ISSN 1981-1179

Id on Line. Revista de Psicologia

DOI: 10.14295/idonline.v18i72.4042

Artigo de Revisão

Incidentes de Segurança: Regulação e Prática de Vazamento de Dados Pessoais Frente à LGPD

Heideivirlandia Leite Galvão[1]; Alyne Leite de Oliveira[2]; Bethsaida de Sá Barreto Diaz Gino[3]; Hudson Josino Viana[4]; Francisco Gledison Lima Araújo[5]; Noélia Marques Silva Benevinuto[6]; Denis Leonardo Ferraz da Silva[7]

Resumo: Nos dias atuais, apesar do avanço tecnológico, ainda se fala muito em vazamento de dados pessoais e suas respectivas consequências, sejam elas prejuízos emocionais ou financeiros. Este fenômeno caracteriza-se como um incidente de segurança no qual dados pessoais ou informações sensíveis são expostos publicamente ou transferidos para terceiros sem consentimento do titular. Diante desse cenário, no qual a preservação dos dados é crucial para as organizações empresariais, a Lei nº 13.709/2018 foi sancionada para proteger os direitos fundamentais de liberdade e privacidade de cada cidadão, estabelecendo que os responsáveis pelo tratamento dos dados respondam por incidentes, promovendo assim um ambiente de segurança jurídica. Contudo, questiona-se por que ainda há uma grande incidência de vazamentos de dados pessoais mesmo após a vigência dessa lei? Para abordar essa questão, optou-se por uma pesquisa de natureza puramente bibliográfica, investigando a frequência crescente de vazamentos de dados e a aplicação da Lei 13.709/2018, juntamente com sua regulamentação sobre o tratamento das informações dos usuários. Com base nas pesquisas realizadas e nos estudos de casos recentes envolvendo vazamentos de dados, é evidente o transtorno causado pela disseminação de informações pessoais. Portanto, ao utilizar aplicativos e softwares, é crucial agir com cautela, desde o cadastro em aplicativos de compras até a navegação em sites de pesquisa e lojas virtuais, entre outros.

Palavras-chave: Vazamento de dados. Cibercrime. Internet. Dados pessoais.

[1] Estudante, graduada em Direito pelo Centro Universitário Doutor Leão Sampaio. vih.galvao2@gmail.com.
[2] Professora dos Cursos de Administração e Direito do Centro Universitário Doutor Leão Sampaio, Mestranda em Administração pela Universidade Federal do Cariri. alyneoliveira@leaosampaio.edu.br.
[3] Professora do Curso de Direito da Universidade Regional do Cariri, Mestra em Direito da Empresa e dos Negócios pela Universidade do Vale do Rio dos Sinos. bethsaida.barreto@urca.br.
[4] Professor dos Cursos de Administração, Sistema de Informação, Mecânica e Eletrotécnica do Instituto Federal de Educação, Ciência e Tecnologia do Ceará- IFCE, Especialista em Controladoria e Auditoria pelo Centro Universitário Vale do Salgado. hudson.josino@gmail.com.
[5] Professor do Curso de Direito do Centro Universitário Doutor Leão Sampaio, Especialista em Direito Digital e Inteligência Artificial. gledisonaraujo@vestrasolution.com.
[6] Professora do Curso de Administração do Centro Universitário Doutor Leão Sampaio, Especialista em Administração, Finanças e Marketing. Marques.noelia@gmail.com.
[7] Delegado de Polícia Civil do Estado do Ceará, Mestre em Direito da Empresa e dos Negócios pela Universidade do Vale do Rio dos Sinos. denisleonardof@hotmail.com.

Security Incidents: Regulation and Practice of Personal Data Leakage in Light of the LGPD

Abstract: Nowadays, despite technological advances, there is still much talk about personal data leaks and their respective consequences, whether emotional or financial losses. This phenomenon is characterized as a security incident in which personal data or sensitive information is publicly exposed or transferred to third parties without the consent of the holder. Given this scenario, in which data preservation is crucial for business organizations, Law No. 13,709/2018 was enacted to protect the fundamental rights of freedom and privacy of each citizen, establishing that those responsible for data processing are liable for incidents, thus promoting an environment of legal security. However, the question is why there is still a high incidence of personal data leaks even after this law came into effect? To address this issue, we opted for bibliographical research, investigating the increasing frequency of data leaks and the application of Law 13.709/2018, together with its regulations on the treatment of user information. Based on the research carried out and recent case studies involving data leaks, the disruption caused by the dissemination of personal information is evident. Therefore, when using applications and software, it is crucial to act with caution, from registering on shopping applications to browsing search sites and online stores, among others.

Keywords: Data leak. Cybercrime. Internet. Personal data.

Introdução

Na contemporaneidade, percebe-se que, apesar do avanço e evolução tecnológica, ainda se fala muito na ocorrência de vazamento de dados e suas respectivas consequências, sejam elas prejuízos emocionais ou financeiros. O vazamento de informações caracteriza-se como incidente de segurança no qual dados pessoais, como nome completo, CPF, RG, entre outros, ou informações sensíveis, como origem racial, étnica, religião, entre outras, são expostos publicamente ou transferidos para terceiros sem o consentimento do titular. Essa exposição indevida ocorre devido à popularização dos meios e plataformas digitais.

Diante do exposto, pode-se inferir a importância de entender a temática e sua funcionalidade para identificar ferramentas que previnam a disseminação e propagação do cibercrime, visto que a criminalidade também migra para o mundo virtual, algo ainda ignorado por muitos usuários.

Com o advento da quarta revolução industrial e a digitalização crescente de diversos meios, o uso de plataformas digitais aumenta principalmente em interações sociais e profissionais. Contudo, apesar dos benefícios que os serviços online oferecem, os usuários

tornam-se mais vulneráveis ao terem seus dados coletados por sistemas variados, seja ao cadastrarem-se em redes sociais, realizar compras remotas ou acessar sites que requerem pré-cadastro.

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018 - foi criada para adaptar as empresas ao tratamento adequado dos dados dos usuários, protegendo os direitos fundamentais de liberdade e privacidade de cada cidadão. Esta legislação impõe que os responsáveis pelo tratamento (controladores e operadores) sejam responsabilizados por incidentes, promovendo um ambiente de segurança jurídica.

A estrutura da referida lei, disciplina e orienta as Pessoas de direito público e privado, no que tange ao tratamento dos dados, bem como na importância de adequar-se ao novo patamar da era digital. Diante deste cenário, surge a seguinte pergunta: apesar da vigência da lei nº13.709/2018, e a sua orientação quando a devida adequação das organizações na sua aplicabilidade, por que ainda há uma grande ocorrência de crimes de vazamento de dados pessoais?

O presente estudo, busca analisar os fatores que contribuem para a incidência de vazamento de dados pessoais, mesmo com a vigência da lei 13.709/2018. Para o alcance de tal objetivo, se faz necessário: Apontar a influência da Lei Geral de Proteção de Dados- LGPD na minimização de vazamento de dados; verificar o nível de segurança de dados lançados nas diversas plataformas digitais; apresentar uma abordagem histórica quanto a evolução e uso das tecnologias e verificar como ocorre a responsabilização em casos de vazamento de dados.

Diante do cenário atual, observa-se um desafio significativo para o legislativo em acompanhar os frequentes casos de cibercrimes virtuais, com os infratores constantemente aprimorando suas técnicas. Assim, mesmo com leis que regulam o tratamento de dados pessoais, há uma demanda contínua para que empresas privadas e a Administração Pública se adaptem aos requisitos necessários para prevenir incidentes de segurança. Portanto, este estudo contribui para as discussões acadêmicas e pode ajudar a disseminar a importância do tratamento adequado dos dados dos usuários, considerando que as práticas investigadas têm impacto direto na vida de cada cidadão.

Contexto Histórico da Internet e a Indústria 4.0

Antigamente, a Internet foi criada para facilitar a comunicação entre indivíduos distantes geograficamente. Sua criação ocorreu na década de 1960, começando com a

ARPANET (*Advanced Research Projects Agency Network*), uma rede que permitia a troca de informações em instalações de pesquisa e ambientes militares. Segundo Briggs e Burke (2006, p. 302), os primeiros usuários dessa tecnologia obtinham poder e vantagens em relação aos demais.

Com o uso crescente da Internet, gradualmente a tecnologia se popularizou e expandiu para fins comerciais e privados, tornando-se um pilar de desenvolvimento. Como Briggs e Burke (2006, p. 302) explicam, sua imersão no comércio marcou uma nova fase. A Internet também desempenhou um papel crucial na educação, facilitando a evolução dos jovens no mundo digital, aumentando a acessibilidade às informações e facilitando sua formação acadêmica.

Diante do exposto, percebe-se o impacto significativo da Internet nas relações sociais e na sociedade como um todo. Apesar de facilitar as interações pessoais e profissionais, é essencial manter "uma relação saudável e equilibrada com todos esses dispositivos tecnológicos no cotidiano, buscando evitar consequências negativas e aproveitando com sabedoria os benefícios que oferecem", conforme explicado por King (2015, p. 11).

Assim, as inovações tecnológicas são constantes, e ao longo da história e do desenvolvimento tecnológico, várias inovações têm sido observadas, como destacado por Schwab (2016, p. 18):

> A primeira revolução industrial ocorreu aproximadamente entre 1760 e 1840. Provocada pela construção das ferrovias e pela invenção da máquina a vapor, ela deu início à produção mecânica. A segunda revolução industrial, iniciada no final do século XIX, entrou no século XX e, pelo advento da eletricidade e da linha de montagem, possibilitou a produção em massa. A terceira revolução industrial começou na década de 1960. Ela costuma ser chamada de revolução digital ou do computador, pois foi impulsionada pelo desenvolvimento dos semicondutores, da computação em mainframe (década de 1960), da computação pessoal (década de 1970 e 1980) e da internet (década de 1990).

Com o passar do tempo e o avanço das primeiras, segunda e terceira revoluções industriais, atualmente estamos vivendo a era da Indústria 4.0, a quarta revolução industrial. Caracterizada por uma transformação profunda nas estruturas sociais, essa era se destaca pela fusão do mundo físico e digital, visando maior eficiência em ações e operações específicas, redução de desperdício e melhor aproveitamento dos recursos.

Nessa perspectiva, a quarta revolução industrial se distingue pela integração cada vez maior de descobertas e disciplinas diversas. As inovações tecnológicas resultantes da interação entre diferentes tecnologias já não são mais ficção científica. Por exemplo, em "*The Second*

Machine Age", Brynjolfsson e McAfee afirmam que "a inteligência artificial (IA) está presente em nossas vidas, em carros autônomos, drones, assistentes virtuais e softwares de tradução. Isso está transformando nossas vidas" (SCHWAB, 2016, p. 22).

A Lei 13.709/2018 e o Devido Tratamento de Dados Pessoais

A internet é uma ferramenta de acesso direto que se destaca como fonte de informações globais e entretenimento. Por meio dela, os usuários podem acessar uma variedade de informações, navegar em sites, realizar compras e até mesmo utilizá-la como instrumento profissional. Conforme explicam Tamaro e Salarellei (2008, p. 164), "Os usuários têm a possibilidade de acesso a instrumentos eletrônicos com os quais podem construir sua própria base de dados, criar novos documentos, manipular ou estabelecer conexões com outras pessoas, ou colaborar com outros estudiosos em projetos comuns."

Entretanto, apesar dos benefícios proporcionados pelo uso da internet, também existem malefícios, especialmente para aqueles usuários que não estão instruídos sobre os perigos que redes sociais e plataformas digitais podem apresentar, como informações desorganizadas e websites suspeitos. É crucial ter habilidade na escolha dos sites acessados e das plataformas utilizadas.

Ao acessar plataformas ou redes digitais, é comum que dados pessoais como nome completo, email, data de nascimento, CPF, endereço, entre outros, sejam solicitados para ingresso ou cadastro. Portanto, é essencial que haja um tratamento adequado dessas informações pessoais, garantindo sua proteção e segurança. Qualquer atividade realizada com esses dados é considerada tratamento, englobando coleta, uso, transmissão e armazenamento, seja em operações online ou offline.

Para assegurar o controle e a transparência nas ações, bem como o cumprimento dos objetivos centrais da Lei Geral de Proteção de Dados (LGPD), cabe ao controlador e ao operador documentar adequadamente as informações dos usuários. Conforme estipulado pelo artigo 5º, inciso IX, da Lei 13.709/2018, o controlador é responsável por receber as informações do usuário, enquanto o operador de dados é encarregado de realizar o tratamento dos dados pessoais de cada indivíduo. Ambos os agentes possuem responsabilidade solidária conforme estabelecido nos contratos firmados entre eles e de acordo com suas respectivas funções.

Com a promulgação da Lei 13.709/2018, busca-se efetivar sua aplicabilidade, protegendo as informações pessoais de cada indivíduo e garantindo seus direitos fundamentais, incluindo privacidade, integridade e dignidade humana.

No entanto, mesmo com a implementação da LGPD, ainda há uma significativa falta de adesão à legislação devido aos altos custos que as organizações precisam suportar para sua implantação. A escassez de capital para investimentos em inovação tecnológica dificulta e retarda a adoção de novos programas que visam prevenir incidentes de segurança de dados pessoais.

Da Responsabilidade Civil

Com o avanço tecnológico, o âmbito legislativo necessitou acompanhar essas mudanças e se adaptar aos novos anseios da sociedade. Dessa forma, diversas leis abordaram essa temática, como o Código de Defesa do Consumidor, o Marco Civil da Internet (Lei 12.965/2014), a Lei de Acesso à Informação (Lei 12.527/2011), entre outras. Contudo, mesmo com essas legislações, surgia o questionamento sobre a necessidade de uma lei específica para tratar de forma eficaz o tratamento dos dados pessoais dos usuários, o que foi realizado com a edição da Lei 13.709/2018 (LGPD).

A LGPD trata da responsabilidade civil na Seção III do Capítulo VI, intitulada "Da responsabilidade e do ressarcimento de danos". Do artigo 42 ao artigo 45, há previsões sobre o tratamento irregular dos dados pessoais dos usuários, estabelecendo o direito à indenização, conforme análise dos casos concretos. Conforme observa Bodin de Moraes (2006, p. 239), "a responsabilidade civil consistirá justamente na imputação do evento danoso a um sujeito determinado, que será então obrigado a indenizá-lo".

Nos termos do artigo 14 do Código de Defesa do Consumidor (Lei 8.078/90), há clara consonância quanto à responsabilidade objetiva do fornecedor de serviços e dos responsáveis pelas operações relacionadas às informações dos usuários. O descumprimento dos padrões estabelecidos pela LGPD configura tratamento irregular.

Essa irregularidade no tratamento de dados ocorre quando há qualquer procedimento em desacordo com a Lei Geral de Proteção de Dados - LGPD. Conforme dispõe o artigo 44 da referida lei:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

A responsabilidade diante de tal ocorrência será atribuída tanto ao controlador quanto ao operador, sendo este último responsabilizado de forma solidária apenas em circunstâncias específicas, como o descumprimento de obrigações estabelecidas na referida lei e o não seguimento das diretrizes determinadas pelo controlador. Em resumo, o ônus da prova caberá ao titular, que estará no polo ativo da ação, demonstrando coerentemente os danos sofridos.

Ademais, caso haja dificuldade na produção de provas, o juiz poderá intervir no ônus da prova em favor do réu, que deverá então demonstrar ter cumprido regularmente as determinações legais, visando não prejudicar as informações pessoais dos usuários.

Diante do exposto, nos termos do artigo 43 da Lei 13.709/2018, existem situações específicas em que tanto o controlador quanto o operador não serão responsabilizados, não havendo, portanto, o dever de ressarcir eventuais danos causados aos usuários:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
>
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Assim, mediante a apresentação de provas que demonstrem a exclusão da responsabilidade civil dos agentes de tratamento de dados pessoais, estes estarão garantidos contra a aplicação de sanções. Segundo o inciso I do referido dispositivo legal, é abordada a situação em que o agente não realizou o tratamento dos dados que lhe foram concedidos, portanto, mesmo havendo tratamento de dados, o agente não possui qualquer relação com ele, caracterizando-se pela ilegitimidade passiva.

O inciso II trata da situação em que houve o tratamento de dados pessoais dos envolvidos, mas não houve violação das disposições da LGPD. Por fim, o inciso III menciona a culpa exclusiva do titular, quando o dano foi especificamente causado por ele, por terceiros ou pela ação conjunta entre titular e terceiros.

Da Autoridade Nacional de Proteção de Dados no Brasil – ANPD

A ANPD foi criada pela Medida Provisória nº 869/2018, posteriormente convertida na Lei 13.853/2019. O Decreto 10.474/2020 validou a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da ANPD. Essas disposições entraram em vigor na data da publicação da nomeação do Diretor-Presidente da ANPD no Diário Oficial da União, ocorrida em 2020, marcando o início efetivo das operações da ANPD. A missão da ANPD é garantir o amplo cumprimento do que dispõe a Lei Geral de Proteção de Dados no Brasil, assegurando os direitos fundamentais de privacidade, liberdade e livre desenvolvimento da personalidade dos indivíduos. Assim, conforme explica Patricia Peck Garrido:

> Pode-se afirmar que a ANPD foi criada para trazer mais segurança e estabilidade para a aplicação da Lei Geral de Proteção de Dados. No caso específico do Brasil há uma previsão bem ampla de artigos da Lei que dependem de futura regulamentação por parte da Autoridade, logo caberá a ela executar as adequações necessárias para que a legislação tenha uma aderência maior com a realidade social e econômica". (2023, p.21).

Nesse sentido, é imprescindível a cooperação entre as autoridades reguladoras e fiscalizadoras, bem como os três poderes Executivo, Legislativo e Judiciário, para desenvolver políticas públicas voltadas para a adequação e efetiva aplicação de códigos de conduta e certificações, conforme estabelecido no art. 50 da Lei 13.709/2018.

O art. 55-A da referida lei trata da criação da ANPD, e o § 1º menciona sua natureza jurídica transitória, que pode ser convertida em autarquia após dois anos, o que de fato ocorreu. Essa mudança de status é positiva, pois confere maior autonomia ao órgão. A ANPD é composta pelo Conselho Diretor, Conselho Nacional de Proteção de Dados e Privacidade, Corregedoria, Ouvidoria, órgão de Assessoramento Jurídico Próprio, Unidades Administrativas e Unidades Especiais.

Portanto, destaca-se a importância crucial da Autoridade Nacional de Proteção de Dados, pois cabe exclusivamente a este órgão a aplicação de sanções previstas na LGPD, e sua autonomia prevalece sobre as competências correlatas de outras entidades ou órgãos da Administração Pública no que diz respeito à proteção de dados, conforme estabelecido no art. 55-K da Lei 13.709/2018.

Falta de Adequação das Empresas aos Padrões da Lei 13.709/2018

Com a evolução tecnológica, as organizações, bem como as startups vislumbraram a necessidade de investir recursos financeiros para adequar-se as novas modificações digitais. Segundo Patrícia Peck Pinheiro (2018, p.33):

> Atender aos requisitos da LGPD exige adequação dos processos de governança corporativa, com implementação de um programa mais consistente de compliance digital, o que demanda investimento, atualização de ferramentas de segurança de dados, revisão documental, melhoria de procedimentos e fluxos internos e externos de dados pessoais, com aplicação de mecanismos de controle e trilhas de auditoria e, acima de tudo, mudança de cultura.

Deste modo, as corporações, por meio dos agentes responsáveis pelo devido tratamento de dados, devem empregar estratégias e recursos técnicos para garantir a proteção dos dados dos usuários. É essencial demonstrar a efetividade dessa regulamentação, além de ser necessário que os titulares compreendam o que realmente significa proteção de dados pessoais e sua relevância.

Segundo pesquisas realizadas pela RD Station (empresa de tecnologia e marketing), as empresas estão enfrentando dificuldades para se adaptar às diretrizes da Lei Geral de Proteção de Dados. O estudo revela que, das mil empresas participantes, 93% têm conhecimento sobre o tema da regulação de dados e o tratamento adequado desses dados. No entanto, apenas 15% delas estão em processo de preparação, apesar das sanções previstas por essa legislação - Maioria das empresas não conseguem se adaptar à LGPD (Sitecontabil, 2021).

O cenário demonstra que as empresas estão progredindo lentamente no processo de implementação e adequação às diretrizes da LGPD. Elas têm dificuldade em formular políticas de proteção de dados e também enfrentam falta de investimento em um profissional conhecido como Data Protection Officer (DPO), responsável por fiscalizar a aplicação efetiva da lei. Além disso, as empresas não dispõem de recursos suficientes para investir em novos processos tecnológicos e carecem de profissionais especializados para orientar a implementação das políticas de proteção, o que dificulta a adaptação à legislação e contribui para a lentidão no processo de conformidade.

Princípio da Privacidade como Garantia Fundamental

O direito à privacidade individual é uma garantia fundamental para todos os seres humanos e engloba um conjunto de informações da vida privada de cada indivíduo, sejam elas pessoais ou profissionais. Essas informações não devem ser expostas além do necessário, e a consagração desse direito abrange todas as esferas íntimas, privadas e da personalidade de cada pessoa. No ordenamento jurídico brasileiro, conforme o art. 5º, inciso X da Constituição Federal de 1988, e em conformidade com o art. 21 do Código Civil de 2002, fundamenta-se a proteção da esfera privada dos indivíduos, bem como sua intimidade e integridade.

Segundo Stefano Rodotà:

> a privacidade pode ser definida mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações" sendo a esfera privada "aquele conjunto de ações, comportamentos, opiniões, preferências, informações pessoais, sobre os quais o interessado pretende manter um controle exclusivo" (RODOTÀ, 2008, p. 92).

Posto isso, é vedada a divulgação no meio social de informações dos titulares sem o devido consentimento destes. Em resumo, a garantia da privacidade resulta de um conjunto de diversos direitos e valores constitucionais que carecem de uma fiscalização efetiva quanto ao tratamento adequado dos dados dos titulares, visando resguardá-los e garantir a integridade de cada indivíduo. Conclui-se que, apesar de os meios de tecnologia facilitarem as relações sociais e as plataformas comerciais possibilitarem transações mais rápidas, e as trocas constantes de informações serem frequentes, há uma falta de compreensão sobre os riscos associados ao acesso indevido à rede e às plataformas digitais, o que pode resultar em vazamento imprudente de informações pessoais.

Com o uso generalizado das redes sociais e a popularização da internet, os usuários estão cada vez mais imersos no mundo digital, onde os serviços e plataformas online facilitam a troca de informações. No entanto, apesar do avanço tecnológico e dos benefícios proporcionados pela internet, existem riscos envolvidos no uso desses meios.

Assim, o compartilhamento excessivo de informações dos usuários pode comprometer sua integridade, especialmente quando buscadores e redes sociais armazenam dados e os utilizam para gerar anúncios personalizados por meio de algoritmos. Portanto, apesar da era da Indústria 4.0 e da digitalização, muitos indivíduos não têm conhecimento dos riscos associados

aos meios digitais e não percebem os perigos de fornecer suas informações pessoais, o que facilita a ocorrência de crimes cibernéticos.

Diante das questões levantadas, apesar da ampla utilização da internet, os usuários ainda não estão completamente conscientes dos malefícios associados ao seu uso nem dos riscos decorrentes do compartilhamento de suas informações pessoais em plataformas digitais. Portanto, é fundamental que essas operações de dados sejam regulamentadas para garantir uma maior proteção aos dados fornecidos.

Método

Para a elaboração do presente estudo, optou-se por uma pesquisa de natureza básica estratégica, na qual se busca adquirir novos conhecimentos direcionados a diversas áreas visando a solução de problemas práticos reconhecidos (GIL, 2022). O trabalho foi desenvolvido com abordagem qualitativa, focando na interpretação das realidades sociais, utilizando fontes de pesquisa bibliográficas e documentais. Assim, o enfoque qualitativo concentrou-se na exploração, descrição e compreensão do problema, conforme explicam Marina de Andrade Marconi e Eva Maria Lakatos (MARCONI, LAKATOS, 2022, p.295).

Inicialmente, foram analisados artigos que destacam a importância da aplicabilidade da Lei Geral de Proteção de Dados (LGPD) e sua regulamentação para o tratamento adequado das informações dos indivíduos, tanto em operações online quanto offline. A pesquisa revelou que a adaptação das empresas à lei continua sendo um processo inovador. Em um segundo momento, foram conduzidas pesquisas mais aprofundadas sobre a frequência de incidentes de segurança e crimes cibernéticos, investigando como esses incidentes ocorrem e as possíveis formas de preveni-los, relacionando-os à falta de conhecimento dos usuários sobre a aplicação das legislações que regem as operações na internet. A análise dos dados foi realizada por meio de análise textual discursiva, examinando casos de grande repercussão que ocorreram no Brasil e envolveram incidentes de segurança.

Análise e Discussão dos Resultados

Considerando os estudos realizados, nota-se que as plataformas digitais são utilizadas com uma grande frequência, bem como a quantidade de usuários crescem de maneira desenfreada. Consequência de tal fato, é que o número de informações lançadas na internet

aumenta constantemente, podendo ocasionar vazamento de tais informações, e levando a graves prejuízos. No Brasil, ocorreram algumas situações das quais pode-se inferir uma grande repercussão e correlação entre a importância e aplicabilidade da LGPD, bem como no devido tratamento de dados pessoais dos usuários.

Netshoes

No ano de 2018, o site de comércio eletrônico - *Netshoes*, que é caracterizado por oferecer aos consumidores utensílios das mais variadas espécies, sejam elas esportivas ou casuais, sofreu com episódios de vazamento de dados pessoais de quase 2 milhões de clientes, comprometendo informações dos usuários (nome completo, Email, CPF, data de nascimento, e histórico de compras) de centenas de pessoas e servidores públicos politicamente expostos. Ato contínuo, foi constatado com as investigações do Inquérito civil nº 08190.044813/18-44, que os dados dos cartões de crédito, ou as respectivas senhas dos clientes não foram reveladas, no entanto, o transtorno tornou os usuários vulneráveis a fraudes futuras.

Em suma, diante de tal evento, e na inobservância do presente estudo, a Lei Geral de Proteção de Dados (LGPD) estabelece a opção abrangente de buscar ações judiciais perante o sistema judiciário para proteger os interesses e os direitos dos proprietários de dados que foram lesados. Deste modo, embora não haja aplicabilidade efetiva em todas as plataformas digitais da legislação, bem como o devido tratamento de dados, o poder judiciário, com base no CDC, poderá considerar a responsabilidade objetiva do fornecedor, independente de culpa, nos casos em que ocorra prejuízos decorrentes da atividade.

Posto isto, a Comissão de Proteção dos Dados de MPDF recomendou medidas a serem tomadas para que o dano não se tornasse maior aos clientes lesados. Assim, o Ministério Público do Distrito Federal, firmou termo de ajustamento de conduta (TAC) com a empresa Netshoes, que foi proposto pela Unidade Especial de Proteção de Dados e Inteligência Artificial (Espec).

Conforme explica o promotor de justiça Frederico Meinberg Ceroy: “a assinatura do presente Termo de Ajustamento de Conduta demonstra ser possível a resolução de conflito de forma consensual, com o devido ressarcimento da coletividade ante ao dano moral sofrido, sem, contudo, onerar excessivamente a empresa que colaborou com as investigações do Ministério Público”.

Para mais, a indenização foi fixada por danos morais no valor de R$500.000,00 (quinhentos mil reais), além de comprometer-se a implementação de medidas adicionais ao seu Programa de Proteção de Dados, bem como a sua adequação a Lei Geral de Proteção de Dados (LGPD), vindo a ser responsabilizada em casos de descumprimento. Portanto, diante de tais situações, serão considerados a efetividade de cumprimento do que dispõe a legislação, a fim de que haja garantia a segurança das informações dos usuários, tal como a maneira que foram realizados o devido tratamento e as técnicas utilizadas para a proteção das informações pessoais/sensíveis lançadas, de modo que, aquelas que não se adequar aos padrões de exigências da lei 13.709/2018, sejam obrigadas a reparar os danos ocasionadas pela negligência.

Ministério da Saúde

Os incidentes de vazamento de dados têm evidenciado os desafios enfrentados também pelo governo, no que tange a proteção adequada das informações, conforme estipulado pela legislação. Esses eventos também destacam as fraquezas no manejo de dados altamente sensíveis e revelam deficiências na segurança das empresas terceirizadas encarregadas do tratamento desses dados.

Destarte, no ano de 2020, os dados de mais de 200 milhões de brasileiros que se utilizavam do SUS (Sistema Único de Saúde) e até aquelas que não se utilizavam de tal mecanismo, ficaram expostos na rede por alguns meses devido a uma falha de segurança no sistema do Ministério da Saúde. Dados como nome completo, CPF, endereço, e telefone foram vazados, certificando novamente a relevância do comprometimento com a Lei Geral de Proteção.

A Autoridade Nacional de Proteção de Dados (ANPD) instaurou processo administrativo (nº 00261.000456/2022-12), com o objetivo de investigar as condutas de não atendimento as requisições pelo Ministério da Saúde, como a ausência do responsável encarregado pelos dados pessoais dos usuários, e a falta de comunicação do evento de incidente de segurança aos envolvidos, tornando-os cientes da situação. O processo encontra-se em fase de instrução processual.

Em conformidade com a LGPD, os órgãos governamentais devem processar informações pessoais com o propósito de satisfazer objetivos públicos particulares, alinhados com o bem comum. Esse procedimento deve seguir as competências e responsabilidades legais

estabelecidas para os serviços públicos. Outrossim, no contexto da Administração Pública, o tratamento e o armazenamento de dados, devem ser programados para garantir a efetividade de atividade de políticas públicas e a busca do interesse público.

Nos artigos 25 e 26 da lei 13.709/2018, é disposto atividades típicas dos órgãos públicos no que tange aos dados pessoais, na qual devem ser mantidos em formato interoperável e estruturado para o uso compartilhado, de modo que sejam respeitados os princípios norteadores pautados no referido dispositivo legal.

Desta feita, a Autoridade Nacional de Proteção de Dados(ANPD) orienta os encarregados ao atendimento de alguns preceitos que devem ser analisados pela Administração Pública quando realizarem o compartilhamento de dados pessoais, de modo que, todas as operações que envolva informações de usuários pelo poder público, estão sujeitos a fiscalização da ANPD, sendo este, o órgão responsável pela garantia e proteção dos titulares dos dados, bem como, na aplicação de sanções em casos de descumprimento ou violação a LGPD.

Portanto, é de suma relevância o enquadramento e efetividade dos padrões da Lei Geral de Proteção de Dados, em Pessoa Jurídica de Direito Privado e Pessoa Jurídica de Direito Público, nos termos do art.1º da lei supracitada, tendo como principal prerrogativa, uma relação segura entre os usuários e de transparência.

Pix

Com o referido estudo, é de notório saber que com a inovação tecnológica, a segurança digital faz-se necessária, uma vez que as interações demandam alta proteção contra ameaças. Deste modo, pode-se destacar a utilização crescente do PIX, que criado no ano de 2020, é o método de transação bancário eficiente, competitivo e inclusivo, conforme explica o diretor de política monetária do comitê de política monetária, Reinado Le Grazie.

Recentemente, houve mais um incidente de segurança na qual acarretou vazamento de informações de alguns clientes da instituição financeira do estado do Pará, devido a falhas no sistema. Em abril de 2024, o Banco Central informou por meio de nota, o vazamento de dados cadastrais de mais de três mil clientes que estavam sob a guarda e responsabilidade do banco Banpará (Banco do estado do Pará), sendo tal evento o oitavo episódio desde a criação do método pix. Pode-se inferir que casos semelhantes já ocorreram, como a Sumup Sociedade de

Crédito, na qual teve 87 (oitenta e sete mil) mil chaves vazadas, a empresa de Pequeno Porte Limitada tendo 46 (quarenta e seis mil) chaves também vazadas, dentre outros.

Ocorre que, o Banco Central ainda informou que apesar do acontecimento, não foram expostos dados sensíveis, apenas dados como nome completo, cpf, agência, conta e instituição de relacionamento, e que as vítimas seriam notificadas a fim de que possuíssem ciência acerca do ocorrido. Ademais, o comunicado também evidenciou que foram adotadas ações necessárias para a averiguação detalhada da situação, razão pela qual serão aplicadas sanções conforme a legislação.

Ante o exposto, nota-se que apesar das atualizações digitais, e de meios que tornam o cotidiano mais acessíveis, os incidentes de segurança tornam-se mais frequentes em transações bancárias, devido a possíveis falhas no sistema das instituições financeiras, bem como na ausência da adequação as exigências do que dispõe a LGPD.

Considerações Finais

Apesar da promulgação da lei 13.709/2018, ainda há uma grande ocorrência de incidentes de segurança no Brasil, razão pela qual fez-se necessário o presente estudo, no intuito de analisar as razões que ensejam o vazamento de dados mesmo com a vigência da LGPD, a importância das empresas privadas e órgãos da Administração Pública aderirem tais orientações, de modo que realizem o devido tratamento dos dados pessoais.

Nesse sentido, com base no que foi apresentado no presente trabalho, analisou-se que há uma grande incidência de cibercrimes no âmbito brasileiro, de modo que, devido a popularização da rede, os usuários tornaram-se mais vulneráveis a possíveis fraudes, pois as plataformas digitais são utilizadas para cunho pessoal e profissional. Assim, as pesquisas expuseram a relevância da legislação que disciplina tais operações, em consonância com a adequação das organizações públicas ou privadas e pessoas físicas ou jurídicas, aos requisitos intrínsecos da referida legislação.

Tendo em vista as pesquisas realizadas, e os estudos dos casos recentes que tiverem a ocorrência de vazamento de dados, fica evidente o transtorno causado com a disseminação de informações de caráter sensíveis. Deste modo, ao utilizar-se de aplicativos e softwares, deve-se ter cautela desde o cadastro em um aplicativo de compra até a sua finalização de aquisição, como ficou demonstrado com o caso de vazamento de dados da Netshoes, bem como no acesso

em redes sociais, confinado pelo incidente do Facebook no ano de 2022 e plataformas governamentais, como foi o caso do Ministério da Saúde, no ano de 2020. Da mesma maneira, também foi certificado eventos de exposição em transações bancárias online, como ficou evidente no caso mais recente do banco Banpará, neste ano.

Em síntese, resta evidente que não basta apenas o zelo dos envolvidos quanto as suas informações, mas que é indispensável a devida adequação aos padrões da LGPD pelas empresas e entidade públicas, de modo que aos passos das evoluções sociais e digitais, estas devem corresponder as novas pretensões para a garantia e proteção dos dados pessoais de cada indivíduo, constituindo dessa forma, uma via de mão dupla.

Assim sendo, considera-se que o trabalho de pesquisa obteve-se que , o real teor sobre a lentidão de tal processo por partes das organizações devido ao investimento necessário para a adequação aos padrões da lei 13.709/2018, e as respectivas responsabilidades advindas da negligência no que tange a falta de aplicabilidade da referida lei, bem como a valia da consciencialização dos envolvidos nos riscos inerentes ao uso indevido dos meios digitais, e as consequências que podem acarretar em informações lançadas de modo imprudente, foram os resultados obtidos pela pesquisa.

Ante o exposto, o presente trabalho despertou nos pesquisadores, o interesse em buscar mais formas de modificar a situação atual da vasta ocorrência de vazamento de dados pessoais, visando contribuir com a sociedade.

Referências

BCB, **BC comunica ocorrência em instituição**, 2024. Disponível em: <https://www.bcb.gov.br/detalhenoticia/18143/nota\>. Acesso em: 28 maio 2024.

BLING. **Vazamento de dados e privacidade: os riscos e como se prevenir, 2023**. Disponível em: <https://blog.bling.com.br/vazamento-de-dados-e-privacidade-os-riscos-e-como-se-prevenir/#:~:text=O%20vazamento%20de%20dados%20%C3%A9,ou%20repassados%20ilegalmente%20a%20terceiros\>. Acesso em: 08 out. 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm\>. Acesso em: 14 set. 2023.

BRASIL. **Lei 13.709/2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm\>. Acesso em: 30 ago. 2023.

BRIGGS, A.; BRUKE, P. **Uma história social da mídia, de Gutemberg a internet**. Rio de Janeiro: Jorge Zahar ed., 2006. Acesso em: 05 jun. 2024.

CARTILHA LGPD NOVO, **Tribunal de Justiça**, 2023. Disponível em: <https://www.stj.jus.br/sites/portalp/WebPub/NovoPortal/midias/cartilha-lgpd-novo.pdf\>. Acesso em: 25 out. 2023.

CORA. **Vazamento de dados, como ocorre e como se proteger, 2022**. Disponível em: <https://www.cora.com.br/blog/vazamento-de-dados/\>. Acesso em: 29 out. 2023.

DIREITO NET. **Responsabilidade civil no caso de vazamento de dados pessoais, 2023**. Disponível em: <https://www.direitonet.com.br/artigos/exibir/12841/Responsabilidade-civil-no-caso-de-vazamento-de-dados-pessoais-LGPD\>. Acesso em: 02 out. 2023.

GIL, Antonio Carlos. **Como Elaborar Projeto de Pesquisa**. 7ª ed. São Paulo: Atlas, 2022. Disponível em: <https://files.cercomp.ufg.br/weby/up/150/o/Anexo_C1_como_elaborar_projeto_de_pesquisa_-_antonio_carlos_gil.pdf\>. Acesso em: 29 out. 2023.

GOV. BR. **Perguntas frequentes à ANPD, 2023**. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#c1\>. Acesso em: 30 maio 2024.

GOV. BR. **ANPD divulga lista de processos sancionatórios, 2023**. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-lista-de-processos-sancionatorios\>. Acesso em: 28 maio 2024.

KING, A. L. S.; NARDI, A. E.; CARDOSO, A. **Nomofobia: dependência do computador, internet, redes sociais, dependência do telefone celular**. 2015. Disponível em: <https://www.amazon.com.br/Nomofobia-Depend%C3%AAncia-Computador-Internet-Telefone/dp/8538805630?asin=B0725SYJTQ&revisionId=&format=4&depth=1\>. Acesso em: 19 abr. 2024.

LGPD BRASIL**. LGPD na Administração Pública. 2023**. Disponível em: <https://www.lgpdbrasil.com.br/lgpd-na-administracao-publica/\>. Acesso em: 28 maio 2024.

LGPD: **Um marco na Regulamentação de dados**. Superior Tribunal de Justiça, 2020. Disponível em: <https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protecao-de-dadospessoaislgpd#:~:text=LGPD%3A%20Um%20marco%20na%20regulamenta%C3%A7%C3%A3o,vigor%20em%20setembro%20de%202020\>. Acesso em: 21 ago. 2023.

MATOS, Évilin. **Avanço da tecnologia nos últimos 10 anos: de casa ao trabalho**. Runrun.it/blog, 2021. Disponível em: <https://blog.runrun.it/avanco-da-tecnologia/\>. Acesso em: 10 out. 2023.

MORAES, Maria Celina Bodin. **Princípios do direito civil contemporâneo**. Rio de Janeiro: 2006. Acesso em: 02 jun. 2024.

MPDF. **MPDF e Netshoes firmam acordo para pagamento de danos morais após vazamento de dados.** 2019. Disponível em: <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados#\>. Acesso em: 28 maio 2024.

NONES, Fernanda. **ANPD: pesquisa aponta que maioria das empresas não conseguem se adaptar à LGPD**. Sitecontabil, 2021. Disponível em: <https://www.sitecontabil.com.br/noticias_empresariais/ler/anpd---pesquisa-aponta-que-maioria-das-empresas-nao-conseguem-se-adaptar-a-lgpd\>. Acesso em: 20 out. 2023.

PEDRA, David. **O que é a indústria 4.0? Tudo sobre a revolução industrial**. Siteware, 2023. Disponível em: <https://www.siteware.com.br/metodologias/o-que-e-industria-4-0/\>. Acesso em: 29 out. 2023.

PORTAL G1. **Netshoes terá de pagar 500 mil por vazamento de dados de 2 milhões de clientes**. 2019. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/2019/02/05/netshoes-tera-de-pagar-r-500-mil-por-vazamento-de-dados-de-2-milhoes-de-clientes.ghtml\>. Acesso em: 23 maio 2024.

PORTAL G1. **Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet**. 2020. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml\>. Acesso em: 2 maio 2024.

RODOTÀ, Stefano. **Il problema della responsabilità civile. Milano: Giuffrè, 1967**. Acesso em: 21 abr. 2024.

SCHWAB, Klaus. **Quarta Revolução Industrial**. 1ª edição. 2016. Disponível em: <https://pt.slideshare.net/JedielVitalSempreAdo/a-quarta-revolucao-industrial-klaus-schwabpdf\>. Acesso em: 13 out. 2023.

SEBRAE. **Empresas devem se adequar à Lei Geral de Proteção de Dados**. 2022. Disponível em: <https://sebrae.com.br/sites/PortalSebrae/ufs/ac/artigos/empresas-devem-se-adequar-a-lei-geral-de-protecao-de-dados-pessoais,7c41bfc644601810VgnVCM100000d701210aRCRD#:~:text=Os%20primeiros%20passos%20para%20essa,pr%C3%A1ticas%20da%20LGPD%20na%20empresa\>. Acesso em: 28 ago. 2023.

SERPRO. **Violação de dados pessoais: o que fazer antes, durante e depois de um incidente**. 2022. Disponível em: <https://www.serpro.gov.br/menu/noticias/noticias-2022/o-que-fazer-em-caso-de-violacao-de-dados-pessoais/\>. Acesso em: 15 set. 2023.

SITECONTÁBIL. Disponível em: https://sitecontabil.com.br/. Acesso em: 28 ago. 2023.

SILVA, Danilo Alves. **Direito à Privacidade**. Aurum, 14 jun. 2023. Disponível em: <https://www.aurum.com.br/blog/direito-a-privacidade/\>. Acesso em: 08 set. 2023.

TAMMARO, Anna Maria; SALARELLI, Alberto. **A biblioteca digital**. 2009. Acesso em: 19 abr. 2024.

UOL. Brasil Escola. **História da internet**. 2023. Disponível em: <https://brasilescola.uol.com.br/informatica/internet.h\>. Acesso em: 12 out. 2023.

VIENAZINDYTE, Ilma. **Os perigos da internet: como reconhecer e evitá-los.** NordVPN, 2021. Disponível em: <https://nordvpn.com/pt-br/blog/perigos-da-internet/\>. Acesso em: 29 out. 2023.

●

Como citar este artigo (Formato ABNT):

GALVÃO, Heideivirlandia Leite; OLIVEIRA, Alyne Leite de; GINO, Bethsaida de Sá Barreto Diaz; VIANA, Hudson Josino; ARAÚJO, Francisco Gledison Lima; BENEVINUTO, Noélia Marques Silva; SILVA, Denis Leonardo Ferraz da. Incidentes de Segurança: Regulação e Prática de Vazamento de Dados Pessoais Frente à LGPD. **Id on Line Rev. Psic**., Julho/2024, vol.18, n.72, p.179-197, ISSN: 1981-1179.

Recebido: 10/07/2024; Aceito 18/07/2024; Publicado em: 31/07/2024.