

CENTRO UNIVERSITÁRIO UNINOVAFAPI BACHARELADO EM DIREITO

ELAYNE VELOSO ARAUJO

**A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE
DADOS PESSOAIS E SUA APLICAÇÃO NO ÂMBITO EMPRESARIAL**

TERESINA – PI

2022

ELAYNE VELOSO ARAUJO

**A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE
DADOS PESSOAIS E SUA APLICAÇÃO NO ÂMBITO EMPRESARIAL**

Artigo apresentado à Banca Examinadora do Centro
Universitário Uninovafapi, como requisito parcial
para obtenção do grau de Bacharel em Direito.

Orientadora: Profa. Dra. Cléa Mara Coutinho Bento

TERESINA – PI

2022

FICHA CATALOGRÁFICA

A663i Araujo, Elayne Veloso.

A Importância da Lei Geral de Proteção de dados pessoais e sua aplicação no âmbito empresarial. Elayne Veloso Araujo – Teresina: Uninovafapi / Afya, 2022.

Artigo (Graduação em Direito) – Centro Universitário UNINOVAFAPI, Teresina, 2022.

20. p.; il. 23cm.

Orientadora: Profa. Dra. Cléa Mara Coutinho Bento. Centro Universitário UNINOVAFAPI, 2022.

1. Proteção de dados pessoais. 2. Empresarial. 3. Mundo digital.
I. Título. II. Bento, Cléa Mara Coutinho.

CDD 336.29

Catálogo na publicação
Antonio Luis Fonseca Silva– CRB/1035
Francisco Renato Sampaio da Silva – CRB/1028

ELAYNE VELOSO ARAUJO

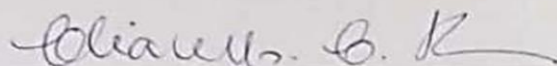
**A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE
DADOS PESSOAIS E SUA APLICAÇÃO NO ÂMBITO EMPRESARIAL.**

Artigo apresentado à Banca Examinadora do
Centro Universitário Uninovafapi, como
requisito parcial para obtenção do grau de
Bacharel em Direito.

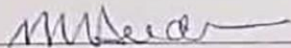
Orientadora: Prof. Dra. Cléa Mara Coutinho
Bento

Data de Aprovação: 16 / 11 / 2022

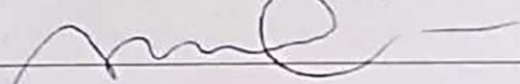
BANCA EXAMINADORA



Prof.ª Doutora em Direito Cléa Mara Coutinho Bento
Centro Universitário - UNINOVAFAPI(Orientador)



Prof.ª Doutora em Direito Marília Martins Soares de Andrade
Centro Universitário - UNINOVAFAPI(1º Examinador)



Prof.º Mestre em Direito José Augusto de Carvalho Mendes Filho
Centro Universitário - UNINOVAFAPI(2º Examinador)

AGRADECIMENTOS

Agradeço, primeiramente, a Deus e à minha família, Elza Veloso (mãe), João Wagner (pai), Evelyn Maria (irmã), Evana Mairy (tia, madrinha e mãe do coração) e aos meus avós, primos e tios pelo apoio e momentos proporcionados que foram e, ainda, são indispensáveis para me dar forças em todos os desafios desta vida. Obrigada por vocês serem minha fortaleza.

Por meio deste artigo, quero agradecer ao Centro de Ciências Jurídicas da Universidade Uninovafapi por promover um ambiente acadêmico produtivo e fértil à pesquisa. Agradeço imensamente à professora Cleá Mara pela orientação deste Trabalho de Conclusão de Curso (TCC), pela disponibilidade e dedicação, obrigada por aceitar ser minha orientadora.

Agradeço, ainda, aos amigos que cativei ao longo desse caminhar na estrada sinuosa do Direito, represento-os aqui, nos nomes da Sarah Gysele, Agnar Lohrana e do Júlio César, os quais tornaram as manhãs mais divertidas e os estudos do **Vade Mecum** mais leves. Pois, com vocês aprendi que o Direito é dinâmico e a atualização deve ser constante.

Agradeço ao meu noivo José Renato Damasceno que desde o início esteve incansavelmente ao meu lado, sendo meu lar e minha parceria mais absoluta em todos os momentos dessa jornada. Obrigada por ser o meu companheiro de todas as horas e o meu amigo preferido.

RESUMO

O presente estudo sobre “a importância da Lei geral de proteção de dados pessoais e sua aplicação no âmbito empresarial”, justificou-se pela necessidade de compreensão do direito digital, no âmbito da proteção de dados pessoais. A metodologia aplicada na pesquisa foi de revisão bibliográfica e documental, com foco na análise de dados por meio de abordagem qualitativa descritiva. Este estudo teve como objetivo verificar a aplicação efetiva da Lei 13.709/18 (Lei Geral de Proteção de Dados – LGPD) e seus desdobramentos quanto a garantia dos direitos sociais e jurídicos. Para tanto, descreveu a aplicação das novas regras da Lei Geral de Proteção de Dados no ambiente empresarial, nas relações interpessoais e jurídicas, identificando a aplicabilidade e implementação dessa lei que assegura o sigilo de dados pessoais. Revelou a urgência de adaptação das empresas que possuem seus negócios pautados em dados em investir em formas de garantir a segurança e o tratamento adequado dos dados, principalmente de seus clientes. Concluiu-se que, a instituição da LGPD foi de suma importância para o cidadão, pois assegura a confiabilidade necessária para as relações pessoais e para o desenvolvimento das atividades empresariais jurisdicionadas, no contexto de um mundo globalizado, constituindo-se contudo, como um grande desafio ao mercado empresarial, sobretudo, diante da velocidade do compartilhamento de informações decorrentes do mundo digital e redes sociais.

Palavras-chave: Proteção de dados pessoais. Empresarial. Mundo digital.

ABSTRACT

The present study about “the importance of the General Law for the Protection of Personal Data and its application in the business environment”, was justified by the need to understand the digital law, within the scope of personal data protection. The methodology applied in the research was a bibliographic and documental review, focusing on data analysis through a descriptive qualitative approach. This study aimed to verify the effective application of Law 13.709/18 (General Data Protection Law – LGPD) and its consequences regarding the guarantee of social and legal rights. To this end, it described the application of the new rules of the General Data Protection Law in the business environment, in interpersonal and legal relationships, identifying the applicability and implementation of this law that ensures the confidentiality of personal data. It revealed the urgency of adapting companies that have their business based on data to invest in ways to ensure the security and proper handling of data, especially those of their customers. It was concluded that the institution of LGPD was of paramount importance for the citizen, as it ensures the necessary reliability for personal relationships and for the development of juridical business activities, in the context of a globalized world, however, it constitutes a great challenge to the business market, especially given the speed of information sharing arising from the digital world and social networks.

Keywords: Protection of personal data. Business. Digital world.

1 INTRODUÇÃO

A tecnologia está cada vez mais presente na vida dos indivíduos, com o surgimento de novas mídias, principalmente as digitais, e a transformação de mídias antigas aparecem diversas questões sobre o uso dessas tecnologias, no que diz respeito aos serviços que são prestados à sociedade para facilitar a vida das pessoas. São inovações tecnológicas cada vez mais rápidas, abrangentes e frequentes no campo da informação, são Tecnologias de Informação e Comunicação (TICs) que afetam diretamente as relações interpessoais e empresariais, que dentro de um mundo digital e globalizado, requer parâmetros que fundamentem o uso dos caracteres de identidade e individualidade das pessoas, daí a importância da criação e implementação da Lei Geral de Proteção de Dados (LGPD), especialmente no âmbito do empresarial.

A Lei nº 13.709, de 14 de agosto de 2018, denominada de Lei Geral de Proteção de Dados Pessoais (LGPD) foi criada para regulamentar a coleta e o uso de dados pessoais por empresas. Estas tiveram que se adaptar à era digital, uma vez que precisaram redefinir a relação com aqueles que utilizam e consomem seus serviços, no que se refere ao banco de dados pessoais. Para tanto, foi necessário regimentar o uso de informações das pessoas para que as mesmas não tenham seus dados usados ou comercializados indevidamente, pondo em risco os princípios de liberdade e privacidade.

A nova legislação tem como objetivo garantir a necessária proteção à privacidade dos indivíduos e verificar se está de acordo com o novo paradigma proposto pela modernidade advinda do progresso tecnológico, que impactam e transformam a vida do ser humano, trazendo uma nova forma de viver e estar em sociedade, seja ele de qualquer classe social e nível intelectual.

Nesse aspecto, um dos maiores avanços recentes na comunicação humana veio com a popularização da internet e a enorme revolução tecnológica que trouxe especialmente no campo da comunicação. O que antes tinha acesso limitado e propósitos específicos tornou-se algo disponível à massa, com algumas exceções, teve uma abrangência social significativa. Assim, trabalho, estudo, comunicação, lazer e negócios movimentaram-se para garantir o acesso para todas as gerações, jovens, crianças, adultos e idosos não podem imaginar um mundo sem internet.

Desse modo, a adequação de ferramentas convenientes, como mecanismos de busca, enciclopédias eletrônicas, sites de entretenimento e relacionamento, serviços de

streaming e redes sociais, são modalidades digitais que possibilitaram a criação de ambientes virtuais que tornaram possíveis a apropriação de informações e atividades, que vão desde as questões mais gerais da vivência das pessoas, até questões mais específicas e privativas e, seja em qualquer uma delas, fez-se necessário, regulamentar, ou até mesmo limitar o acesso a algumas informais, especialmente, aquelas mais individuais.

As empresas, como um setor fundamental à economia, ao trabalho e ao desenvolvimento social, têm se apropriado dessas inovações e novas interações sociais, como componentes-chave e executores de múltiplas transações econômicas. É um novo fazer empresarial, mais célere, mais dinâmico e menos analógico, precisou se adaptar especialmente, no que diz respeito à sua relação com funcionários, clientes e fornecedores. Para isso, atualizou arquivos dos dados pessoais de clientes, dando a eles um tratamento baseado em leis que regem a proteção, privacidade e segurança das pessoas.

Nesse contexto, a revolução tecnológica, no campo da informação, trouxe muitos avanços e facilidades para as pessoas, mas também, a necessidade de impor restrições éticas à coleta, uso e distribuição de informações pessoais. Nos últimos anos, os bancos de dados eletrônicos se expandiram muito, a coleta de dados acontece o tempo todo, tanto on-line quanto off-line, e ganha poder de processamento e armazenamento quase ilimitado. Daí, a preocupação com a privacidade individual não é por acaso, sendo assim, o Direito assume uma tarefa importante devido à complexidade da questão e de todas as relações jurídicas que decorrem desse princípio.

Dessa feita, a problemática investigada, neste estudo, consiste em verificar os desafios impostos pela LGPD às empresas e, se a nova normativa é passível de execução (cumprimento), de forma que o presente artigo analisa a LGPD, verificando os avanços, desafios e impactos que permeiam a sua aplicação no âmbito empresarial.

O estudo será realizado por meio de uma revisão bibliográfica e documental e fornecerá uma breve revisão da história da revolução da tecnologia e da informação a partir de uma perspectiva jurídica.

Sabe-se que os desafios são variados, de forma que o presente estudo precisa compreender o contexto, que envolve o cenário de criação da Lei Geral de Proteção de Dados pessoais, para em seguida apresentar a importância da presente Lei na proteção de dados pessoais, bem como os instrumentos tecnológicos utilizados pelas empresas para execução da nova normativa; a questão do vazamento de dados pessoais e suas principais consequências e o ponto de encontro com as redes sociais, para ao final, a título de considerações finais, apresentar os principais resultados encontrados na pesquisa.

2 A IMPORTÂNCIA DA LGPD PARA PROTEÇÃO DOS DADOS PESSOAIS

A necessidade de uma proteção jurídica eficiente das informações pessoais dos cidadãos brasileiros ganhou força com o desenvolvimento da tecnologia da informação, diante da grande facilidade de acesso e divulgação de informações pessoais e a grande rotatividade dessas informações.

A compreensão de que as informações sobre as atividades do usuário do sistema digital se tornaram ‘mercadorias’ de fácil acesso e transferência, especificamente no aspecto mercadológico, em que, por meio do rastreamento dos perfis das pessoas, coleta-se informações preciosas sobre elas, com o intuito de direcionar anúncios, campanhas, produtos e serviços específicos aos usuários, independentemente de seu consentimento ou solicitação, isso ocorre de forma descontrolada, regida por algoritmos.

Dessa feita, a LGPD surge trazendo uma série de protocolos de boas práticas e limites para proteção desses dados pessoais, objetivando que sejam negociados, como mercadorias ou serviços, em detrimento da privacidade dos seus titulares.

2.1 O uso de dados pessoais na produção de anúncios

A partir da coleta das informações pessoais, é possível se fazer manobras de marketing, atraindo a atenção dos usuários para os produtos expostos pela internet, que chegam à sua página de rede social ou privada, porém, os usuários não estão fornecendo seus dados pessoais para que, esses produtos cheguem até ele. Eis uma questão que se justifica pela utilização de instrumentos de captação de dados: aplicativos de comida; redes sociais diversas; sites que pedem registro/cookies; bancos digitais; aplicativos de conversa; jogos on-line.

Essas situações são muito comuns, um exemplo disso é quando ao pesquisar um produto pela internet, os dados do usuário ficam registrados e ficam disponíveis para uso, assim, as empresas que disponibilizam serviços e produtos captam automaticamente esses dados e fazem uso deles na rede social do próprio usuário. Isso acontece porque normalmente os smartphones ficam conectados a uma conta pessoal, a qual possui todos os dados pessoais do indivíduo (CARDOSO, 2021).

Foi, inicialmente, como resposta a esse uso arbitrário das informações dos usuários das redes sociais que surgiu a Lei Geral de Proteção de Dados, que, apesar de ser recente, tornou-se

indispensável à sociedade, por proporcionar a utilização das mídias digitais em rede, maior segurança aos seus usuários, para garantir a privacidade das pessoas e assegurar que a utilização dos seus dados tenham seu conhecimento e consentimento. Por outro lado, possibilite às empresas de produtos e serviços a utilização legal dos dados das pessoas, seguindo, os termos da lei, sob pena de responsabilização e punição prevista por ela.

2.2 As políticas das empresas de smartphones e computadores com segurança dos dados pessoais

De acordo com a Secretaria Especial de Desburocratização, Gestão e Governo Digital foi emitido um Guia de Requisitos Mínimos de Segurança e Privacidade para Aplicativos Móveis de acordo com Lei Geral de Proteção de Dados Pessoais (LGPD), esse Guia é baseado no artigo 46 da LGPD (2021, p. 05) e tem o propósito de fomentar orientações básicas aos desenvolvedores de aplicativos da Administração Pública Federal sobre o desenvolvimento seguro dos aplicativos móveis.

O referido Guia tem a função de orientar as empresas de como devem trabalhar com o nível mínimo de proteção aos dados pessoais dos usuários por meio do desenvolvimento de seus aplicativos. Ainda assim, os dados dos usuários ainda ficam vulneráveis ao vazamento no banco de dados e ao acesso de hacker que buscam por informação das pessoas para diversos crimes.

O Guia oferece oito estratégias de design de privacidade e suas respectivas táticas de proteção de dados que são descritas a seguir com exemplos de como podem ser aplicadas no desenvolvimento, (1) Minimizar: Limitar ao máximo o processamento de dados pessoais. (2) Segregar: Evitar a correlação de dados pessoais, separando o processamento lógico e físico. (3) Abstraírem: Limitar ao máximo possível o detalhamento (granularidade e especificidade) dos dados pessoais que estão sendo processados. (4) Ocultar: Proteger dados pessoais ou torná-los desvinculáveis ou inobserváveis. (5) Evitar que dados pessoais se tornem públicos. Evitar a exposição de dados pessoais restringindo o acesso ou ocultando sua própria existência. (6) Informar: Fornecer aos titulares dos dados informações adequadas sobre quais dados pessoais são processados, como são processados e para qual finalidade. (7) Impor: Comprometer-se com a privacidade no processamento de dados pessoais e se fazer cumpri-la. (8) Demonstrar: Fornecer evidências de que você processa dados pessoais seguindo as melhores práticas de privacidade (GUEDES *et al*, 2021).

3 LEI GERAL DE PROTEÇÃO DE DADOS NA PRÁTICA

A eficácia de qualquer lei torna-se visível a partir da sua aceitação e aplicabilidade, com a LGPD não é diferente, sabendo que ela foi criada para suprir várias necessidades dos usuários da rede digital, e para implantar adequadamente e manter o controle exigido pela legislação. Por mais que seja um processo complexo, é preciso adotar procedimentos adequados e legais para o seu cumprimento de fato e de direito. Como também, fazer a fiscalização e monitoramento por parte do poder público e jurídico.

O primeiro passo é organizar um monitoramento e cumprimento da referida Lei de acordo com legislação, outro, é buscar formas de conectar ações diretamente com o que a Lei estabelece. Em relação ao uso de dados pessoais, pelas empresas, é necessário mapear os principais fluxos desses dados, elaborar planilhas que ilustram o caminho percorrido pelo dado pessoal dentro da empresa, incluindo os processos e procedimentos pelos quais transita, ou seja, qual a origem, a base legal que respalda o tratamento desse dado pessoal, o nível de segurança da base de dados a qual o dado pertence, entre outras informações necessárias para a análise de vulnerabilidades técnicas e jurídicas.

No Brasil, para atender aos requisitos de adequação à LGPD é imprescindível realizar o mapeamento e monitoramento de dados, uma vez que é esse documento que dará um panorama geral de como a empresa está lidando com a questão da privacidade e segurança da informação.

Um dos principais objetivos do mapeamento de dados é diagnosticar a forma como a empresa lida com a privacidade e a segurança da informação de seus clientes, colaboradores e parceiros terceirizados, cumprindo, a exigência constante no artigo 37 da LGPD, que estipula a função do controlador e do operador na manutenção do registro das operações de tratamento de dados pessoais que realizam.

Identificar e priorizar riscos de privacidade, certamente é o passo mais importante para colocar a LGPD na prática, contudo, uma das atividades mais desgastante de todo o processo de adequação da Lei. Vale ressaltar que mapear corretamente os fluxos de tratamento de dados pessoais não é tarefa fácil, pois requer organização, conhecimento, engajamento de várias áreas da empresa, como também, o estabelecimento de um esforço cooperativo, contando com a participação de partes distintas. Sobre isso, seguem algumas ideias sobre como organizar um mapeamento de dados, segundo (BRANDÃO, 2021).

Tipo de Dados	Categorias de dados trafegadas nesse fluxo (ex: cadastrais, transacionais, especiais, sensíveis, trabalhistas etc.).
Volume de Dados	O volume de dados trafegados nesse fluxo e a frequência desse tráfego (ex: online, diária, semanal, mensal etc.).
Etapas do fluxo de dados	Descrição das etapas de tratamento do fluxo: coleta, armazenagem, sanitização, enriquecimento, processamento, segmentação, inferências, transferências, descarte.
Tecnologias	Apontar no mapeamento de dados as principais tecnologias utilizadas nesse fluxo de dados (ex: sistemas, aplicações, bancos de dados que suportam o fluxo etc.).
Locais de Armazenamento	Indicar os locais onde o dado é coletado, armazenado, tratado ou processado. Nesse momento, deve-se indicar se é internamente ou externamente.
Origem dos Dados	Indicar as principais origens dos dados (entradas) e canais de captura de dados (ex: site, aplicativos, estabelecimentos físicos, SAC, parceiros, empresas coligadas).
Campanhas de Marketing	Informar como os dados pessoais são tratados visando campanhas de marketing. Indicar também no mapeamento de dados quais os tipos de dados pessoais são utilizados.
Compartilhamento de dados com parceiros	Indicar os principais parceiros com os quais os dados são compartilhados – parceiros de negócio ou parceiros de tecnologia/dados (ex: slack, escritório de contabilidade terceirizado, emissor de Nfe etc.).
Empresas coligadas	Indicar no mapeamento de dados às empresas coligadas do grupo econômico cujos dados são compartilhados entre si.
Localidades do tratamento	Indicar os países, estados e localidade onde sua empresa possui atividade.
Transferência Internacional de dados	Plataformas de cloud (ex: amazon aws, Microsoft azure, Google cloud); Data centers terceirizados; Softwares terceirizados; Transferência de dados pessoais para a sede da empresa no exterior.
Base legal	Indicar a base legal para realização do tratamento de dados referente ao fluxo descrito.
Política de Privacidade	A Política de privacidade referente ao fluxo descrito está atualizada e atende aos requisitos da LGPD? Ela está disponível em todas as fases da coleta de dados?

3.1 Vazamentos de dados e suas consequências

A LGPD rege sobre o vazamento de dados pessoais de usuários, afirmando que a partir do momento em que um usuário de internet compartilha seus dados pessoais seja por uma informação via e-mail, rede social ou por uma compra que realiza, ele já se torna vulnerável ao vazamento de seus dados, com isso confirma a vulnerabilidade a que está exposto, o que confirma a sua desvantagem na relação ao sistema em que acessa. Esse é

problema que a lei está para resolver, amparando a parte mais frágil da relação, no caso, o usuário.

Por isso, tem-se a Lei que abrange esse conteúdo e buscar tratamento como no artigo 7, que fala sobre o tratamento de dados pessoais. De acordo com a Lei nº 13.709, de 14 de agosto de 2018:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

- I – mediante o fornecimento de consentimento pelo titular;
- II – para o cumprimento de obrigação legal ou regulatória pelo controlador;
- III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
- IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- VIII – para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
- VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019);
- IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
- X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (BRASIL, 2018).

O setor empresarial tem a possibilidade de adquirir as melhores tecnologias de segurança, pode também, oferecer um treinamento excelente aos seus funcionários detentores dos segredos de seus usuários, podem até mesmo contratar seguranças para proteger as empresas, mas ainda assim, os dados dos seus clientes estão vulneráveis e podem ter seus dados vazados.

Segundo Mitnick (2003), os usuários do sistema da rede digital, podem adotar as melhores práticas de segurança recomendadas pelos melhores especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança, ainda assim, estarão completamente vulneráveis.

O fator humano ainda é o responsável pela grande parte dos vazamentos e percas das informações, seja por descontentamento dos usuários com a organização, falta de

conhecimento e por técnicas de Engenharia Social (MITNICK, 2003).

As consequências do vazamento de dados são inúmeras, porém, algumas causam mais prejuízos aos usuários do que outras, como por exemplo a invasão à contas bancárias e fraudes financeiras, isso acontece porque muitas vezes, as credenciais de acesso vazadas podem facilitar a ação de criminosos em um ataque de *phishing*. Unidas a outros dados sensíveis, podem ser o suficiente para ciber criminosos conseguirem efetuar fraudes bancárias em nome das empresas, e ainda fazerem extorsão e chantagem com as pessoas.

Um golpe virtual em alta no país, e que também é um dos maiores causadores de vazamento de dados, é o ataque de *ransomware*. Nele, por meio de um programa malicioso e perigoso, o cibercriminoso bloqueia o acesso aos dispositivos e às informações dos aparelhos infectados, tornando-os de fácil manipulação. “A Lei Geral de Proteção de Dados define regras para o uso, proteção e transferência de dados pessoais coletados pelas empresas, independentemente de seu segmento de atuação, porte ou faturamento. Os negócios que registram informações dos clientes sem sua autorização, ou que os repassem, armazenem sem necessidade comprovada, ou que tenham esses dados vazados de alguma forma também estará sujeitos aqui às penalidades da lei, que variam de advertências a multas de até R\$ 50 milhões por ocorrência”, adverte Victor Perego, especialista em Riscos Cibernéticos da AIG.

Portanto a LGPD, no ano de 2022 ganhou status de direito fundamental na Constituição Federal, assim, o cumprimento das determinações estabelecidas por ela, podendo resultar em sanções administrativas diversas, como: advertência, multa simples, multa diária, publicização da infração, bloqueio dos dados pessoais e eliminação dos dados pessoais.

3.2 Vazamentos de dados empresariais no Brasil

Na realidade atual, é muito comum a disponibilização de dados pessoais dos usuários da internet e as implicações que promovem nas relações entre as pessoas e empresas. A seguir, alguns exemplos para ilustrar esse fato.

Em dezembro de 2017, cerca de dois milhões de dados pessoais de clientes de uma determinada empresa (Netshoes) foram disponibilizados em um site de compartilhamento de arquivos. As informações comprometidas não foram poucas, como nome completo, CPF, e-mail, data de nascimento e histórico de compras no e-commerce. A empresa só confirmou o vazamento desses dados em fevereiro de 2018.

Para não comprometer a imagem da empresa e evitar uma ação jurídica coletiva, a referida empresa conseguiu fechar um acordo extrajudicial com o Ministério Público do Distrito Federal e Territórios (MPDFT) e pagar R\$ 500 mil como indenização, valor que será recolhido ao Fundo de Defesa de Direitos Difusos. Além do pagamento, a empresa citada (Netshoes) assinou um Termo de Ajustamento de Conduta (TAC), pelo o qual se compromete a implementar medidas adicionais de segurança a seu Programa de Proteção de Dados, pois, na lei há confirmação de que é cobrado um valor devido caso tenha infrações graves ou divulgação de dados sem autorização. De acordo com a Lei nº 13.709, de 14 de agosto de 2018:

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento. (BRASIL, 2018).

Caso descumpra essas medidas, a empresa está sujeita a uma ação cível de reparação pelos danos morais coletivos no valor de R\$ 10 (dez) milhões, além de um processo de R\$ 85 (oitenta e cinco) milhões por danos patrimoniais.

A C&A foi vítima de um ciber ataque em agosto de 2018, que resultou em um vazamento de dados tão grande quanto o da Netshoes. Estima-se que mais de 2 milhões de clientes possam ter sido afetados pela invasão de hackers ao sistema dos cartões de vale-presente da empresa. Os dados violados incluem CPF do comprador, e-mail, número do cartão e valor da compra. O caso está sendo investigado pela Comissão de Proteção de Dados Pessoais do MPDFT.

O Banco Inter após negar a possibilidade de um vazamento de dados durante meses, um dos maiores bancos digitais do país, acabou confirmando que informações de cerca de 20 (vinte) mil dos seus correntistas foram violadas. Em dezembro de 2018, a empresa fechou um acordo com o MPDFT para o pagamento de R\$ 1 milhão destinado a instituições públicas de combate a crimes cibernéticos e R\$ 500 (quinhentos) mil destinados a instituições de caridade.

Para evitar consequências como essas e proteger os dados de ataques cada vez mais frequentes, as empresas brasileiras precisam priorizar soluções de segurança em toda sua estrutura – da nuvem aos aplicativos. Além disso, a conscientização das equipes de TI e dos funcionários no geral, sobre segurança digital, é um ponto que merece atenção redobrada.

Como esses ataques cibernéticos estão cada vez mais recorrentes, é necessário que as empresas priorizem a segurança buscando soluções e conscientizando as pessoas, principalmente as equipes de TI e os funcionários em geral para assim oferecer aos seus usuários um sistema cada vez mais seguro e confiável.

Esses exemplos mostram que tanto as pessoas, quanto as empresas, estão vulneráveis ao vazamento de seus dados e ao risco do uso indevido dos mesmos. Isso comprova a importância da LGPD e outros instrumentos legais para garantir o acesso e o direito à internet pelas pessoas e pelas empresas, como também, para regulamentar o seu uso de maneira legal e responsável, de modo que esse mundo digital e tecnológico sirva para facilitar a vida das pessoas e o funcionamento e desenvolvimento das empresas.

3.3 A Lei Geral da Proteção de Dados e as Redes Sociais

É inegável a frequente presença das redes sociais na vida das pessoas de forma contínua, basta ver o quanto de informações pessoais, dados privados ficam disponíveis às outras pessoas. Pode-se observar que, à medida que os usuários movimentam suas redes sociais, formulam seus perfis sociais, disponibilizando informações e dados pessoais, na busca de interações com outras pessoas cadastradas em determinada rede social.

Nesse cenário, as redes sociais se configuram como ambientes propícios a uma rápida conexão e troca de informações entre os seus usuários, em contrapartida, são facilmente visíveis e acessíveis. No entanto, é nessa conectividade virtual que surge a fragilidade da privacidade do indivíduo, um direito da pessoa muito difícil de garantir totalmente, pois ao passo que as redes sociais possibilitam a conexão e proximidade entre seus usuários, torna-se também um viés para pessoas oportunistas se apropriarem de informações para uso inadequado.

Embora muitas pessoas usem as redes sociais como entretenimento, outras vêm nela, uma possibilidade de mercado, compra e venda, com a presença de um consumidor e de um fornecedor. Assim, as relações comerciais se estabelecem a partir delas e da necessidade de regulamentar essa relação, definindo o papel de cada um.

As cláusulas contratuais das redes sociais, são definidas sem uma negociação equilibrada entre as partes do contrato, tem-se as cláusulas instituídas pelas redes sociais que precisam estar em consonância com o que estabelece o direito dos indivíduos conforme os diplomas legais, a Lei Geral de Proteção de Dados Pessoais, de modo a amparar o titular de dados que, “pelo simples ato de apertar o botão de aceitação” (MARTINS, 2016, p. 131),

passa a se configurar como usuário e consumidor, estando em uma condição de vulnerabilidade.

CONSIDERAÇÕES FINAIS

Do estudo, revelou-se a urgência de adaptação das empresas que possuem seus negócios pautados em dados em investir em formas de garantir a segurança e o tratamento adequado dos dados, principalmente de seus clientes.

A LGPD proporcionou significativas alterações no que tange à proteção de dados pessoais, o que demanda, tratando-se de um direito fundamental, uma rápida adequação das redes sociais às novas obrigações sociais e jurídicas, pois o que se busca deve ser realmente proteger os indivíduos que se encontram por trás dos dados pessoais.

Pela conformidade da Lei Geral de Proteção de Dados Pessoais, conclui-se que existe um grande desafio para as organizações, em especial o Poder Público, que via de regra, detém grande volume de dados pessoais sob sua custódia inerentes à condução e desenvolvimento de suas atividades, o tratamento destinado a esses dados requer responsabilidade, sigilo e proteção.

Nesse cenário, a aplicação prática da LGPD depende de inúmeros fatores, quais sejam humanos, tecnológicos, normativos, entre outros. Percebe-se que todo o contexto de busca por conformidade à Lei está intrinsicamente relacionado com a segurança da informação e, é por meio dela, que o Poder Público deve construir o alicerce para programar o controle de seu funcionamento, com políticas regimentais, processos, procedimentos e estrutura organizacional, que uma vez estabelecidos, devem ser monitorados, analisados criticamente e melhorados, quando necessário, para manter o nível adequado de proteção dos dados pessoais contra ameaças, vulnerabilidades, riscos e ataques, garantindo assim, a tríade confidencialidade, integridade e disponibilidade dos dados.

O ponto central desse artigo pautou-se na análise de princípios da Lei que se concentrou em observar os aspectos mais importantes da LGPD, a partir do comportamento do setor empresarial, que respondam aos desafios de um mundo digital hiper conectado baseado em uma economia de fluxo incessante de dados, atentos às inovações trazidas pela modernidade e à ocupação das ferramentas tecnológicas e digitais.

A interpretação da LGPD não pode ser realizada sem a observação de seus princípios norteadores, sendo essencial e necessário entender a forma com a qual a privacidade alterou-se diante da sociedade informacional, moldando-se para dar ao indivíduo o poder de controle

sobre a coleta e tratamento de seus dados pessoais.

Observada a forma comercial com a qual os dados pessoais são tratados atualmente no Brasil, a LGPD poderá barrar diversas ilegalidades, como a forma abusiva de publicidade direcionada e conservada ao binômio de adequação e necessidade para coleta e tratamento de dados. A Lei de Proteção de Dados Pessoais, o Marco Civil da Internet são produtos advidos de demandas sociais, vêm direto da necessidade de uma área do direito que ainda tem muito a crescer e se transformar.

Resultantes de uma preocupação fundamentada, apesar de recentes, são essenciais para a construção de respeito à identidade e privacidade dos indivíduos e já estão preparadas para transformar a ciência jurídica de modo a aperfeiçoá-la para que produza resultados reais e pertinentes com um mundo cada vez mais conectado e complexo.

REFERÊNCIAS

- BEZERRA, M. L. A. **A lei 13.709/18 e os Novos Desafios da Proteção de Dados Pessoais e Identidade**. 2019. Disponível em: <<https://repositorio.ufpe.br/handle/123456789/36323>>. Acesso em: 02 out. 2022.
- BRANDÃO, G. **Direito Digital, LGPD, Privacidade & Proteção de Dados**. 2021. Disponível em: <<https://blconsultoriadigital.com.br/mapeamento-de-dados/#%3A~%3Atext%3DIndicar%20os%20locais%20onde%20o%2Cse%20%C3%A9%20interamente%20ou%20externamente.%26text%3DIndicar%20as%20principais%20origens%20dos%20C%2C%20empresas%20coligadas%2C%20etc>>. Acesso em: 19 out. 2022.
- BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 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: <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337> Acesso em: 01 out. 2022.
- CARDOSO, O. V. **Consentimento Válido na Lei Geral de Proteção de Dados, Informações Adequadas e Envio de Propagandas Online**, Jusbrasil, [S.L], 2021. Disponível em: <<https://ovcardoso.jusbrasil.com.br/artigos/1223042324/consentimento-valido-na-lei-geral-de-protecao-de-dados-informacoes-adequadas-e-envio-de-propagandas-online>>. Acesso em: 19 out. 2022
- FORUM, I. **6 consequências devastadoras de um vazamento de dados corporativos**. 2021. Disponível em: <<https://itforum.com.br/noticias/6-consequencias-devastadoras-de-um-vazamento-de-dados-corporativos/>> Acesso em: 25 set. 2022.
- GOMES, H. D. S. **Lei Geral de Proteção de Dados LGPD**, Segurança de dados. 2019. Disponível em: <<http://repositorio.fdv.br:8080/handle/fdv/1327>> Acesso em: 01 out. 2022.
- GUEDES, P. R. N. *et al.* **Lei geral de proteção de dados pessoais (lgpd)**. Guia de requisitos mínimos de segurança e privacidade para aplicativos móveis, Ministerio da economia, Brasília, 2021, Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_seguranca_apps.pdf/view>. Acesso em: 04 nov. 2022.
- MARTINS, G. M. **Contratos Eletrônicos de Consumo**. 3. ed. São Paulo: Atlas, 2016.
- MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar**. São Paulo: Pearson Makron Books, 2003. Disponível em: <<https://bibliopedra.files.wordpress.com/2015/09/arte-de-invadir-a-kevin-mitnick.pdf>>. Acesso em: 08 out. 2022.
- PANEK, T. C. L. **Lei geral de proteção de dados n. 13.709/2018: uma análise dos Principais aspectos e do conceito de privacidade na sociedade**. Curitiba, 2019. Disponível em: <<https://acervodigital.ufpr.br/bitstream/handle/1884/68114/TCC%20FINAL%20-%20lgpd.pdf?isAllowed=y&sequence=1>>. Acesso em: 01 out. 2022.
- PIURCOSKY, P. F *et al.* **A lei geral de proteção de dados pessoais nas empresas brasileiras: uma análise de múltiplos casos**.

2019. Disponível em: <<https://editorial.konradlorenz.edu.co/2019/06/a-lei-geral-de-protecao-de-dados-pessoais-em-empresas-brasileiras-uma-analise-de-multiplos-casos.html>>. Acesso em: 17 out. 2022.

ROTTA, M. **LGPD na prática: 7 passos para implementar na sua empresa.** [S.L] 2022. Disponível em: <<https://www.gepcompliance.com.br/blog/lgpd-na-pratica-7-passos-para-implementar-na-sua-empresa/>> Acesso em: 18 out. 2022.

SANTOS, A. **Entenda como a manipulação de dados pessoais está presente no dia a dia da pessoas.** 2020. Disponível em: <<https://www.contabeis.com.br/noticias/45014/entenda-como-a-manipulacao-de-dados-pessoais-esta-presente-no-dia-a-dia-das-pessoas/#:~:text=S%C3%A3o%20alguns%20exemplos%2C%20cotidianos%2C%20de,aplicativos%20de%20conversa%3B%20jogos%20online>>. Acesso em: 04 nov. 2022.

SOUZA, D. B. F. **Usuário, o elo mais fraco da segurança da informação.** Revista Scientia Alpha, [S.L] 2022. Disponível em: <<https://revista.alfaumarama.edu.br/index.php/rsa/article/view/34>> Acesso em: 20 set. 2022.

TEIXEIRA, C. G. **O Papel social da lei geral de proteção de dados no Brasil.** Araranguá SC, 2020. Disponível em: <<https://repositorio.animaeducacao.com.br/bitstream/ANIMA/7514/1/Monografia%20Guilherme%20Cardoso%20Teixeira.pdf>>. Acesso em: 10 out. 2022.

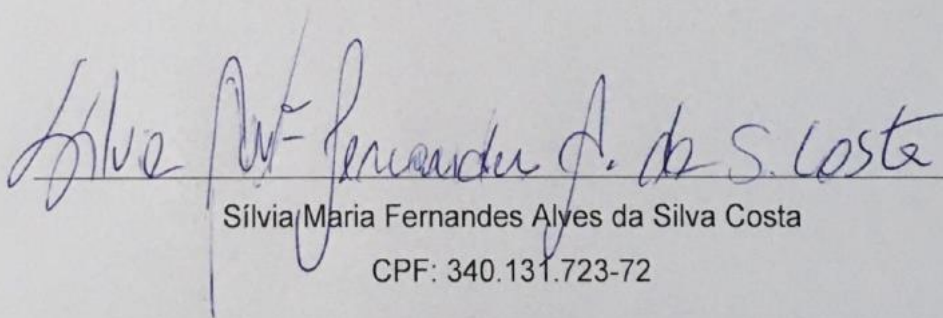
VASCONCELOS, R. C.; SALIB, L. L. M. **Lei Geral de Proteção de Dados Pessoais: Desafios e impactos para o Poder Público.** [S.L], 2021. Disponível em: <https://lgpd.tcero.tc.br/wp-content/uploads/2021/07/TCC-Charles-Roge%CC%81rio-Vasconcelos_TCE-RO.pdf>. Acesso em: 01 out. 2022.

WALL, S. S. T. **Vazamento de dados e suas consequências para empresas.** 2019. Disponível em: <<https://www.softwall.com.br/blog/vazamento-de-dados-e-suas-consequencias-para-empresas/>> Acesso em: 28 set. 2022.

DECLARAÇÃO DE REVISÃO ORTOGRÁFICA

Eu, Sílvia Maria Fernandes Alves da Silva Costa, doutora em Letras pela Universidade Federal da Paraíba, declaro para o Centro Universitário UNINOVAFAPÍ que revisei o Trabalho de Conclusão de Curso de Bacharelado em Direito intitulado "A importância da Lei geral de proteção de dados pessoais e sua aplicação no âmbito empresarial", da aluna Elayne Veloso Araujo. Declaro ainda que o presente trabalho se encontra de acordo com as normas ortográficas e gramaticais vigentes.

Teresina, 16 de novembro de 2022.



Sílvia Maria Fernandes Alves da Silva Costa
CPF: 340.131.723-72