

## **A PROTEÇÃO DE DADOS PESSOAIS NA ERA DA INFORMAÇÃO: ANÁLISE DOS MECANISMOS DE SEGURANÇA JURÍDICA PARA A DEFESA DA PRIVACIDADE DO INDIVÍDUO**

*Marco Antônio Ferreira Dutra*

Graduando (a) em Direito pelo UNIPTAN

e-mail: marcoantoniodutra@hotmail.com

Professor Coautor: Pedro Arruda Júnior

**Resumo:** Na era da informação, a preservação de dados pessoais é uma preocupação crucial, abrangendo a segurança jurídica e a privacidade individual. Este artigo explorou as vulnerabilidades nos sistemas responsáveis pela coleta, armazenamento e processamento de dados e sua possível exploração por agentes maliciosos. As vulnerabilidades podem surgir em várias etapas do ciclo de vida dos dados, incluindo práticas inseguras de coleta, falta de criptografia adequada durante o armazenamento e inadequações na segurança do processamento de dados. As consequências da exploração dessas vulnerabilidades variam de violações de dados a roubo de identidade, destacando a necessidade urgente de medidas robustas de proteção de dados. O artigo enfatizou a importância de abordar essas vulnerabilidades e implementar medidas abrangentes de segurança, incluindo criptografia, políticas de segurança claras, auditorias regulares, treinamento de funcionários e conformidade com leis de proteção de dados, como a LGPD (Lei Geral de Proteção de Dados) no contexto brasileiro. Ele destaca a relevância de manter a conscientização em um cenário em constante evolução de ameaças cibernéticas e a necessidade de medidas proativas para proteger dados pessoais, garantindo privacidade, segurança e conformidade legal. A metodologia utilizada teve como base revisão bibliográfica, análise documental, estudo de casos e análise estatística que permitiu uma abordagem ampla e aprofundada do tema. E como principal conclusão este trabalho demonstrou a importância e os desafios da proteção de dados pessoais na era da informação, bem como as medidas adotadas para garantir esse direito. Foi evidenciado que a era digital trouxe benefícios e riscos para a privacidade dos indivíduos, exigindo uma atuação responsável e consciente dos controladores de dados, bem como uma legislação adequada e atualizada. Nesse sentido, a LGPD e a ANPD representam um marco histórico na defesa da privacidade e da segurança jurídica no Brasil, alinhando-se aos padrões internacionais de proteção de dados. Foi ressaltado que a proteção de dados pessoais é um tema dinâmico e complexo, que demanda uma constante revisão e adaptação às novas tecnologias e demandas sociais.

**Palavras-chave:** Segurança, Dados Pessoais, LGPD.

### **Introdução**

A proteção de dados pessoais na era da informação foi um tema de crescente relevância e complexidade. A cada dia, éramos inundados com um volume impressionante de informações pessoais que circulavam por sistemas digitais e plataformas online. Diante desse cenário, a salvaguarda da privacidade individual e a garantia de segurança jurídica emergiram como desafios cruciais para a sociedade contemporânea.

O tema central deste trabalho de pesquisa concentrou-se na análise dos mecanismos de segurança jurídica destinados a proteger a privacidade do indivíduo no contexto da proteção de dados pessoais. Tratou-se de uma exploração minuciosa dos aspectos legais e práticos envolvidos na preservação dos dados pessoais em um ambiente altamente conectado e digitalizado.

A escolha deste tema não foi aleatória, mas sim uma resposta à crescente importância da proteção de dados pessoais em um mundo cada vez mais dependente da tecnologia. O avanço das comunicações digitais e a proliferação de serviços online tornaram evidente a necessidade de estabelecer um equilíbrio entre a utilização de dados para fins legítimos e a proteção da privacidade individual. Nesse sentido, a pesquisa buscou contribuir para a compreensão das implicações legais e práticas dessa questão premente.

O problema que norteou este trabalho foi: Como os mecanismos de segurança jurídica puderam efetivamente proteger a privacidade do indivíduo em um cenário de crescente exposição de dados pessoais? Com base nesse problema, o objetivo geral deste estudo foi analisar os mecanismos legais e práticos que visam assegurar a proteção de dados pessoais, identificando desafios e oportunidades. Além disso, ficou definido os seguintes objetivos específicos: Avaliar os mecanismos de segurança jurídica existentes no Brasil para a proteção dos dados pessoais; Investigar as consequências da violação da legislação de proteção de dados; Destacar as vulnerabilidades dos sistemas de coleta, armazenamento e tratamento de dados pessoais.

A pesquisa adotou uma abordagem qualitativa, incluindo revisão bibliográfica e análise documental de legislações pertinentes. Foram consideradas as leis de proteção de dados, com foco na Lei Geral de Proteção de Dados (LGPD) no contexto brasileiro. Além disso, foram consultadas pesquisas acadêmicas e estudos de especialistas na área.

## **1. A LGPD no Brasil: Avanços, Desafios e Impactos**

O papel da LGPD, na proteção dos dados pessoais, representou um avanço significativo na proteção dos dados pessoais no Brasil, apesar dos desafios enfrentados. Os princípios e as

regras estabelecidos pela lei, bem como os mecanismos de fiscalização e sanção previstos, são importantes temas de debate.

Os impactos da proteção de dados pessoais na economia digital são considerados significativos, uma vez que o tratamento de informações pessoais é uma parte essencial dos modelos de negócios de muitas empresas. O debate sobre como conciliar a proteção de dados pessoais com o desenvolvimento econômico é crucial.

A relação entre privacidade e segurança também é abordada, com a proteção de dados pessoais sendo intimamente ligada à privacidade e à segurança. O debate sobre como esses conceitos se relacionam e como a proteção de dados pessoais contribui para a segurança e o bem-estar dos indivíduos é de grande importância.

No contexto da proteção de dados pessoais no Brasil, é fundamental analisar como a LGPD tem impactado as práticas das organizações e a conscientização dos indivíduos sobre seus direitos e responsabilidades em relação aos seus dados pessoais.

A conscientização pública sobre a importância da privacidade e da proteção de dados tem aumentado à medida que casos de violações de dados e vazamentos se tornam mais frequentes. Os cidadãos estão mais atentos aos seus direitos de privacidade e ao papel das empresas em garantir a segurança de suas informações pessoais. Isso tem impulsionado as empresas a adotar medidas mais rigorosas de segurança de dados e a promover a transparência em suas práticas de coleta e tratamento de informações pessoais.

Além disso, a LGPD tem incentivado o desenvolvimento de soluções tecnológicas e serviços relacionados à proteção de dados, criando oportunidades de negócios para empresas que oferecem serviços de consultoria em conformidade, software de segurança cibernética e soluções de gerenciamento de dados. Isso representa um impulso significativo para a economia digital, à medida que novas indústrias e empregos são criados em resposta às demandas da lei.

Em relação à relação entre privacidade e segurança, a esta lei desempenha um papel importante na promoção de uma cultura de segurança de dados. A lei exige que as organizações implementem medidas de segurança apropriadas para proteger os dados pessoais que coletam e processam. Isso inclui a criptografia de dados, o controle de acesso e a resposta a incidentes de segurança.

No entanto, ainda há desafios a serem superados, como a necessidade de garantir que as empresas de todos os portes estejam em conformidade com a LGPD e que as sanções sejam aplicadas de maneira eficaz em casos de não conformidade. Além disso, a legislação deve continuar a se adaptar às mudanças tecnológicas e aos desafios emergentes, como a crescente quantidade de dados pessoais gerados por dispositivos e a expansão das redes sociais.

É essencial que a sociedade, o setor privado e o governo continuem a colaborar na construção de um ambiente digital seguro e respeitoso da privacidade, onde a proteção de dados pessoais e o desenvolvimento econômico possam coexistir de forma harmoniosa. A aplicação eficaz da LGPD e o compromisso contínuo com a segurança cibernética e a privacidade são elementos-chave para alcançar esse objetivo.

A Lei Geral de Proteção de Dados representa um avanço significativo na proteção dos direitos fundamentais de liberdade, privacidade e personalidade dos cidadãos brasileiros. No entanto, a lei também enfrenta diversos desafios e impactos, tanto do ponto de vista técnico quanto jurídico, para garantir sua efetividade e adequação ao cenário nacional e internacional. Nesse contexto, é importante analisar os mecanismos de segurança jurídica existentes no Brasil para a proteção dos dados pessoais, bem como as possíveis lacunas e melhorias que podem ser implementadas. O próximo tema aborda os principais instrumentos normativos e judiciais que visam assegurar o cumprimento da LGPD e a defesa dos direitos dos titulares dos dados.

## **2. Mecanismos de segurança jurídica existentes no Brasil para a proteção dos dados pessoais**

No contexto dos mecanismos de segurança jurídica existentes no Brasil para a proteção dos dados pessoais, o trabalho de Joice Agostinelli (2018) intitulado "A Lei Geral de Proteção de Dados Pessoais (LGPD) e suas implicações na sociedade contemporânea" abordou diversos aspectos relacionados à LGPD, incluindo suas consequências, responsabilidades das empresas e órgãos enquanto controladores de dados, mudanças e avanços decorrentes da aprovação da lei, e a importância da segurança jurídica nesse contexto.

Agostinelli (2018) destacou que a LGPD busca analisar as consequências da violação da lei, estabelecendo sanções e penalidades para as empresas e organizações que não cumpriram as disposições relacionadas à proteção de dados pessoais. A lei estabeleceu a possibilidade de aplicação de multas que podiam chegar a 2% do faturamento da empresa, limitadas a um valor máximo, além de outras sanções administrativas, como a publicização da infração e o bloqueio dos dados pessoais.

A aprovação da LGPD trouxe mudanças significativas no cenário da proteção de dados pessoais no Brasil. A lei estabeleceu diretrizes e princípios claros, como a finalidade, necessidade, adequação, transparência e segurança no tratamento de dados pessoais. Além disso, a LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar e regulamentar a aplicação da lei. Com a entrada em vigor da LGPD, houve uma

maior conscientização sobre a importância da proteção de dados pessoais e uma maior preocupação das empresas em se adequarem às suas disposições.

Um aspecto crucial abordado Agostinelli (2018) foi a segurança jurídica proporcionada pela LGPD. A lei estabeleceu um marco legal claro para a proteção de dados pessoais, trazendo maior segurança para os titulares dos dados, empresas e órgãos que tratavam essas informações. A LGPD estabeleceu regras e diretrizes que visavam garantir a privacidade, o controle e a segurança dos dados pessoais, promovendo a confiança dos indivíduos e a segurança jurídica nas relações de tratamento de dados.

De maneira geral, de acordo com Bruno Ricardo Bioni (2019), foi possível categorizar a evolução das leis de proteção de dados pessoais em quatro estágios distintos. A primeira etapa foi caracterizada pelo surgimento da preocupação com o processamento em larga escala de informações pessoais no âmbito governamental, durante a formação do Estado Moderno, com foco nas esferas governamentais. Nesse período, foram estabelecidas regras rigorosas que regulamentavam o uso das tecnologias no que se refere à coleta e ao processamento de dados pessoais de indivíduos ligados ao governo.

A segunda fase representou uma mudança regulatória, abrangendo não apenas os dados pessoais de indivíduos governamentais, mas também os de pessoas da esfera privada. Desse modo, a responsabilidade pela proteção dessas informações foi transferida para os próprios titulares dos dados. Em outras palavras, estabeleceu-se quais informações poderiam ser coletadas, utilizadas e compartilhadas, tudo isso com o consentimento adequado, conferindo maior autonomia aos indivíduos no gerenciamento de seus dados pessoais. (Bioni, 2019)

A terceira etapa referiu-se a regulamentos que garantiram ao indivíduo o direito de participar ativamente de todo o processo, desde a coleta até o compartilhamento de informações, ou seja, conferiu-se uma maior autonomia ao titular dessas informações. Já na quarta etapa, o Estado voltou a desempenhar um papel regulatório, estabelecendo normas específicas para determinados tipos de dados pessoais considerados sensíveis. Com isso, retirou-se do indivíduo a prerrogativa de tomar decisões autônomas, transferindo ao Estado a responsabilidade de gerenciar essas informações, conforme os regulamentos estabelecidos pelas leis de proteção de dados. (Bioni, 2019)

A LGPD representa um avanço significativo no campo da proteção de dados pessoais no Brasil. Ao analisar as consequências da violação da lei, a responsabilidade das empresas e órgãos enquanto controladores de dados, as mudanças e avanços trazidos pela LGPD e a importância da segurança jurídica, compreende-se a relevância dessa legislação para a proteção da privacidade e da dignidade do indivíduo na era da informação. A LGPD contribuiu para o

estabelecimento de uma cultura de respeito aos direitos dos titulares dos dados, promovendo a transparência, a confiança e a segurança jurídica nas relações de tratamento de dados pessoais.

Em relação à inaplicabilidade da LGPD, encontramos no artigo 4º o seguinte teor:

Art. 4º Esta Lei não é válida para o tratamento de dados pessoais:

I - realizado por indivíduos para fins estritamente pessoais e não econômicos;

II - realizado exclusivamente para fins:

a) jornalísticos e artísticos; ou

b) acadêmicos, com a aplicação dos artigos 7º e 11 desta Lei;

III - realizado exclusivamente para os fins de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de crimes; ou

IV - originados de fora do território nacional, que não sejam comunicados, compartilhados com agentes de tratamento brasileiros ou transferidos internacionalmente para outro país que não seja o de origem, desde que o país de origem proporcione um nível adequado de proteção de dados pessoais, conforme previsto nesta Lei.

Observou-se que a lei estabeleceu limitações em relação aos tipos de dados que foram regulados pela LGPD. De acordo com Patricia Peck (2018, p. 43-44):

[...] o tratamento de dados pessoais deveria ter uma finalidade específica e funcional, mas sem ultrapassar a liberdade de informação e expressão, a soberania, segurança e defesa do Estado.

Essas limitações visaram proporcionar uma maior segurança em questões relevantes da sociedade.

Pode-se inferir, a partir do texto da Lei, que essas restrições tiveram o objetivo de contribuir para um equilíbrio adequado entre a proteção da privacidade e da segurança pública. Ou seja, houve uma busca constante por um equilíbrio que beneficiasse o indivíduo em relação aos seus dados pessoais, sem ultrapassar a fronteira que representaria um perigo para o Estado e para a sociedade como um todo.

Os mecanismos de segurança jurídica existentes no Brasil para a proteção dos dados pessoais são fundamentais para garantir o cumprimento da LGPD e a defesa dos direitos dos titulares dos dados. No entanto, esses mecanismos não são suficientes para eliminar os riscos de violação, perda ou uso indevido dos dados pessoais, que podem ocorrer em virtude das

vulnerabilidades dos sistemas de coleta, armazenamento e tratamento de dados pessoais. Essas vulnerabilidades podem ser de natureza técnica, humana ou organizacional, e podem comprometer a integridade, a confidencialidade e a disponibilidade dos dados pessoais. O tema seguinte aborda essas vulnerabilidades, bem como as medidas de prevenção e mitigação que podem ser adotadas pelos agentes de tratamento de dados.

### **3. Vulnerabilidades dos sistemas de coleta, armazenamento e tratamento de dados pessoais**

Antes de abordar as atividades que compõem o chamado processamento de informações pessoais, é crucial discutir os princípios aplicáveis e que validam tal tratamento de dados, com isso, Rafael Ramos Soares (2020) destacou os principais que são orientadores do tratamento de dados pessoais como: adequação, propósito, necessidade, livre acesso, transparência, segurança, responsabilidade e prestação de contas, prevenção, não discriminação e qualidade dos dados.

No contexto dos princípios norteadores da proteção de dados, emerge o princípio do propósito como um farol orientador, ele diz que os dados coletados dos indivíduos devem ter uma finalidade específica, e o processamento dessas informações deve estar restrito a esse propósito, sendo claro para qual fim esses dados pessoais são coletados. (Soares, 2020)

Na esteira desse princípio, desenha-se o princípio da adequação, onde todo o processo de tratamento dos dados deve estar diretamente relacionado aos propósitos informados anteriormente pelo princípio do propósito, ajustando-se ao que é solicitado. Por exemplo, se um usuário solicitar a exclusão de seus dados do banco de dados, a empresa responsável não deve apenas ocultá-los, mas sim removê-los. Caso contrário, estaria violando o princípio da adequação e poderia ser punida. (Soares, 2020)

Alicerçado na noção de justificativa, o princípio da necessidade diz que a coleta de dados dos usuários deve ter uma justificativa, ou seja, deve ser realmente necessária para o fim pretendido. (Soares, 2020)

O princípio do livre acesso, por sua vez, destaca que os dados pessoais coletados devem estar sempre disponíveis gratuitamente e de forma fácil para consulta pelos seus titulares. Todas as informações relacionadas ao usuário, inclusive quanto tempo os dados serão tratados, as formas de tratamento, entre outras informações, devem estar acessíveis. (Soares, 2020)

Sob a égide do princípio da qualidade dos dados, os portadores e titulares de dados pessoais devem ter a garantia de que suas informações são tratadas corretamente, de forma

clara, relevante e atualizada, conforme necessário e para o cumprimento específico do propósito para o qual os dados foram coletados. (Soares, 2020)

Por último, mas não menos importante, o princípio da transparência afirma que os dados e os processos de tratamento devem ser informados de maneira clara, precisa e transparente, ou seja, todo o processo de tratamento pelo qual os dados passam deve ser descrito de maneira abrangente. (Soares, 2020)

Todos os dados devem ser tratados com técnicas que garantam a maior proteção contra acessos não autorizados, bem como situações acidentais ou ilícitas que possam causar destruição, perda, alteração, vazamento ou divulgação não autorizada. Esse princípio é conhecido como princípio da segurança e dele decorre o princípio da prevenção, que enfatiza a necessidade de adotar medidas preventivas para evitar qualquer tipo de dano aos dados pessoais dos titulares. (Soares, 2020)

Por fim, temos o princípio da não discriminação e o princípio da responsabilidade e prestação de contas. O primeiro enfatiza que os dados não devem ser tratados com propósitos discriminatórios, abusivos ou ilegais. Já o segundo aponta que o responsável pelo tratamento dos dados pessoais é responsável por eles e deve ser capaz de demonstrar que está adotando as medidas necessárias para cumprir adequadamente as normas de proteção de dados pessoais, inclusive demonstrando a eficácia das medidas adotadas. (Soares, 2020)

Após falar sobre os princípios que norteiam o tratamento de dados pessoais, destacou-se as vulnerabilidades dos sistemas de coleta, armazenamento e tratamento de dados pessoais que são fragilidades ou falhas que podem ser exploradas por indivíduos mal-intencionados para obter acesso não autorizado às informações pessoais.

Essas vulnerabilidades podem ocorrer em diferentes etapas do ciclo de vida dos dados pessoais. Na fase de coleta, por exemplo, as vulnerabilidades podem surgir devido a práticas inseguras, como solicitar informações desnecessárias ou coletar dados sem o consentimento adequado dos indivíduos. Falhas no armazenamento podem incluir a falta de criptografia dos dados, sistemas de segurança inadequados ou a retenção desnecessária de informações pessoais. A autora Thalyta Soares de Farias (2020) defende que o armazenamento de dados deve ser feito de forma segura, eficiente e responsável, seguindo o princípio da segurança, que exige a adoção de medidas técnicas, administrativas e organizacionais aptas a proteger os dados de acessos não autorizados, destruição, perda, alteração ou divulgação indevida e complementa que o tratamento de dados deve ser feito de forma ética, legal e adequada, observando o princípio da adequação, que determina que o tratamento deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Já na etapa de tratamento dos dados, as vulnerabilidades podem ocorrer devido à falta de medidas de segurança, como a ausência de sistemas de autenticação, controle de acesso inadequado ou a não implementação de políticas claras de proteção de dados. Além disso, falhas no desenvolvimento de aplicativos e sistemas podem levar a vulnerabilidades de software, tornando os sistemas mais suscetíveis a ataques e explorações. Para Thalyta Soares de Farias (2020) o desenvolvimento de aplicativos e sistemas deve levar em conta o princípio da prevenção, que implica a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Essas vulnerabilidades podem ser exploradas por hackers, criminosos cibernéticos, funcionários mal-intencionados ou até mesmo por falhas acidentais de segurança. Quando exploradas com sucesso, as consequências podem ser graves, incluindo roubo de identidade, vazamento de informações pessoais, danos à reputação e até mesmo prejuízos financeiros.

Em um cenário em constante evolução de ameaças cibernéticas, é fundamental que as organizações estejam constantemente atualizadas e atentas às novas vulnerabilidades que possam surgir, implementando medidas proativas para proteger os dados pessoais dos indivíduos e preservar sua segurança e privacidade.

No artigo "Privacidade, Monetização De Dados Pessoais e a LGPD: desafios e impactos da Lei nº 13.709/2018" de Thalyta Soares de Farias (2020), a autora aborda uma questão crucial no contexto da proteção de dados: as vulnerabilidades existentes nos sistemas utilizados para coletar, armazenar e tratar dados pessoais. Essas vulnerabilidades representam uma ameaça à segurança e privacidade das informações dos indivíduos, podendo resultar em violações de dados e potenciais danos.

A coleta de dados pessoais ocorre em diversos contextos, como no uso de aplicativos, redes sociais, sites de compras e transações online. Os sistemas responsáveis por essa coleta devem ser projetados de forma a garantir a segurança das informações fornecidas pelos usuários. No entanto, muitas vezes, esses sistemas apresentam vulnerabilidades que podem ser exploradas por agentes maliciosos.

Um estudo recente realizado pelo Instituto de Tecnologia de Massachusetts ("MIT")<sup>1</sup> e divulgado no Journal of Data and Information Quality da ACM (Association for Computing Machinery)<sup>2</sup> indica que houve um aumento de 493% nos incidentes de vazamento de informações no Brasil. Em 2019, mais de 205 milhões de registros de cidadãos brasileiros foram

---

<sup>1</sup> Massachusetts Institute of Technology: instituto de tecnologia localizado em Cambridge, Massachusetts, Estados Unidos.

<sup>2</sup> Association for Computing Machinery: associação profissional internacional de cientistas da computação.

criminosamente expostos. De acordo com a pesquisa, o país registrou 16 incidentes relevantes, um salto significativo em relação aos 3 ocorridos em 2018.

| Country      | 2018  |                   | 2019  |                   | Country              | 2018       |                      | 2019       |                       |
|--------------|-------|-------------------|-------|-------------------|----------------------|------------|----------------------|------------|-----------------------|
|              | Count | Volume of records | Count | Volume of records |                      | Count      | Volume of records    | Count      | Volume of records     |
| Africa       | 0     | 0                 | 1     | 30,000            | Italy                | 0          | 0                    | 1          | 3,000,000             |
| Australia    | 1     | 2,000,000         | 5     | 140,386,000       | Japan                | 0          | 0                    | 2          | 3,560,000             |
| Belgian      | 1     | 64,000            | 0     | 0                 | Lithuania            | 0          | 0                    | 1          | 14,000,000            |
| Brazil       | 3     | 34,600,000        | 16    | 205,186,219       | Malaysia             | 1          | 4,940,203            | 0          | 0                     |
| Bulgaria     | 0     | 0                 | 2     | 5,033,492         | Nederland            | 0          | 0                    | 1          | 250,000               |
| Canada       | 3     | 15,060,304        | 5     | 22,537,000        | New Zeland           | 0          | 0                    | 1          | 24,300,000            |
| Cayman       | 0     | 0                 | 1     | 600,000           | Norway               | 2          | 3,035,000            | 1          | 35,000                |
| Chile        | 0     | 0                 | 2     | 341,186           | Poland               | 1          | 2,200,000            | 1          | 2,200,000             |
| China        | 3     | 146,500,000       | 4     | 3,703,500,000     | Seychelles           | 0          | 0                    | 1          | 400,000               |
| Colombia     | 0     | 0                 | 1     | 2,400,000         | Singapore            | 1          | 1,500,000            | 1          | 808,000               |
| Cyprus       | 0     | 0                 | 1     | 108,000,000       | South Korea          | 0          | 0                    | 1          | 27,800,000            |
| Ecuador      | 0     | 0                 | 1     | 20,800,000        | Sweden               | 0          | 0                    | 1          | 299,055,819           |
| Estonia      | 0     | 0                 | 1     | 808,539,939       | Swiss                | 1          | 440,000,000          | 0          | 0                     |
| France       | 0     | 0                 | 2     | 7,400,600,000     | Turkey               | 0          | 0                    | 1          | 77,000                |
| German       | 3     | 42,871,432        | 1     | 800,000           | United Arab Emirates | 1          | 14,000,000           | 1          | 1,131,229             |
| Hong Kong    | 2     | 15,800,000        | 2     | 10,200,000        | U.K.                 | 1          | 380,000              | 3          | 21,612,000            |
| India        | 2     | 1,002,600,000     | 6     | 431,687,000       | U.S.                 | 134        | 2,312,620,111        | 185        | 5,559,343,789         |
| Iran         | 0     | 0                 | 1     | 15,000,000        | Unknown Country      | 0          | 0                    | 8          | 3,264,500,000         |
| Israel       | 1     | 92,283,889        | 3     | 9,950,000         |                      |            |                      |            |                       |
| <b>Total</b> |       |                   |       |                   |                      | <b>161</b> | <b>4,130,454,939</b> | <b>265</b> | <b>22,107,663,673</b> |

**Figura 1.** Volume de registros por país.

**Fonte:** J. Data and Information Quality, Vol. 13, No. 1, Article 3, Publication date: January 2021.

Esses dados englobam os dois grandes vazamentos recentemente divulgados pela empresa de segurança cibernética PSafe, ocorridos no Brasil. O primeiro vazamento envolveu cerca de 223 milhões de números de CPF, contendo informações pessoais de indivíduos falecidos e vivos, como identidades e datas de nascimento. Além disso, foram expostas informações de 104 milhões de veículos e 40 milhões de empresas, incluindo CNPJ, razão social, nome fantasia e data de constituição. O segundo vazamento revelou detalhes precisos de 140 milhões de pessoas, como números de telefone, histórico acadêmico, salário, endereços, mudanças de cidade e fotografias. Essas informações permaneceram expostas durante meses ou até mesmo anos, sem que seja possível determinar quantas vezes foram compartilhadas e comercializadas.

É importante ressaltar que essas vulnerabilidades não estão restritas apenas ao ambiente digital, mas também podem ocorrer em ambientes físicos, como a perda ou roubo de dispositivos de armazenamento contendo dados pessoais, ou a negligência no descarte seguro de documentos impressos.

Diante desse cenário, é fundamental que as empresas e organizações adotem medidas efetivas para identificar, prevenir e mitigar as vulnerabilidades nos sistemas de coleta,

armazenamento e tratamento de dados pessoais. Isso envolve a implementação de políticas de segurança da informação, a realização de auditorias de segurança regulares, a adoção de práticas de criptografia robustas, a conscientização e treinamento dos colaboradores, e o cumprimento das diretrizes estabelecidas pela legislação de proteção de dados, como a LGPD.

A conscientização dos usuários também desempenha um papel crucial na proteção contra vulnerabilidades. Os indivíduos devem ser informados sobre riscos envolvidos na divulgação de seus dados pessoais, bem como melhores práticas de segurança que podem adotar, como a utilização de senhas fortes, a ativação da autenticação de dois fatores e a verificação da segurança dos sites acessados.

Em suma, a crescente exposição de vulnerabilidades nos sistemas de tratamento de dados pessoais destaca a importância da segurança cibernética e da proteção de informações pessoais. As organizações e indivíduos devem estar vigilantes e tomar medidas proativas para garantir a integridade, confidencialidade e disponibilidade dos dados pessoais, evitando potenciais danos e violações de privacidade. Além disso, o cumprimento dos princípios estabelecidos na legislação de proteção de dados, como a LGPD, desempenha um papel fundamental na promoção de práticas seguras e responsáveis de tratamento de dados pessoais.

## **Considerações Finais**

Este trabalho investigou a proteção de dados pessoais na era da informação, explorando os mecanismos de segurança jurídica destinados a preservar a privacidade do indivíduo em um cenário de crescente exposição de informações pessoais. O tema revelou-se de extrema relevância, uma vez que a era digital trouxe consigo um fluxo sem precedentes de dados pessoais, demandando ações eficazes para equilibrar a utilização dessas informações com a garantia da privacidade individual.

Reforçando a importância do tema, foi destacado que a proteção de dados pessoais é um direito fundamental que afeta a dignidade e a autonomia dos indivíduos. A integridade dessas informações é vital, pois sua exposição indevida pode resultar em consequências sérias, incluindo violações de privacidade, roubo de identidade e danos à reputação. Portanto, a necessidade de mecanismos legais e práticos que assegurem essa proteção é inegável.

Ao longo desta pesquisa, foram obtidos importantes resultados que contribuem para a compreensão desse cenário complexo. Analisando as consequências da violação da legislação de proteção de dados, foi identificado que sanções e penalidades efetivas são essenciais para garantir a conformidade das empresas e organizações. A avaliação da responsabilidade das

empresas e órgãos como controladores de dados destacou a necessidade de implementação de medidas de segurança robustas, o que inclui políticas internas, treinamento de funcionários e auditorias periódicas.

Além disso, a pesquisa evidenciou que a aprovação de leis específicas de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no contexto brasileiro, trouxe mudanças significativas. Essas leis estabeleceram diretrizes claras, princípios fundamentais e a criação de autoridades reguladoras, como a Autoridade Nacional de Proteção de Dados (ANPD). Isso reflete um avanço notável na proteção da privacidade e na promoção da segurança jurídica nas relações de tratamento de dados.

De forma concisa, este estudo reforçou a importância da proteção de dados pessoais na era da informação e resumiu os principais resultados obtidos. A segurança jurídica e a preservação da privacidade individual devem permanecer no centro das discussões à medida que avançamos em um mundo cada vez mais conectado digitalmente. A busca por um equilíbrio eficaz entre a utilização de dados e a proteção da privacidade é essencial para garantir uma sociedade mais justa e segura.

## **Referências**

AGOSTINELLI, Joice. A importância da lei geral de proteção de dados pessoais no ambiente online. ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498, v. 14, n. 14, 2018.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Ed. Forense Ltda, 2019.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 10 de setembro de 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, ano 155, nº 157, p. 1-3, 15 ago. 2018. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-](https://www.planalto.gov.br/ccivil_03/_ato2015-)

2018/2018/lei/l13709.htm. Acesso em: 13 de set. de 2023.

CORACCINI, Rapahael. " Fotos e até salários estão entre os dados vazados de 223 milhões de brasileiros ". CNN BRASIL. Disponível em: <https://www.cnnbrasil.com.br/economia/fotos-e-ate-salarios-estao-entre-os-dados-vazados-de-223-milhoes-de-brasileiros/>. Acesso em: 14 de set. de 2023.

FARIAS, Thalyta Soares de. Privacidade, monetização de dados pessoais e a LGPD: desafios e impactos da Lei Nº 13.709/2018. 2020.

PINHEIRO, Patricia Peck. Proteção de dados pessoais – Comentários à Lei N. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

SOARES, Rafael Ramos. Lei geral de proteção de dados–LGPD: direito à privacidade no mundo globalizado. 2020.

Revista de Qualidade de Dados e Informação. Volume 13. Edição 1. Artigo n.º: 3 pag. 1–33. Disponível em: <https://doi.org/10.1145/3439873>. Acesso em: 13 de set. de 2023.

VOCÊ S/A. Vazamentos de dados aumentaram 493% no Brasil, segundo pesquisa do MIT [online]. Disponível em: <https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit>. Acesso em: 13 de set. de 2023.