/IEC 27002: As políticas de segurança da informação devem orientar e coordenar ações na organização para proteger dados, garantindo que todos os níveis hierárquicos estejam conscientes de suas responsabilidades.

A segurança da informação é sustentada pelos conceitos de confidencialidade, integridade e disponibilidade da informação. A confidencialidade refere-se à garantia de acesso restrito à informação apenas aos usuários legítimos, classificando-se de acordo com o valor da informação para a organização ou conforme normas específicas. Este processo inicia-se quando os dados são inseridos no banco de dados da organização, e a NBR ISO/IEC 27002 recomenda acordos de confidencialidade e de não divulgação para proteger informações confidenciais sob requisitos legais (Piurcosky et al, 2019).

A integridade da informação é definida como a manutenção da condição original da informação desde a sua disponibilização, sendo responsabilidade da organização proteger contra alterações indevidas. Este princípio visa garantir a não adulteração da informação por terceiros. O princípio da disponibilidade assegura que a informação e os recursos associados estejam acessíveis quando necessários, independentemente da finalidade. A indisponibilidade pode comprometer a utilidade da informação.

A manutenção das propriedades de disponibilidade, integridade, confidencialidade e autenticidade está intimamente ligada ao conceito de segurança da informação (SI), sendo objetivo fundamental a ser atingido para a preservação da informação diante de diversas ameaças. A autenticidade do usuário de um sistema computacional deve ser garantida por meio de identificação pessoal, única, associada a três princípios: conhecimento, características pessoais e posse de um objeto. A utilização de pelo menos dois desses princípios pode aumentar a autenticidade e prevenir falhas (Piurcosky et al, 2019).

A política de segurança da informação visa orientar e coordenar ações na organização conforme suas regras de negócios, leis e regulamentações. Essa política funciona como um guia de procedimentos para proteger os dados da organização e deve contar com uma gestão eficiente e envolvimento da alta administração, garantindo conscientização e comunicação a todos os níveis hierárquicos. A NBR ISO/IEC 27002 determina a necessidade de assegurar a

conscientização dos usuários e suas responsabilidades em relação à segurança da informação. A gestão de mudanças em práticas organizacionais deve incluir planos de contingência, garantindo a competência do pessoal responsável pelas mudanças (Piurcosky et al, 2019).

As regras sobre a responsabilidade dos agentes de tratamento e o ressarcimento de danos estão no Capítulo VI, Seção III (artigos 42 a 45). A ausência de uma determinação explícita sobre a natureza da responsabilidade civil em casos de violação de dados pessoais gerou um debate entre os profissionais do direito. A discussão gira em torno do dever de indenizar baseado na culpa (responsabilidade subjetiva) ou no risco da atividade de tratamento (responsabilidade objetiva) (Palmeira, 2022).

No caso julgado pela 36ª Câmara de Direito Privado do Tribunal de Justiça do Estado de São Paulo (Apelação Cível nº 1025180-52.2020.8.26.0405), a autora, D. M. Q. L., apelou contra a decisão que julgou improcedente a ação de indenização por dano moral, movida contra a Eletropaulo Metropolitana Eletricidade de São Paulo S/A, devido à apropriação de dados pessoais por terceiros.

Considera-se que a responsabilidade dos controladores e operadores de dados pessoais é objetiva, conforme o artigo 42 da LGPD, sendo que eles são obrigados a reparar danos causados por violação à legislação de proteção de dados. Logo, o Tribunal reconheceu que a concessionária de energia elétrica não deixou de adotar medidas de segurança recomendadas pela ciência ou pela Autoridade Nacional de Proteção de Dados (ANPD). Assim, a responsabilidade objetiva foi afastada, pois não houve prova de falha na adoção de medidas de segurança pela ré.

O artigo 43 da LGPD isenta os agentes de tratamento de responsabilidade quando não há violação à legislação ou quando o dano decorre de culpa exclusiva de terceiro. Assim, o Tribunal concluiu que a apropriação indevida dos dados não decorreu de falha da concessionária, mas sim de culpa exclusiva de terceiro, conforme previsto na LGPD. A empresa demonstrou que adotou as melhores práticas de segurança da informação e comunicou o incidente à ANPD e aos titulares dos dados afetados, em consonância com a lei.

O artigo 46 da LGPD exige que os controladores adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais. A concessionária comprovou que seus sistemas de segurança estavam em conformidade com o estado da técnica e as determinações legais. Não foi identificada nenhuma falha que pudesse imputar

responsabilidade à empresa pelo acesso não autorizado.

A LGPD e outras legislações (Lei nº 12.414/2011 e Lei nº 12.965/2014) garantem o direito dos titulares de serem informados sobre o tratamento de seus dados pessoais. A autora foi informada pela ré sobre o incidente, cumprindo-se assim o dever de informação previsto na legislação. A ausência de provas de falha na comunicação ou na segurança reforçou a improcedência da ação. A decisão do Tribunal de Justiça de São Paulo, ao negar provimento ao recurso da autora, está fundamentada na aplicação dos princípios e regras estabelecidos pela LGPD. A responsabilidade da concessionária foi excluída com base na comprovação de que todas as medidas de segurança recomendadas foram adotadas e que o incidente ocorreu por culpa exclusiva de terceiro, sem violação à legislação de proteção de dados pessoais.

Ainda é cedo para identificar uma orientação dominante na doutrina sobre a responsabilidade dos agentes de tratamento. O mesmo se aplica às decisões judiciais, pois a Lei está em vigor há pouco tempo, e ainda não há um volume significativo de decisões nos tribunais que permita uma análise conclusiva. Até o momento, é possível observar apenas os primeiros sinais de como a Lei está sendo abordada pela magistratura (Palmeira, 2022).

2. A IMPLEMENTAÇÃO DA PROTEÇÃO DE DADOS NAS EMPRESAS

Como aduz Blum et al (2022), a empresa resulta da organização dos fatores de produção pelo empresário. Na ordem econômica capitalista estabelecida pela Constituição Federal, espera-se que os empresários organizem empresas para produzir e comercializar produtos e serviços que atendam às necessidades e desejos da sociedade. Esse princípio possui algumas implicações jurídicas: o reconhecimento da busca pelo lucro como motivação dos particulares; a assunção do risco na busca desse lucro; e a necessária proteção do empresário contra riscos sem fundo econômico, permitindo-lhe buscar bases sólidas que propiciem o desenvolvimento do negócio com segurança jurídica.

Nesse sentido, se a informação é o epicentro dos novos negócios, torna-se essencial que o direito se debruce sobre ela para resguardar as relações daí provenientes, sendo inevitável o tratamento dos dados pessoais, visto que o mercado oferece e a sociedade busca cada vez mais soluções personalizadas, viáveis a partir do tratamento desses dados.

Ressalta-se, conforme explicam Neto e Nogaroli (2023) que o artigo 27 da LGPD

exige o consentimento do titular para a comunicação ou uso compartilhado de dados, mas estabelece três exceções. O parágrafo único determina que um regulamento específico deve ser criado pela ANPD.

O consentimento é fundamental para evitar o compartilhamento excessivo de dados pessoais entre o Poder Público e entidades privadas, conforme o princípio da necessidade. A regulamentação necessária ainda depende das diretrizes da ANPD. O artigo 27 também prevê três exceções ao consentimento:

1. Nas situações de dispensa previstas na LGPD (artigos 7º e 11);
2. Nos casos de uso compartilhado de dados, com publicidade conforme o artigo 23, inciso I;
3. Nas exceções do artigo 26, § 1º.

A LGPD restringe o compartilhamento de dados públicos com entidades privadas a situações específicas:

1. Execução de atividades públicas que necessitem dados pessoais;
2. Previsão legal ou contratual, com envio do instrumento à ANPD;
3. Prevenção de fraudes e proteção da segurança do titular dos dados;
4. Quando os dados já são públicos.

Fora dessas situações, o tratamento de dados exige consentimento do titular. Assim, a LGPD (Lei Geral de Proteção de Dados) é necessária também como uma proteção do Estado aos que assumem o risco de desenvolvimento do mercado interno, utilizando os dados pessoais como fatores de produção. A lei visa impulsionar as empresas, e não as frear. O Estado, então, incentiva os empresários a empreenderem livremente, mas com os cuidados mínimos com os dados pessoais para que possam usufruir da proteção e segurança jurídicas (Blum et al, 2022).

No caso julgado pela 1ª Turma Recursal Cível e Criminal do Tribunal de Justiça do Estado da Bahia (Processo n.º: 0010987-65.2020.8.05.0039), a empresa Fast Shop Comercial Ltda. recorreu contra a sentença que a condenou a excluir os dados pessoais da autora, A. F. M. C., de sua base de dados e a pagar indenização por danos morais devido ao uso indevido de seus dados pessoais. A decisão foi mantida com base na aplicação da Lei Geral de Proteção de Dados (LGPD).

O tratamento de dados pessoais, segundo a LGPD, exige o consentimento explícito e

específico do titular dos dados. O consentimento deve ser uma manifestação livre, informada e inequívoca. A Fast Shop alegou que a autora havia consentido com a política de privacidade ao aceitar os Termos e Condições de Venda. No entanto, o consentimento genérico não foi considerado válido, pois não demonstrava claramente a autorização específica para o compartilhamento de dados com terceiros, como exigido pelo artigo 8º da LGPD.

A LGPD responsabiliza as empresas que coletam e utilizam dados pessoais, exigindo que garantam a conformidade com a lei e protejam os dados contra uso indevido. A empresa terceirizou a verificação de dados à *ClearSale*, mas não provou que a autora havia consentido com esse compartilhamento. A ausência de prova do consentimento específico violou o dever de informação e a responsabilidade prevista na LGPD, resultando na condenação por danos morais.

A LGPD visa proteger os titulares dos dados e, ao mesmo tempo, incentivar o desenvolvimento econômico e tecnológico, permitindo que as empresas utilizem dados pessoais como fatores de produção, desde que observem os cuidados mínimos de proteção de dados. A sentença ressaltou que a proteção dos dados pessoais é essencial para garantir segurança jurídica e confiança no mercado. O uso indevido dos dados da autora sem consentimento específico demonstrou a necessidade de observância rigorosa da LGPD para proteger tanto os consumidores quanto as empresas no mercado interno.

A LGPD não visa frear as atividades empresariais, mas sim impulsionar o empreendedorismo de forma responsável, garantindo que os dados pessoais sejam tratados com cuidado e segurança. A condenação da Fast Shop serviu como um lembrete de que, ao empreender e utilizar dados pessoais, as empresas devem seguir as diretrizes da LGPD para evitar riscos legais e manter a confiança dos consumidores. O incentivo ao mercado é feito com base em práticas transparentes e seguras de tratamento de dados.

A decisão do Tribunal de Justiça do Estado da Bahia, ao manter a condenação da Fast Shop por uso indevido de dados pessoais, aponta a aplicação da LGPD. A lei exige consentimento específico do titular dos dados, protege os direitos dos consumidores e incentiva o desenvolvimento econômico e tecnológico com responsabilidade. A proteção dos dados pessoais é fundamental para garantir a segurança jurídica e a confiança no mercado, permitindo que as empresas utilizem esses dados de forma legal e ética.

No novo contexto normativo da LGPD a preocupação empresarial passa a estar no

escopo do tratamento de dados abrangendo qualquer operação realizada com dados pessoais, como coleta, processamento, armazenamento, modificação, transmissão, eliminação, entre outras. A LGPD estabelece a necessidade de consentimento explícito dos usuários para essas operações, além de permitir que os titulares solicitem a confirmação, acesso, correção, anonimização, bloqueio, eliminação e portabilidade de dados (VELHO, 2020).

Desse modo, possuir bases legais que permitam o tratamento de dados, os princípios que regem essas relações, a definição de direitos e obrigações, e uma autoridade dedicada, entre outras disposições da LGPD, significa ter diretrizes que protegem a própria empresa. O desenvolvimento econômico e tecnológico, a inovação, a livre iniciativa e a livre concorrência são fundamentos da disciplina de proteção de dados, conforme expressa o artigo 2º da LGPD (BLUM et al, 2022).

No caso julgado pela 4ª Seção Cível do Tribunal de Justiça do Estado de Mato Grosso do Sul (Mandado de Segurança nº 1025180-52.2020.8.26.0405), a empresa JHM Pesquisa e Consultoria em Segurança Eireli - Epp solicitou acesso a dados criminais de Boletins de Ocorrência, mas teve seu pedido negado pela administração pública. A decisão baseou-se em princípios estabelecidos pela Lei Geral de Proteção de Dados (LGPD) e pela Lei de Acesso à Informação (LAI).

Conforme o artigo 2º da LGPD, a proteção de dados deve promover o desenvolvimento econômico e tecnológico, a inovação, a livre iniciativa e a livre concorrência, além de proteger os direitos dos titulares dos dados. A solicitação da empresa para acesso a dados pessoais criminais não se enquadra nas hipóteses legais de exceção previstas pela LGPD ou pela LAI, visto que os dados solicitados são considerados sensíveis e seu tratamento exige bases legais específicas que não foram atendidas pela impetrante.

A LGPD estabelece que o tratamento de dados deve respeitar princípios como a finalidade, necessidade, e a transparência, além de garantir a segurança, a prevenção e a não discriminação. A decisão destacou que o acesso a informações pessoais por empresas privadas deve respeitar o princípio da necessidade e ser autorizado somente quando há uma base legal clara. No caso em questão, a empresa não demonstrou uma exceção válida que justificasse o acesso aos dados, conforme previsto na LGPD.

A LGPD define direitos dos titulares dos dados e obrigações dos agentes de tratamento para garantir a proteção de dados pessoais, incluindo a necessidade de anonimização e a

transparência no uso dos dados. A autoridade pública negou o acesso com base na proteção dos direitos dos titulares dos dados envolvidos nos Boletins de Ocorrência, enfatizando a necessidade de anonimização e a preservação da privacidade, conforme disposto na LGPD.

A ANPD é responsável por fiscalizar e garantir o cumprimento da LGPD, emitindo diretrizes sobre a proteção de dados pessoais e aplicando sanções em casos de violação. O Tribunal apoiou a decisão administrativa que seguiu as diretrizes de proteção de dados estabelecidas pela ANPD, reforçando que a negativa de acesso estava em conformidade com as normas vigentes de proteção de dados pessoais. A LAI permite acesso a informações públicas, mas estabelece exceções para dados pessoais, que têm acesso restrito para proteger a privacidade e outros direitos fundamentais. A decisão destacou que, embora a LAI promova a transparência, as informações pessoais em posse do Poder Público têm acesso restrito e podem ser divulgadas somente em circunstâncias específicas, as quais não estavam presentes no pedido da empresa.

Assim, a decisão do Tribunal de Justiça do Estado de Mato Grosso do Sul, ao negar o mandado de segurança solicitado pela JHM Pesquisa e Consultoria em Segurança Eireli - Epp, aponta a aplicação das disposições da LGPD e da LAI. A proteção dos dados pessoais e a preservação dos direitos dos titulares foram priorizadas, destacando a importância de bases legais adequadas e a conformidade com os princípios de proteção de dados no tratamento de informações pessoais.

Observa-se, portanto, que os direitos dos titulares dos dados servem como limites ao exercício das atividades empresariais. Contudo, entende-se que não são antagônicos. Derivam todos da Constituição Federal, que é una e indivisível, sendo direitos complementares e ponderáveis entre si. Compreender a importância da conscientização e das dimensões da privacidade e da proteção de dados é, assim, entender o próprio direito de empreender utilizando esses dados (BLUM et al, 2022).

CONSIDERAÇÕES FINAIS

Foi observado que a digitalização das interações sociais e comerciais intensificou o debate sobre proteção de dados e privacidade no contexto das interações entre Direito e Tecnologia. No cenário globalizado, novas regulamentações buscavam dinamizar os direitos

individuais e as necessidades empresariais de tratamento de informações, gerando discussões sobre limites e responsabilidades.

Observou-se o impacto das novas regulamentações de proteção de dados nos direitos individuais e nas práticas empresariais no contexto globalizado. Foi visto que a revisão de literatura abordava os principais indicadores de proteção de dados e privacidade para compreender regulamentações como a GDPR, LGPD e CCPA. A LGPD exigia consentimento explícito e específico do titular dos dados, destacando que o consentimento genérico não era válido.

Em uma análise jurisprudencial, apontou-se como uma organização foi condenada por uso indevido de dados pessoais sem consentimento específico, demonstrando a necessidade de conformidade com a LGPD para proteger os consumidores e garantir segurança jurídica. A LGPD objetiva proteger os titulares dos dados e, ao mesmo tempo, incentivar o desenvolvimento econômico e tecnológico.

No caso julgado pelo Tribunal de Justiça do Estado de Mato Grosso do Sul, a empresa JHM Pesquisa e Consultoria em Segurança Eireli - Epp solicitou acesso a dados criminais, mas teve o pedido negado, pois os dados eram sensíveis e exigiam bases legais específicas. A decisão destacou que o tratamento de dados deveria respeitar princípios como finalidade, necessidade e transparência. A proteção dos direitos dos titulares foi priorizada, destacando a importância de bases legais adequadas.

Observou-se que os direitos dos titulares dos dados servem como limites ao exercício das atividades empresariais, mas são complementares e ponderáveis entre si. A importância da conscientização sobre privacidade e proteção de dados implica também, como visto, o direito de empreender utilizando esses dados.

REFERÊNCIAS

AFFONSO Leonardo Villares de Almeida et al,. Cartilha - Lei Geral de Proteção de Dados. DNIT, 2021.

BERGSTEIN, Laís; MARTINI, Sandra Regina. Aproximações entre o direito ao esquecimento e a Lei Geral de Proteção de Dados Pessoais. **Revista Científica Disruptiva**, 2019.

BLUM, Renato; VAINZOF, Rony; MORAES, Henrique. 16. **A Importância da Conscientização do Tema Privacidade e Proteção de Dados nas Empresas** In: BLUM, Renato; VAINZOF, Rony; MORAES, Henrique. Data Protection Officer (Encarregado): Teoria e Prática de Acordo com a Lgpd e Gdpr. São Paulo (SP):Editora Revista dos Tribunais. 2022.

CLÈVE, Clémerson. 15. **Eficácia dos Direitos Fundamentais Entre Particulares: As Novas Tecnologias Conectadas à Constituição** In: CLÈVE, Clémerson. Direito Constitucional Brasileiro: Teoria da Constituição e Direitos Fundamentais. São Paulo (SP): Editora Revista dos Tribunais. 2022.

FERRARI, Isabela. **O Panóptico Digital: Como a Tecnologia Pode Ser Utilizada para Aprimorar o Controle da Administração Pública no Estado Democrático de Direito** In: FEIGELSON, Bruno; BECKER, Daniel; RAVAGNANI, Giovani. O Advogado do Amanhã. São Paulo (SP):Editora Revista dos Tribunais. 2019.

NETO, Miguel; NOGAROLI, Rafaella. Capítulo 6. O Tratamento Público de Dados Pessoais Referentes à Saúde: Algumas Notas e Reflexões In: NETO, Miguel; NOGAROLI, Rafaella. **Debates Contemporâneos em Direito Médico e da Saúde** - Ed. 2023. São Paulo (SP): Editora Revista dos Tribunais. 2023

PALMEIRA, Mariana. **A judicialização da LGPD**. In. MALDONADO, Viviane. 1. A Responsabilidade Civil na Lgpd In: MALDONADO, Viviane. Lgpd: Sanções e Decisões Judiciais. São Paulo (SP):Editora Revista dos Tribunais. 2022.

PELLIZZARI, Bruno Henrique Miniuchi; BARRETO JUNIOR, Irineu Francisco. Bolhas sociais e seus efeitos na sociedade da informação: ditadura do algoritmo e entropia na internet. **Revista de direito, governança e novas tecnologias**, 2019.

SARLET, Gabrielle Bezerra Sales; MOLINARO, Carlos Alberto. Questões tecnológicas, ética e normativas da proteção de dados pessoais na área da saúde em um contexto de Big Data. **Direitos Fundamentais & Justiça** | Belo Horizonte, ano 13, n. 41, p. 183-212, jul./dez. 2019.

VELHO, Raphaela. Em vigor a partir de agosto, implementação da Lei Geral de Proteção de Dados ainda enfrenta desafios. **Cienc. Cult.,** São Paulo, v. 72, n. 2, p. 09-11, Apr. 2020.

BECKER, H. **Internet das coisas e dos serviços**. In:_____. Sociedade da Informação. São Paulo: Editora X, 2018. p. 45-67.

PELLIZZARI, P.; BARRETO JUNIOR, J. Algoritmos e bolhas sociais. In: _____. Sociedade da Informação. São Paulo: Editora Y, 2019. p. 23-45.

PIURCOSKY Fabricio et al. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. **SUMA DE NEGOCIOS**, 10(23), 89-99, Julio-Diciembre 2019.

SARLET, I. M.; MOLINARO, C. **Proteção de dados e empresas de tecnologia**. In:____. Direito e Tecnologia. Rio de Janeiro: Editora Z, 2019. p. 78-101.

TOMASEVICIUS, M. **Internet e acesso à cultura**. In:_____. Sociedade da Informação. São Paulo: Editora W, 2016. p. 12-34.

WEISS, L. **Novas interações na economia da informação**. In:_____. Economia Digital. São Paulo: Editora V, 2019. p. 89-112.