UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
CURSO DE ENGENHARIA DA COMPUTAÇÃO

HILTON OLIVEIRA SEGUNDO

AS BASES LEGAIS DA LEI GERAL DE PROTEÇÃO DE DADOS: um estudo sobre o papel do profissional de Tecnologia da Informação

SÃO LUÍS
2023

HILTON OLIVEIRA SEGUNDO

AS BASES LEGAIS DA LEI GERAL DE PROTEÇÃO DE DADOS: um estudo sobre o papel do profissional de Tecnologia da Informação

Trabalho de Conclusão de Curso apresentado à coordenação do curso de Engenharia da Computação da Universidade Federal do Maranhão para obtenção de título de Bacharel em Engenharia da Computação.

Orientador: Sérgio Souza Costa

SÃO LUÍS

2023

Oliveira Segundo, Hilton.
AS BASES LEGAIS DA LEI GERAL DE PROTEÇÃO DE DADOS : um estudo sobre o papel do profissional de Tecnologia da Informação / Hilton Oliveira Segundo. - 2023.
46 f.

Orientador(a): Sergio Souza Costa.
Monografia (Graduação) - Curso de Engenharia da Computação, Universidade Federal do Maranhão, São Luís, 2023.

1. Direito à privacidade. 2. Lei Geral de Proteção de Dados. 3. Tecnologia da Informação. I. Costa, Sergio Souza. II. Título.

HILTON OLIVEIRA SEGUNDO

AS BASES LEGAIS DA LEI GERAL DE PROTEÇÃO DE DADOS: um estudo sobre o papel do profissional de Tecnologia da Informação

Trabalho de Conclusão de Curso apresentado à coordenação do curso de Engenharia da Computação da Universidade Federal do Maranhão para obtenção de título de Bacharel em Engenharia da Computação.

Orientador: Sérgio Souza Costa

Aprovado em: 20/12/2023

BANCA EXAMINADORA

_____

Prof. Sérgio Souza Costa (orientador)

Doutor em Computação Aplicada

_____

Prof. Bruno Feres de Souza

Doutor em Ciências da Computação e Matemática Computacional

_____

Prof. Davi Viana dos Santos

Doutor em Informática

AGRADECIMENTOS

Agradeço aos meus pais e padrasto, que sempre me apoiaram em toda a minha jornada acadêmica, me incentivando a continuar e persistir apesar de todos os percalços que apareciam em minha frente.

À minha namorada, Mauritânia Gomes, por ser minha parceira durante todo o caminho que eu percorri nos cursos que fiz e principalmente por não me deixar desistir de nada, me tornando mais forte e fazendo com que eu me sentisse capaz de realizar qualquer coisa que eu quisesse.

Agradeço a Universidade Federal do Maranhão por me oportunizar partilhar uma porcentagem da minha vida ao meu aprimoramento pessoal e profissional. Nela aprendi a minha profissão e descobri meu lugar no mundo, sou muito grato por carregar o nome da UFMA em um diploma e agora em um segundo, e é só o começo.

A todos os meus amigos, professores da Universidade, agradeço a cada um por sua disponibilidade e ensinamentos diários, tudo foi muito importante durante a minha jornada profissional. Agradeço aos professores que aceitaram participar da banca examinadora deste trabalho, professor Bruno e Davi, todos os ensinamentos foram muito importantes durante as aulas, cada aprendizagem que tive foi muito importante no meu crescimento pessoal e profissional. Agradeço principalmente ao meu orientador e coordenador de curso, Sérgio Souza Costa, que apesar de toda a minha falta de tempo, sempre entendeu que o meu ofício precisava ser valorizado e não visto como segundo plano dentro da universidade.

“A vida é combate”

(Gonçalves Dias)

RESUMO

O trabalho é uma discussão sobre a aplicabilidade da Lei Geral de Proteção de Dados para os profissionais da área de Tecnologia da Informação. O objetivo da presente pesquisa é investigar como a função dos profissionais da área se relaciona com a lei e quais os desafios enfrentados para efetivá-la. O trabalho utiliza apenas a pesquisa bibliográfica como metodologia, para investigar o que está sendo discutido da literatura sobre a lei. Além disso, é abordada a Lei Geral de Proteção de Dados como principal fonte documental, fazendo a análise dos princípios norteadores da lei, direitos dos titulares dos dados e deveres das organizações que tratam os dados. O texto expõe a importância da lei para a população, baseado no atual cenário tecnológico brasileiro. Além disso, a pesquisa apresenta a discussão acerca de outras legislações de privacidade, fazendo o comparativo das leis do Japão, União Europeia e Califórnia com a legislação brasileira. Também há o debate sobre o papel do profissional de tecnologia perante a lei, como protagonista para resguardar a privacidade dos usuários. Como resultado, a pesquisa apresenta os desafios enfrentados para a implementação da lei, no que diz respeito ao que as organizações estão fazendo atualmente para efetivá-la e o que os profissionais da área de tecnologia poderão enfrentar no trabalho para executar a lei de maneira satisfatória dentro das atuais possibilidades. Ademais, o trabalho expõe como consideração final a compreensão das dificuldades enfrentadas no que diz respeito à aplicação da lei e o reconhecimento do futuro promissor, especialmente no Brasil. A pesquisa apresenta ainda a urgência da implementação da Lei Geral de Proteção de Dados para garantir avanços na segurança da informação.

Palavras-chave: Lei Geral de Proteção de Dados. Direito à privacidade. Tecnologia da Informação.

ABSTRACT

The work is a discussion on the applicability of the General Data Protection Law to professionals in the Information Technology field. The aim of this research is to investigate how the role of IT professionals relates to the law and what challenges they face in enforcing it. The work solely employs bibliographic research as a methodology to explore what the literature discusses about the law. Additionally, the General Data Protection Law is approached as the main documentary source, analyzing the guiding principles of the law, the rights of data subjects, and the duties of organizations handling the data. The text highlights the importance of the law for the population, based on the current technological scenario in Brazil. Furthermore, the research discusses other privacy legislations, comparing the laws of Japan, the European Union, and California with Brazilian legislation. There is also a debate on the role of the technology professional in relation to the law, acting as a protagonist in safeguarding user privacy. As a result, the research presents the challenges faced in implementing the law, addressing what organizations are currently doing to enforce it and what technology professionals may encounter in their efforts to execute the law satisfactorily within current possibilities. Moreover, the work concludes by highlighting the understanding of the difficulties in applying the law and recognizing the promising future, especially in Brazil. The research also emphasizes the urgency of implementing the General Data Protection Law to ensure advancements in information security.

Keywords: General Data Protection Law. Right to privacy. Professional work in Information Technology.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

A crescente digitalização e o aumento da utilização de tecnologias de informação têm gerado um enorme volume de dados pessoais sendo coletados, processados e armazenados por organizações de diversos setores. Segundo Oliveira (2023) esse fato figura-se como um problema, pois a coleta de dados de forma desordenada tende a levar à violação dos direitos pessoais e à exposição indevida de informações sensíveis. Trazendo, assim, grandes desafios relacionados à privacidade e segurança das informações, que exigem a implementação de regulamentações que garantam a proteção adequada dos direitos dos indivíduos.

É nesse sentido que a Lei Geral de Proteção de Dados (LGPD) é promulgada, com o objetivo de "[...] proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural." (BRASIL, 2018, não paginado).

Com o aumento do uso da rede mundial de internet e o mundo cada vez mais globalizado, percebe-se a importância de tratar os dados dos usuários de forma responsiva e segura, potencializado pela promulgação da LGPD. Todavia, surge a necessidade de conhecer qual o profissional habilitado para protagonizar a busca pelo resguardo dos dados pessoais.

Apesar da Lei prever a Autoridade Nacional de Proteção de Dados (ANPD), apenas um órgão nacional não é capaz de garantir a prevalência do disposto em lei, pois é necessário um trabalho de treinamento e conscientização de tratadores dos dados para que conheçam e implementem o previsto em lei de forma permanente.

Pensando nisso, surge o questionamento: "Qual é o papel do profissional de TI diante da LGPD, considerando as bases legais da legislação e o tratamento da privacidade dos dados pessoais, e quais são os desafios enfrentados por esses profissionais nesse contexto?"

Portanto, a presente pesquisa tem por objetivo analisar o papel do profissional de Tecnologia da Informação na aplicação da Lei Geral de Proteção de Dados por meio de uma abordagem baseada em pesquisa bibliográfica, investigando o que

está sendo discutido em meio acadêmico sobre as relações entre esses profissionais e a LGPD.

Para o alcance desse objetivo, foram traçados objetivos específicos, a saber:

a) Discutir as diretrizes da LGPD e as suas relações com a proteção da privacidade de dados pessoais;

b) Avaliar os impactos causados pela lei e os desafios enfrentados pelas empresas;

c) Analisar o papel do profissional de tecnologia da informação, identificando suas responsabilidades na gestão de dados sensíveis.

Para o alcance do resultado, foi utilizada a pesquisa bibliográfica a fim de identificar o quanto o papel do profissional de TI perante a Lei está sendo discutido, além de analisar de que forma é apresentada essa relação. Consonante a isso, Fernandes (2022) em sua dissertação, entrevistou profissionais de TI e revelou que 10% dos entrevistados desconhecem os princípios da Lei Geral de Proteção de Dados, além disso, informa que cerca de 25% dos entrevistados estão cientes de que os seus próprios dados pessoais podem ser compartilhados a qualquer momento pelas organizações. Esse resultado revela a pequena quantidade de conhecimento dos profissionais perante a lei.

Como conclusão, obteve-se que a LGPD está sendo implementada nas empresas, apesar de não ser vista ainda com a prioridade merecida. Além disso, os grandes desafios são superáveis, caso sejam levados em consideração as adversidades trazidas pela lei.

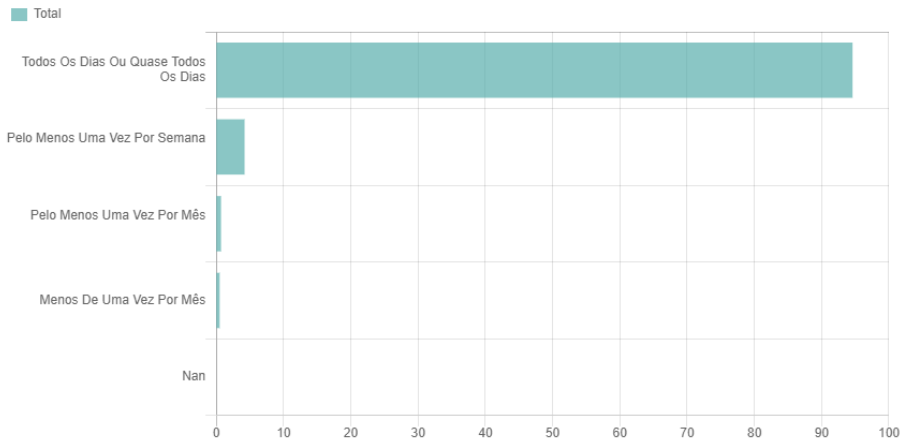
2 MARCOS LEGAIS DA LEI GERAL DE PROTEÇÃO DE DADOS

A LGPD representou um marco significativo para o Brasil, estabelecendo normativas essenciais para a proteção da privacidade e segurança das informações pessoais dos cidadãos. Este capítulo propõe uma análise detalhada das bases legais que fundamentam a LGPD, proporcionando uma compreensão aprofundada das responsabilidades e direitos delineados por essa legislação, através da discussão dos princípios norteadores da lei e as relações entre direitos e deveres dos titulares dos dados e as organizações empresariais.

Devido à crescente ascensão da internet no mundo moderno e todas as transformações que ela causa, percebe-se que desenvolveu-se uma dependência muito grande de todo o potencial fornecido pela web. Segundo Faccioni Filho (2016), a internet como nós a conhecemos possui somente cerca de 30 anos em nossa sociedade, e ainda assim ela já é essencial para diversas tarefas do dia a dia, como negócios, relacionamentos, lazer e até mesmo atividades corporativas, como trabalhar ou pagar contas.

Em razão deste fator, tem-se em mente que os usuários tornam-se cada vez mais envolvidos ao que tange o uso da internet, como redes sociais, sites de busca, jogos, e até mesmo no uso de aparelhos domésticos. O que é corroborado segundo os dados fornecidos pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC), em que indica que mais de 90% dos indivíduos consultados pela pesquisa, utilizam a internet todos os dias, conforme exibe a figura 1.

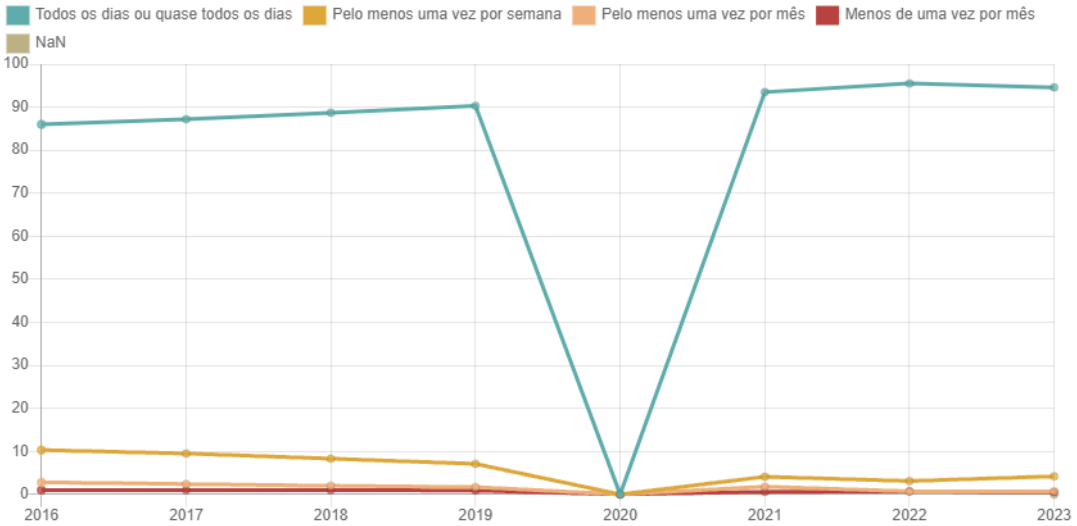
Figura 1 - Usuários de internet, por frequência de uso



Fonte: CETIC, 2023.

A pesquisa do CETIC, tem os indicadores do TIC (Tecnologia de Informação e Comunicação) do CGI.br (Comite Gestor da Internet no Brasil) realizadas em domicílios, empresas, governo, organizações sem fins lucrativos, escolas, estabelecimentos de saúde. Ainda conforme o CETIC (2023), percebe-se que houve uma crescente no percentual de usuários que utilizam da internet todos os dias, conforme exibe figura 2.

Figura 2 - Usuários de internet, por frequência de uso no decorrer dos anos



Fonte: CETIC, 2023.

O trecho em queda representa o período de pandemia de COVID-19 no ano de 2020, em que, por conta da situação atual em questão, não houve a realização da pesquisa no ano corrente.

De acordo com a crescente integração dos usuários à internet e o constante aprimoramento dos softwares, nota-se uma tendência persistente de aumento no compartilhamento de informações pessoais e no monitoramento comportamental. Embora essa dinâmica possa contribuir para a melhoria da experiência do usuário, cria problemas significativos no que tange a privacidade.

Rosa, Casagranda e Spinelli (2017) realizaram uma pesquisa sobre a importância do marketing digital utilizando a influência do comportamento do consumidor. As autoras apresentam que as empresas investem muito capital em ferramentas que possibilitem entender o consumidor e poder assim direcionar o seu produto para um determinado grupo, buscando assim aumento dos lucros, e quando o marketing começa a utilizar a internet, seu alcance se expandiu.

Dessa forma, percebe-se que os dados pessoais têm se tornado uma grande forma de riqueza devido ao que pode ser proporcionado aos usuários através do que é atrelado ao seu perfil. Essas informações são baseadas nos dados que são fornecidos com ou sem consentimento ao utilizar a internet.

Portanto a LGPD age nesse âmbito como um regulador de como as informações pessoais podem ou não ser manipuladas. A LGPD

> [...] dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018, não paginado).

A LGPD dispõe que, todo dado pessoal é tido como importante, e por esse fato foi mantido um conceito bem amplo acerca do tema, englobando toda informação que possa ser relacionada a uma pessoa natural identificada ou identificável (TEFFÉ; VIOLA, 2020). A abordagem ampla do conceito de dados pessoais revela a importância da privacidade e da proteção aos indivíduos e visa ainda garantir que as empresas e organizações que tratem de dados pessoais estejam sujeitas às obrigações quanto às obrigações legais contidas na lei.

Dessa forma, a lei surge como resposta às crescentes demandas por regulamentações que garantem a proteção dos dados em um cenário digital em constante evolução. Inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a legislação brasileira dispõe de cláusulas importantes para o tratamento de informações pessoais no país.

Os princípios estabelecidos na LGPD são fundamentais para orientar o tratamento adequado dos dados pessoais. Desde a transparência nas práticas de coleta e uso até a responsabilização das organizações pelo manejo adequado dessas informações, cada princípio é analisado em profundidade. Compreender esses fundamentos é essencial para garantir a conformidade e a ética no tratamento de dados.

A LGPD não apenas estabelece direitos e deveres, mas também prevê avaliações para o não cumprimento de suas disposições. Multas, adaptadas à gravidade da infração e ao porte da organização, são discutidas em detalhes. A compreensão destas implicações legais é crucial para motivar as organizações a

adotarem práticas de tratamento de dados em conformidade com a legislação, promovendo a responsabilidade e a seriedade na proteção de dados.

2.1 Princípios norteadores da proteção de dados

Para o melhor entendimento acerca da criação da Lei, é imprescindível a compreensão acerca dos fundamentos ou diretrizes que orientam e guiam ações, decisões e comportamentos no contexto da Lei. Os princípios norteadores funcionam como pontos de referência, fornecendo uma base ética ou regulatória para orientar o desenvolvimento de políticas, práticas e normas em uma área específica.

No contexto da LGPD, os princípios norteadores referem-se aos princípios fundamentais que delineiam como as organizações devem tratar e proteger os dados pessoais dos indivíduos. Esses princípios são estabelecidos para garantir a privacidade, a segurança e a transparência no que diz respeito a informações pessoais, promovendo uma abordagem ética e responsável no contexto do tratamento de dados.

Esses princípios incluem:

a) transparência;
b) adequação;
c) necessidade;
d) livre acesso;
e) qualidade dos dados;
f) segurança;
g) prevenção;
h) não discriminação; e
i) responsabilização.

É através desses princípios que a lei se alicerça para o desenvolvimento e a implementação de práticas que respeitam os direitos dos titulares dos dados, promovendo uma cultura de proteção de dados e conformidade legal. Segundo Santos (2021)

> [...] os regramentos que estabeleceram os princípios legais da proteção dos dados são de grande imperiosidade, porque ampliam o sistema de proteção ao consumidor, dando a este o direito de determinar os limites à fruição desses dados, limites esses que não podem ser engessados por contratos de adesão ou em meros “Termos de uso”, onde o consumidor não possui verdadeira autonomia decisória[...] (SANTOS, 2021, p. 229).

Os princípios norteadores da Lei Geral de Proteção de Dados (LGPD) desempenham um papel fundamental na definição das diretrizes éticas e operacionais para o tratamento de dados pessoais. Cada um desses princípios representa um alicerce essencial para a construção de uma cultura organizacional que promova a privacidade e a segurança dos dados.

A transparência destaca a importância de tornar claro todas as ações relacionadas ao tratamento de dados pessoais. As organizações devem comunicar de maneira inequívoca aos titulares sobre como seus dados serão coletados, utilizados, processados e armazenados. A transparência reforça a confiança entre as partes envolvidas e permite que os indivíduos tomem decisões informadas sobre o compartilhamento de suas informações.

A finalidade se relaciona com a coleta e o processamento de dados que devem ser realizados com propósitos específicos, claros e legítimos. As organizações devem definir objetivos claros para o uso dos dados desde o início, evitando desvios que possam comprometer a privacidade dos titulares. A garantia da garantia fortalece a confiança dos indivíduos no tratamento de suas informações.

O princípio de adequação diz respeito à coleta e o tratamento de dados que devem ser fornecidos e adequados aos objetivos pretendidos. Isso implica que as organizações não devem coletar mais dados do que o necessário para alcançar a finalidade pretendida. A garantia garante que o processamento seja limitado ao necessário, evitando excessos e preservando a privacidade dos titulares.

Relacionado à adequação, o princípio da necessidade enfatiza a importância de limitar o tratamento de dados apenas ao que é essencial para atingir a pretendida. Evitar a coleta de dados desnecessários reduz o risco de exposição indevida e protege a privacidade dos titulares.

Os titulares dos dados devem ter o direito de acessar suas informações pessoais de forma fácil e gratuita para adequar-se ao princípio de acesso livre. É

através dele que é promovida a transparência e empoderamento dos indivíduos, permitindo que tenham consciência de como suas informações estão sendo utilizadas e possam exercer seus direitos de controle sobre seus próprios dados.

O princípio de qualidade dos dados diz respeito à responsabilidade que as organizações têm de garantir a precisão e a atualização dos dados pessoais que possuem. A qualidade dos dados está intrinsecamente ligada à confiabilidade das informações utilizadas, garantindo que as decisões básicas desses dados sejam precisas e éticas.

O estabelecimento da obrigação de implementar medidas técnicas e organizacionais para garantir a segurança dos dados pessoais está relacionado com o princípio de segurança. Para isso, as organizações devem adotar práticas robustas para proteger as informações contra acessos não autorizados, vazamentos ou qualquer forma de tratamento inadequada.

A LGPD enfatiza a necessidade de adoção de medidas preventivas para evitar incidentes de segurança e transparência de dados, como um dos critérios da prevenção. A prevenção envolve a implementação de protocolos de segurança, treinamento de pessoal e promoção de uma cultura organizacional que prioriza a proteção da informação desde a coleta até o descarte.

Além disso, o tratamento de dados pessoais não deve resultar em discriminação injusta ou ilegal. As organizações devem garantir que suas práticas não perpetuem desigualdades, respeitando a diversidade e promovendo a equidade no tratamento dos titulares.

As organizações são responsáveis por demonstrar conformidade com a LGPD, adotando práticas transparentes e seguras. A responsabilização envolve a criação e implementação de políticas internas, a realização de avaliações de impacto à privacidade, e a prestação de contas às autoridades e aos titulares em caso de incidentes.

Estes princípios, interligados e complementares, formam a espinha dorsal da LGPD, orientando ações e decisões no tratamento responsável e ético dos dados pessoais. A compreensão e aplicação desses princípios são cruciais para garantir a

conformidade legal e promover uma cultura de respeito à privacidade no ambiente digital.

2.2 Direitos e deveres através da LGPD

A LGPD confere aos titulares dos dados uma série de direitos essenciais para garantir o controle e a privacidade de suas informações pessoais. Simultaneamente, impõe obrigações claras às organizações que tratam esses dados. Esta seção explora detalhadamente esses direitos e deveres, destacando a dinâmica entre titulares e responsáveis pelo tratamento.

2.2.1 Direitos dos Titulares

No contexto da LGPD, os direitos dos titulares dos dados são prerrogativas concedidas às pessoas físicas cujos dados pessoais são objeto de tratamento por organizações. Esses direitos conferem aos titulares um maior controle sobre suas informações pessoais, permitindo-lhes tomar decisões informadas e resguardar a privacidade.

De acordo com o previsto no artigo 17 da Lei, “Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade”. (BRASIL, 2018, não paginado)

Nesse sentido, são incluídos o direito de acessar informações sobre o tratamento de seus dados, solicitar retificações, exigir a exclusão de informações, opor-se a determinados tipos de tratamento e até mesmo solicitar a portabilidade de seus dados para outros serviços. Ao conceder esses direitos, a LGPD busca capacitar os indivíduos, promovendo a transparência e a autonomia no âmbito de suas informações pessoais, ao mesmo tempo em que reforça a responsabilidade das organizações no tratamento ético e legal desses dados.

No artigo 18, a LGPD aborda que “O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição” (BRASIL, 2018, não paginado). Essa requisição pode se apresentar em diversas formas, através de diversos motivos mencionados em lei, nos parágrafos I a IV, descritos a seguir.

a) “I - Confirmação da existência de tratamento” (BRASIL, 2018, não paginado);

Esse ponto ressalta a importância dos titulares dos dados terem o direito de confirmar se suas informações são objeto de tratamento por parte das organizações. Essa confirmação é essencial para a transparência no uso de dados, permitindo que os indivíduos tenham conhecimento de como suas informações estão sendo manipuladas.

b) “II - Acesso aos dados” (BRASIL, 2018, não paginado);

O acesso aos dados fornece aos titulares a capacidade de obter informações sobre o tratamento de suas informações pessoais. Esse direito promove a transparência e empodera os indivíduos, permitindo que saibam quais dados estão sendo processados e para quais específicas.

c) “III - Correção de dados incompletos, inexatos ou desatualizados” (BRASIL, 2018, não paginado);

Esse ponto destaca a importância dos titulares poderem solicitar a correção de dados que estejam incorretos ou desatualizados. Essa prerrogativa garante a precisão das informações, evitando decisões equivocadas ou impactos negativos decorrentes de dados imprecisos.

d) “IV - Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei” (BRASIL, 2018, não paginado);

Esse direito visa proteger os titulares de informações desnecessárias ou excessivas, bem como de dados tratados em desconformidade com a legislação. A possibilidade de anonimização, bloqueio ou eliminação garante que apenas os dados pertinentes e legalmente tratados sejam mantidos pelas organizações.

e) V - Portabilidade de dados para outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, coleta de segredos comerciais e industriais” (BRASIL, 2018, não paginado);

A portabilidade permite que os titulares movam seus dados de um provedor de serviço para outro, facilitando a mobilidade e a escolha dos usuários. Esse ponto destaca a importância de regulamentações que respeitem segredos comerciais e industriais para garantir um equilíbrio adequado.

f) “VI - Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei” (BRASIL, 2018, não paginado);

Esse direito garante que os titulares possam solicitar a eliminação de seus dados pessoais, especialmente quando a autorização para o tratamento não for mais desejada. A exceção prevista no artigo 16 reforça a necessidade de considerar situações específicas que justifiquem a retenção dos dados.

g) “VII - Informação das entidades públicas e privadas com as quais o controlador fez uso compartilhado de dados” (BRASIL, 2018, não paginado);

A transparência sobre o uso compartilhado de dados é fundamental para que os titulares tenham consciência das entidades envolvidas. Essa informação permite uma compreensão mais abrangente do ecossistema de tratamento de dados e contribui para a confiança nas práticas das organizações.

h) “VIII - Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa” (BRASIL, 2018, não paginado);

Este ponto destaca a importância de informar os titulares sobre a opção de não fornecer consentimento para o tratamento de dados, bem como as implicações dessa decisão. Essa transparência é crucial para garantir escolhas informadas por parte dos titulares.

i) “IX - Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei” (BRASIL, 2018, não paginado);

Esse direito permite que os titulares revoguem o consentimento fornecido anteriormente. A previsão nos termos do § 5º do artigo 8º estabelece as condições e procedimentos para a revogação, assegurando um processo claro, gratuito e acessível aos titulares (BRASIL, 2018).

Em resumo, os direitos conferidos aos titulares da LGPD representam um avanço significativo na segurança da privacidade e no empoderamento dos indivíduos sobre o tratamento de suas informações pessoais. Estas prerrogativas não apenas estabelecem uma relação de transparência entre as organizações e os titulares, mas também reforçam a responsabilidade ética e legal das instituições no gerenciamento desses dados sensíveis. Na próxima seção, serão explorados os deveres impostos às organizações pela LGPD, delineando como estes devem agir para garantir o cumprimento adequado da legislação e a proteção efetiva dos direitos dos titulares. O entendimento da dinâmica entre direitos e deveres é crucial para promover uma cultura de tratamento de dados pautada pela ética, transparência e conformidade legal.

2.2.2 Deveres das Organizações

As organizações que utilizam os dados pessoais precisam seguir uma série de diretrizes impostas pela LGPD. Essas diretrizes representam obrigações para garantir a conformidade da lei e a efetivação da proteção da privacidade dos dados dos titulares.

Estas responsabilidades vão desde a obrigação de fornecer informações claras e transparentes sobre o processamento de dados até à implementação de fortes medidas de segurança e à comunicação de incidentes de segurança. A importância destas responsabilidades diz respeito à promoção de práticas éticas e transparentes, além de tratar sobre a construção de uma relação de confiança entre a organização e os seus consumidores. Com o cumprimento das responsabilidades, as instituições demonstram o compromisso com a proteção dos dados e com a confiança dos seus clientes, resultando em uma boa reputação para a empresa.

Os deveres das organizações apresentados na lei estabelecem padrões éticos a serem seguidos e garantem a construção de um ambiente digital mais seguro e respeitoso.

No artigo 9, é apresentado que

> [...] o titular [dos dados] tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso. (BRASIL, 2018, não paginado).

Nesse sentido, entende-se que as organizações são responsáveis por fornecer as informações sobre como os dados dos clientes estão sendo tratados, representando o dever de informação. Em consonância a isso, o artigo 46 da lei trata sobre a obrigação da adoção de medidas de garantia da segurança dos dados (BRASIL, 2018). Em concordância, Santi (2020) aborda que este artigo assegura a proteção do princípio da dignidade da pessoa humana e do direito à personalidade.

Somando-se a isso, o artigo 47 da lei trata sobre o sigilo, revelando que o tratador ou qualquer outra pessoa é obrigada a garantir a segurança da informação dos dados pessoais (BRASIL, 2018). É importante mencionar que o artigo 47 menciona na lei os casos pós-contratuais, como por exemplo após o término da aquisição de um serviço, produto ou vínculo empregatício. Em análise disto, Bioni (2020) discute que após o tratamento dos dados, caso estes não sejam excluídos por qualquer que seja o motivo o tratamento dos dados ainda de acordo com a lei.

> A LGPD estabelece a necessidade de que, sempre que possível, haja a anonimização dos dados utilizados em pesquisas (arts. 7º, IV; 11, II, “c”, 13 e 16, II), assim como determina que, embora uma das exceções à eliminação dos dados após o término do tratamento seja o uso exclusivo do controlador, ela está condicionada à vedação do acesso aos dados por terceiro e à anonimização dos dados (art. 16, IV). (BIONI, 2020, p. 106).

Outro ponto interessante a ser discutido é o apresentado no artigo 48 da lei, que prevê que o responsável pelos dados deverá comunicar ao titular dos dados e à autoridade nacional “[...] a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.” (BRASIL, 2018, não paginado). Essa autoridade nacional também é prevista em lei, embora grande parte dos artigos relacionados tenha sido vetada. Com a lei nº 14.460 de 2022 a Autoridade Nacional de Proteção de Dados (ANPD), essa instituição é reforçada como órgão fiscalizador da LGPD.

De acordo com Bezerra (2019), essas autoridades são fundamentais para zelar pela proteção dos dados, como o principal órgão para fiscalizar e conscientizar a população acerca dos seus interesses. A autora menciona ainda as ANPDs de outros países que já consolidaram a proteção de dados, como na União Europeia. As leis internacionais e seus respectivos órgãos fiscalizadores serão mencionados no decorrer do trabalho.

3 PROTEÇÃO DE DADOS NO CONTEXTO INTERNACIONAL

Em um mundo cada vez mais interconectado, a proteção de dados no contexto internacional tornou-se um equilíbrio entre a necessidade de resguardar informações e a busca por estabilidade na era digital.

Em resposta a essas questões, diversas nações têm promulgado legislações específicas para a proteção de dados pessoais, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, a Lei de Proteção de Informações Pessoais (APPI) no Japão e a Lei de Privacidade do Consumidor da Califórnia (CCPA) nos Estados Unidos, contudo, não há apenas essas, mas citamos essas a fim de comparação. Todas essas legislações vêm buscando assegurar os direitos individuais e regulamentar a coleta, armazenamento e utilização dessas informações. Tais normativas visam estabelecer um equilíbrio entre o avanço tecnológico e a salvaguarda da privacidade, oferecendo uma forma legal para enfrentar os desafios emergentes no cenário digital.

3.1 *General Data Protection Regulation*

A GDPR (*General Data Protection Regulation*) foi implementada para substituir a Diretiva de Proteção de Dados da UE de 1995, visando fortalecer e modernizar as regras de privacidade devido aos avanços tecnológicos e à crescente importância da privacidade das informações pessoais.

Descreve em seu texto que a lei

> [...] deve aplicar-se a todos os assuntos relacionados com a proteção de direitos e liberdades fundamentais no que diz respeito ao tratamento de dados pessoais que não estão sujeitos a obrigações específicas [...] (*THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*, 2016, não paginado).

A regulamentação se assemelha muito a LGPD, tendo diferenças principalmente nas quantidades de cada termo, sendo que na verdade asseguram as mesmas coisas, mas com divisões diferentes. Contudo, a regulamentação europeia é bem mais severa quanto às multas aplicadas, tendo em vista que podem chegar a 4% do faturamento anual de uma empresa, com valor máximo de 20 milhões de euros, enquanto que na LGPD apenas 2%, ou 50 milhões de reais, cerca de 9,5 milhões de euros.

A GDPR tem como objetivo fortalecer e unificar as leis de proteção de dados para todos os países membros da União Europeia, tratando três principais objetivos: a proteção de pessoas naturais no que diz respeito ao tratamento de dados pessoais, proteger os direitos e liberdades fundamentais das pessoas naturais, e sobre o livre movimento de dados pessoais dentro da União. (*THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*, 2016).

Segundo Zaeem e Barber (2020), Os principais objetivos do GDPR são dar aos indivíduos o controle sobre seus dados pessoais e unificar o regulamento dentro da União Europeia para facilitar os negócios. como: Legalidade, justiça e transparência, Limitação de finalidade, minimização de dados, precisão, limitação de armazenamento, integridade e confidencialidade (segurança), responsabilidade.

3.2 *Act on the Protection of Personal Information*

A Lei de Proteção de Informações Pessoais (APPI) é a principal legislação de proteção de dados pessoais no Japão. A APPI tem como objetivo.

> [...] proteger os direitos e interesses individuais, considerando a utilidade das informações pessoais, incluindo que a aplicação adequada e eficaz dessas informações contribui para a criação de novas indústrias e a realização de uma sociedade econômica vibrante [...]. (*PERSONAL INFORMATION PROTECTION COMMISSION*, 2017, não paginado).

A APPI define como informações pessoais qualquer informação que possa ser usada para identificar uma pessoa, direta ou indiretamente. Isso inclui informações como nome, endereço, número de telefone, número de identificação, dados de saúde, informações financeiras e registros de compras.

Impõe ainda uma série de obrigações às empresas e organizações que coletam ou usam informações pessoais. Essas obrigações incluem: a obtenção do consentimento do titular dos dados antes da coleta ou uso de suas informações pessoais, uso de informações pessoais apenas para os fins especificados no momento da coleta, armazenamento de informações pessoais de forma segura, notificação aos titulares dos dados em caso de violação de dados, a remoção de informações pessoais quando não forem mais necessárias, dentre outros.

Contudo, há exceções dentro de algumas regras, como para casos em que são baseados na lei ou em regulamentos, casos para proteger a vida, corpo ou

fortuna de alguma indivíduo, casos de higiene pública, casos em que há a necessidade de cooperação em relação a uma organização do governo central ou um governo local e que há a possibilidade de que obter o consentimento do titular interferiria na execução dos referidos assuntos. (*PERSONAL INFORMATION PROTECTION COMMISSION*, 2017).

3.3 *California Consumer Privacy Act*

A *California Consumer Privacy Act* (CCPA), traduzida como Lei de Privacidade do Consumidor da Califórnia e também conhecida como Lei de Privacidade do Consumidor Digital, é uma lei estadual de privacidade de dados que se aplica a empresas que coletam informações pessoais de residentes da Califórnia, fornece aos consumidores mais controle sobre as informações pessoais que as empresas coletam sobre eles e os regulamentos da CCPA fornecem orientações sobre como implementar a lei.

A CCPA concede aos consumidores da Califórnia uma série de direitos em relação às suas informações pessoais, incluindo: Direito de saber, Direito de exclusão, Direito de não participar da venda, Direito de corrigir, Direito à não discriminação, Direito de limitar o uso e a divulgação de informações pessoais confidenciais. (*CALIFORNIA*, 2018).

4 METODOLOGIA

As pesquisas podem ser agrupadas de acordo com diversos critérios, como o campo de conhecimento, os objetivos, os dados coletados ou a natureza da investigação. De acordo com Gil (2010), essa classificação permite organizar as informações do estudo, facilitando seu entendimento. Além disso, uma pesquisa organizada é mais eficiente, pois reduz o tempo de execução, otimiza os recursos e aumenta as chances de sucesso. Por isso, a classificação da pesquisa é essencial para sua realização e para a compreensão de seus resultados.

Quanto à finalidade, o presente estudo classifica-se como aplicado. De acordo Gil (2010), as pesquisas aplicadas são voltadas para a aquisição de conhecimentos para a aplicação de uma conjuntura particular. Nesse caso, refere-se a verificação do papel do profissional de Tecnologia da Informação para garantia da Lei Geral de Proteção de Dados. Os objetivos da pesquisa têm caráter exploratório, que, ainda de acordo com Gil (2010, p. 27), "[...] têm o propósito de proporcionar maior familiaridade com o problema". Neste sentido, buscou-se refletir sobre as variáveis de aspectos relativos ao objeto.

Quanto à classificação dos dados coletados, a pesquisa classifica-se como secundária, pois utilizou-se de documentos já publicados acerca do tema, fazendo uma análise destes, juntamente com o que é previsto em lei.

O procedimento técnico utilizado foi a pesquisa bibliográfica. De acordo com Lakatos e Marconi (2003) este tipo de pesquisa é fundamentado na análise de material já publicado, como livros, artigos científicos, teses, dissertações e outros documentos.

Como o objetivo da pesquisa é analisar o papel do profissional de Tecnologia da Informação na aplicação da Lei, foram analisados artigos científicos, livros e outros documentos acadêmicos que discutem as relações entre esses profissionais e a legislação. Então a pesquisa se deu em duas etapas, sendo a primeira a identificação da literatura, em seguida os dados foram analisados.

Durante a identificação da literatura, foram identificados os principais artigos, livros e outros documentos acadêmicos que discutem as relações entre os

profissionais de TI e a LGPD, além da análise da própria lei e outros documentos oficiais que revogam, autorizam ou vetam no texto da LGPD.

Durante a análise, os documentos identificados na primeira etapa foram analisados de forma crítica, com o objetivo de identificar os principais temas e perspectivas abordados.

5 O PAPEL DO PROFISSIONAL DE TI NA IMPLEMENTAÇÃO DA LGPD

Estar adequado à LGPD implica em adotar uma abordagem abrangente e proativa para garantir a proteção e o tratamento responsável dos dados pessoais. Diante disso, o profissional de TI desempenha um papel fundamental na adequação das organizações à LGPD.

De antemão deve-se informar o que a legislação informa como dado pessoal, dado pessoal sensível e dado anonimizado:

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; (BRASIL, 2018, não paginado).

Tendo em vista esses conceitos, a adequação das organizações à LGPD exige a implementação de medidas técnicas e administrativas robustas para proteger os dados pessoais. Os profissionais de TI desempenham um papel fundamental nesse processo, sendo responsáveis por participar de grande parte das ações ao decorrer de todos os processos de uma solução, como auditoria e mapeamento de dados, criptografia e anonimização, políticas de acesso, treinamento e conscientização, desenvolvimento de sistemas, avaliação de impacto sobre a proteção de dados, notificação de incidentes, a criação de políticas e termos de uso e a segurança das informações.

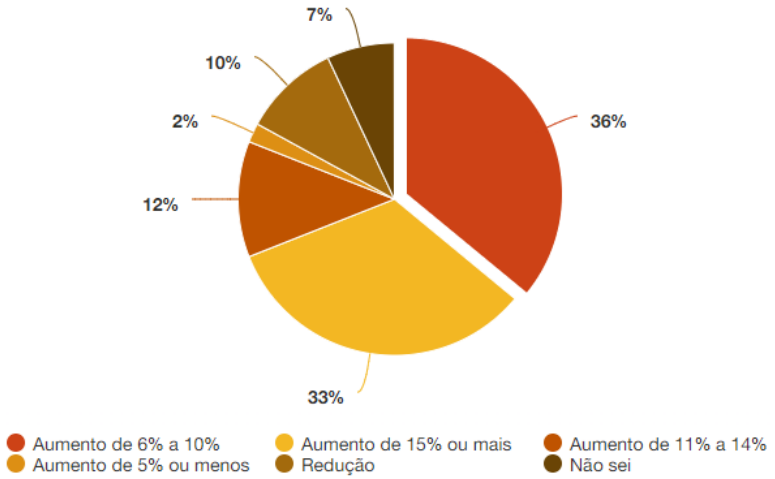
Segundo Medeiros (2022), o gerenciamento e armazenamento dos dados são o mais importante e desafiador ponto para a área de TI e seus profissionais. Nesse sentido, verifica-se a necessidade da capacidade técnica do profissional para lidar com esse novo desafio no ambiente de trabalho. Afinal, segundo a legislação,

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (BRASIL, 2018, não paginado).

Contudo, em pesquisa realizada pela PWC com 3.602 executivos de negócios, tecnologia e segurança de diversas regiões, Europa Ocidental, América do

Norte, Ásia-Pacífico, América Latina, Europa Oriental, Oriente Médio e África em 2021, informa que apenas 33% dos entrevistados responderam que em 2022 aumentariam os gastos em mais de 15% em segurança cibernética, conforme exibe a figura 3.

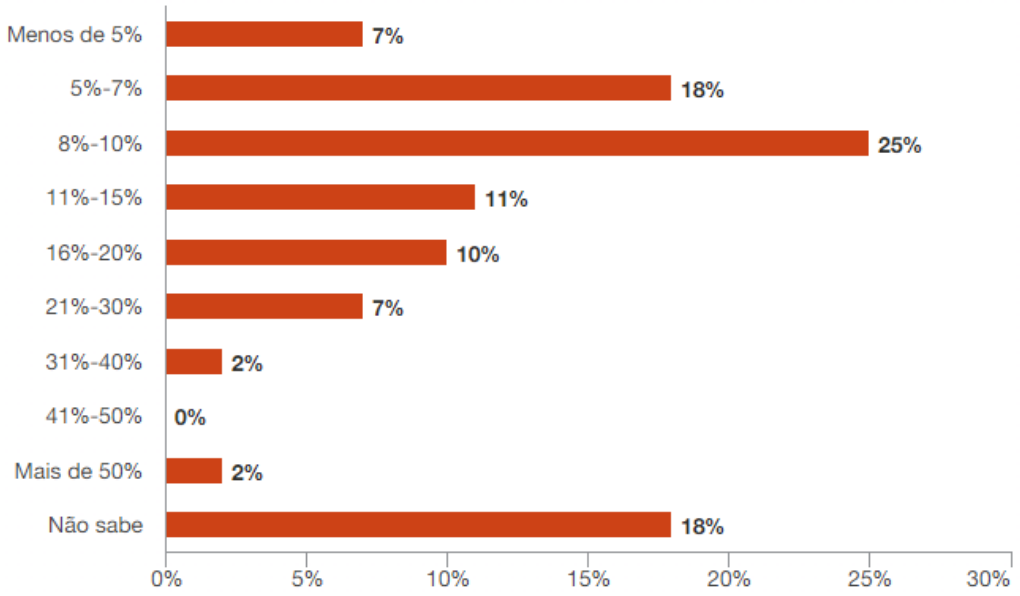
Figura 3 - Mudança no orçamento cibernético para o ano de 2022



Fonte: Global Digital Trust Insights Survey, 2022.

E a pesquisa revela ainda que apenas 11% dos entrevistados investiram mais do que 20% do orçamento de tecnologia da informação para a cibersegurança, conforme exibe a Figura 4.

Figura 4 - Orçamento de TI destinado para segurança cibernética em 2021



Fonte: Global Digital Trust Insights Survey, 2022.

Esses dados revelam que, apesar da maioria das empresas entrevistadas responder positivamente para o aumento dos gastos com cibersegurança, o investimento atualmente corresponde a uma porcentagem baixa do orçamento nesse setor, o que implica em um aumento pouco significativo de receita investida no ano seguinte.

Para garantir a segurança dos dados pessoais, é crucial a gerência de acessos e permissões. Isto implica o estabelecimento de sistemas eficazes de controle que limitem o acesso aos dados pessoais apenas ao pessoal autorizado. Além disso, são necessárias auditorias regulares para detectar e corrigir potenciais vulnerabilidades.

O que confirma Medeiros (2022), quando discorre que o setor de TI, no que se condiz à *Compliance* de TI dentro das instituições, tem a função de proteger redes, programas, sistemas de uma empresa contra ataques cibernéticos, vazamento de dados e ameaças do gênero.

Kanagusku e Lahr (2022) discutem que

> [...] a equipe de TI precisa estar atenta a soluções que atendam ao mesmo tempo a lei e as demandas da empresa, focando em minimizar riscos e incidentes, prevenção de vazamento de dados e ataques cibernéticos.

Ressaltando a importância da equipe de TI em encontrar soluções que harmonizem os requisitos legais com as demandas operacionais da empresa, contudo, a segurança digital é apenas um dos diversos fatores necessários para a implementação e conformidade com a LGPD.

O desenvolvimento seguro de software é outra área na qual os profissionais de TI desempenham um papel fundamental. Segundo Duarte (2021), esse é uma das implicações da lei em que os desenvolvedores devem entender sobre os impactos da LGPD dentro da área, classificando-o como um impacto técnico, em que deve-se integrar práticas de segurança desde as fases iniciais do ciclo de vida do desenvolvimento de software ajuda a prevenir vulnerabilidades e a garantir que as aplicações atendam aos requisitos de privacidade desde sua concepção.

A colaboração entre profissionais de TI e equipes jurídicas e de conformidade é essencial para garantir que as políticas e procedimentos de segurança estejam alinhados com as exigências legais da LGPD. Ainda segundo Duarte (2021), essa é

outra das implicações legais da lei dentro da área, em que é classificada como um impacto formal, descrito por atividades como

> [...] alterações na política de segurança da informação e em regulamentos internos sobre o assunto, mudanças em processos e procedimentos internos que envolvem segurança da informação, como revisões periódicas na política de segurança da informação, processos de análise e avaliação de riscos e classificação de informações [...] (DUARTE, 2021, 50).

A interpretação e aplicação corretas dos requisitos legais relacionados à proteção de dados exigem uma compreensão técnica profunda, e os profissionais de TI desempenham um papel de ponte crucial nesse diálogo interdisciplinar.

Ademais, a rápida resposta a incidentes é uma área crítica em que uma rápida resposta pelos profissionais é fundamental. Desenvolver e implementar planos eficazes de resposta a incidentes permite que as organizações ajam prontamente em caso de violação de dados, minimizando danos e mantendo a conformidade com a LGPD.

Logo, faz-se necessário o desenvolvimento de estratégias para fortalecer as medidas de segurança dentro das normas da LGPD. Como informa Duarte (2021), essas estratégias devem passar pelos três princípios da segurança da informação: integridade, disponibilidade e confidencialidade. Segundo Kanagusku e Lahr (2022), algumas técnicas que podem ser adotadas para a proteção de dados pessoais são a pseudonimização, que corresponde a remoção dos identificadores pessoais e sua substituição por um identificador artificial e a criptografia de dados pessoais, que é a alteração de um valor por um dado criptografado por um chave, a fim de não ser reconhecido.

Ainda de acordo com Kanagusku e Lahr (2022) outras medidas podem ser adotadas, como o controle de acesso com nível de privilégio preestabelecido, e a revisão regular dos acessos concedidos, garantindo que apenas usuários autorizados tenham acesso aos dados e ainda, a exigência de prevenir a exploração de vulnerabilidades técnicas.

Garantir a implementação de medidas técnicas para proteger os dados pessoais, como firewalls e sistemas de monitoramento, são essenciais para prevenir acessos não autorizados e proteger a confidencialidade dos dados. Após

implementar as medidas técnicas e organizacionais, é importante ainda monitorá-las e avaliá-las periodicamente para garantir que estejam funcionando eficazmente.

Segundo Freitas (2019), a política de privacidade é um dos instrumentos de implementação do *privacy by design*, e faz parte da documentação para a proteção de dados. As políticas de privacidade são documentos que fornecem informações sobre o tratamento de dados pessoais realizado por uma empresa ou organização. As políticas de privacidade devem ser elaboradas em conformidade com a LGPD e devem conter as informações mínimas estabelecidas pela lei.

O documento deve ser claro quanto ao tratamento dos dados pessoais, e o motivo para o qual esses dados estão sendo requisitados, o que é reafirmado por Freitas (2019) quando diz que

> [...] é necessário mapear todos os dados pessoais, a finalidade, as bases legais que legitimam o tratamento e a forma de atendimento aos direitos do titular como acesso, retificação, exclusão, revogação de consentimento, oposição, informação sobre possíveis compartilhamentos com terceiros e portabilidade. (FREITAS, 2019, não paginado).

E ainda é afirmado no artigo 9° da legislação que

> O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso. (BRASIL, 2018, não paginado).

Tornando assim indispensável o conhecimento sobre a LGPD, afinal, é necessário analisar e disponibilizar informações sobre os requisitos aplicáveis a cada um dos tratamentos que serão aplicados aos dados pessoais.

Deve-se ainda comentar que o consentimento expresso do usuário e a concordância com a política devem ser demonstrados antes do início do processamento dos dados. Segundo a LGPD, consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (BRASIL, 2018). Ainda conforme a lei, o tratamento de dados pessoais somente poderá ser realizado segundo alguns casos e, de forma geral, mediante o fornecimento de consentimento pelo titular (BRASIL, 2018).

Dessa forma, surge junto da LGPD uma nova profissão, o Encarregado da Proteção de Dados do inglês Data Protection Officer (DPO), pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, tecnicamente é o responsável por formar esse o elo entre o controlador, a quem competem as decisões referentes ao tratamento de dados pessoais, a autoridade nacional, Autoridade Nacional de Proteção de Dados (ANPD), e o titular dos dados. (MEDEIROS, 2022; BRASIL, 2018).

A legislação cita ainda as habilidades e atribuições dos encarregados. Conforme o artigo 41 da lei,

> O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
> § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
> § 2º As atividades do encarregado consistem em:
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
> § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. (BRASIL, 2018, não paginado).

De forma resumida, o DPO deve ter conhecimentos sobre jurisdição, segurança da informação, controles de dados pessoais e uma excelente capacidade de comunicação e diálogo. Além disso, é necessário que o DPO mantenha um registro sobre as operações que foram realizadas com os dados pessoais de terceiros. Conforme o artigo 37° da LGPD,

> O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. (BRASIL, 2018, não paginado).

Medeiros (2022) discute em sua pesquisa que diversas possibilidades concretas se apresentam para profissionais de todas as áreas, destacando-se especialmente aqueles do setor de Tecnologia da Informação. Isso se deve ao surgimento de um considerável número de oportunidades de emprego e avanço na

carreira, impulsionado pela necessidade das empresas e organizações públicas de ajustarem suas práticas às demandas da Lei Geral de Proteção de Dados.

Contudo, Ferreira e Okano (2021), desenvolveram uma pesquisa com mais de 200 profissionais de diversas áreas em que informa que apenas 66,2% das empresas estavam adequadas com a Lei Geral de Proteção de Dados, sendo a principal área de adequação a de Tecnologia da Informação. Os autores revelaram ainda que do seu grupo de pesquisa, 46,7% tem como principal desafio para a implantação da lei a cultura interna da empresa, e apenas 9% acreditam que as organizações têm maturidade para tratar das questões da LGPD, além disso 47% não obtiveram nenhum tipo de treinamento sobre a lei, suas bases e diretrizes.

No entanto, as sanções administrativas dispostas na lei são rigorosas quanto a não aplicação da legislação vigente, levando a multas de até cinquenta milhões de reais por infração ou multas diárias de até o mesmo valor. Outras penalidades citadas pela lei, são:

a) publicização da infração;
b) bloqueio ou eliminação dos dados pessoais a que se refere a infração;
c) suspensão parcial do funcionamento do banco de dados;
d) suspensão, proibição parcial ou proibição total do exercício da atividade de tratamento dos dados pessoais.

É importante mencionar que, de acordo com o previsto em lei, todos os valores arrecadados por aplicação de multas pelas ANPD são destinados ao Fundo de Defesa de Direitos Difusos (FDD). O FDD trata da reparação dos danos causados ao meio ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico, paisagístico, por infração à ordem econômica e a outros interesses difusos e coletivos. (BRASIL, 2018).

Logo, para que a lei seja efetivamente praticada é necessário capacitar os colaboradores das empresas sobre as políticas de privacidade e práticas seguras de manipulação de dados e desenvolvimento de software. Isso contribui para uma cultura organizacional que valoriza a privacidade e a conformidade com a LGPD.

No entanto, a jornada rumo à conformidade com a LGPD está longe de ser isenta de adversidades. A implementação da LGPD é um desafio para muitas

empresas, pois exige mudanças significativas em seu fluxo de trabalho e, por ser uma legislação recente, complexa e dinâmica, as empresas precisam estar preparadas para se adaptar às mudanças. É importante ressaltar que a implementação da LGPD é um processo complexo e contínuo. As empresas precisam incluir em seu planejamento, o investimento de tempo e recursos para atender às exigências da lei. Com organização, as empresas podem superar os desafios da implementação da LGPD e garantir a proteção dos dados pessoais de seus clientes e colaboradores.

6 DESAFIOS NA IMPLEMENTAÇÃO DA LGPD

A implementação da Lei Geral de Proteção de Dados é um desafio para as organizações, pois exige mudanças em processos e sistemas que já são padronizados. Todavia, é importante ressaltar que as mudanças trazidas pela lei podem revelar-se como um diferencial para uma empresa. A preocupação com os dados pessoais pode ser vista pelo cliente como um ponto de confiança, o que traz retorno para e até mesmo novos clientes.

Entretanto, sabe-se que os desafios trazidos para a efetivação da lei são diversos. Em razão da LGPD ter entrado em vigor apenas em 2020, há ainda pouca literatura sobre a implementação da lei. O que se observa é que os mais interessados são escritórios de advocacia e empresas que terceirizam essa implementação.

De acordo com Bento Muniz Advocacia (2022), em pesquisa realizada com cerca de 500 empresas até maio de 2022, apenas 16% das empresas aderiram à LGPD, durante a pesquisa apresentada é revelado ainda que

> [...] foram ouvidas mais de 500 empresas e 74% delas afirmam que o ideal é contratar empresas terceirizadas para regularizar a empresa perante as normas. Foi observado também que 84% das empresas acham que não estão preparadas para se adequarem à lei, por conta do trâmite burocrático e os gastos que a adequação acaba resultando. (BENTO MUNIZ ADVOCACIA, 2022, não paginado).

Em consonância a isso, Kanagusku e Lahr (2022) entrevistaram pessoas do meio acadêmico e empresarial da área de TI na região Metropolitana de Campinas em sua pesquisa. Os resultados revelam que as empresas acreditam na necessidade de investimento em soluções de cibersegurança, demonstrando a preocupação com a proteção dos dados a ataques, e apontam ainda que a maioria dos profissionais da área tem como principal desafio para se adequar a LGPD a compreensão dos princípios e bases legais.

Da mesma forma, Fernandes (2022) em sua dissertação, entrevistou profissionais de TI e revelou que 10% dos entrevistados desconhecem os princípios da Lei Geral de Proteção de Dados, expõe ainda que 45% desse grupo não possui conhecimento de como as empresas as quais trabalham armazenam os dados pessoais dos usuários ou tratam o compartilhamento de informações. Além disso, o

autor informa que cerca de 25% dos entrevistados estão cientes de que os seus próprios dados pessoais podem ser compartilhados a qualquer momento pelas organizações.

Dessa forma, é possível constatar que a principal dificuldade para a execução correta da lei é o conhecimento da população, empresas e colaboradores sobre o assunto, bem como os altos custos para a reelaboração de uma solução para que esteja de acordo com a legislação. Nesse sentido, entende-se que nem as organizações estão priorizando a efetivação da lei e os profissionais de TI, principais capacitados para tal, tampouco estão cientes da necessidade da lei ou mesmo não dão a devida importância para a urgência da segurança de dados pessoais.

Observa-se que no nicho de implantação de LGPD em organizações existem diversas empresas que oferecem o serviço. Empresas essas que são majoritariamente de cunho jurídico, contudo, há também empresas da área de TI, mesmo que em minoria. A empresa OneTrust (2023), por exemplo, descreve as soluções oferecidas ao contratar seus serviços, que são:

> [...] Verificar sites em busca de tecnologias de rastreamento de terceiros, incluindo cookies, tags, pixels, web beacons e mais.
> Categorizar automaticamente os rastreadores descobertos com Cookiepedia ™, banco de dados de mais de 40 milhões de cookies e rastreadores já pré-categorizados.
> Bloquear rastreadores automaticamente até que o consentimento adequado seja obtido usando OneTrust Auto-Block ™.
> Habilitar o suporte para estruturas como IAB TCF 2.0 europeu e opt-outs específicos do fornecedor para enviar sinais de consentimento apropriados.
> Manter uma trilha de auditoria centralizada para demonstrar conformidade e painéis de controle para monitorar as taxas de opt-in e opt-out.
> Usar regras de geolocalização para exibir automaticamente diferentes banners e modelos de consentimento com base na região, país ou estado, com suporte para mais de 250 idiomas.
> Operacionalizar a conformidade com centenas de leis e regulamentos de privacidade.
> Cumprir com diretrizes principiológicas da LGPD, dentre elas, o princípio da transparência associados ao livre, claro e transparente consentimento dado e retirado pelo titular de dados a qualquer momento. (ONETRUST, 2023, não paginado).

Ou seja, dentre as diversas soluções apontadas pela empresa, a LGPD é citada como um dos serviços diferenciais a serem executados para garantir a privacidade dos clientes. Todavia, a terceirização desse serviço não garante por si só o sucesso na efetivação da lei, pois envolve diversas questões a serem observadas.

Cunha *et al* (2021) discorre que os principais desafios para a implementação da lei são: a adequação da empresa; o custo de sistemas ou *softwares* licenciados; o treinamento para os funcionários; a falta de profissionais qualificados; e assessoria jurídica qualificada. Ou seja, essa implantação da lei, ainda que seja terceirizada, gera dificuldades a serem enfrentadas.

Outro ponto importante a ser mencionado é a falta de conhecimento e entendimento da lei. Muitas empresas ainda não têm um entendimento claro a respeito das regras da LGPD, levando a erros e infrações, que podem resultar em sanções administrativas e judiciais. Acerca do conhecimento da legislação,

> Uma pesquisa realizada pela Federação Brasileira de Bancos (Febraban) aponta que apenas 37% dos brasileiros afirmam conhecer “muito bem” ou “mais ou menos” a Lei Geral de Proteção de Dados (LGPD), enquanto que 60% dizem só ter “ouvido falar” ou sequer conhecem a legislação (MATOS; MARQUES JUNIOR, 2021)

Segundo Brasil (2018), a ANPD deve editar normas, orientações e criar procedimentos simplificados e diferenciados, inclusive quanto aos prazos para empresas de pequeno porte e *startups*, facilitando assim a adequação dessas organizações à legislação vigente. Contudo, a solução pode trazer a sensação de que essas empresas são menos seguras para os clientes, podendo, assim, diminuir sua lucratividade e gerar prejuízos financeiros em relação a empresas maiores.

Dessa forma, há a problemática da falta de recursos para a implementação da LGPD. Para a efetivação da lei, é necessário que cada organização faça investimentos em tecnologia, treinamento de funcionários e até mesmo a contratação de especialistas para acelerar o processo de adequação à lei. Outro ponto dificultoso para as empresas de pequeno porte, pois podem encontrar dificuldades em investir os recursos necessários para atender as exigências da lei.

No Brasil, a cultura acerca da proteção de dados pessoais ainda não é difundida. Num cenário onde 15,75% dos domicílios não possuem sequer acesso a internet (CETIC, 2023), é compreensível que muitos não deem tanta importância aos dados pessoais. Esse fato reflete na resistência cultural de algumas empresas de se adequarem a LGPD, pois os próprios profissionais das empresas podem não saber sobre a lei e como aplicá-la.

Para superar esses desafios, as empresas precisam desenvolver um programa de conformidade com a LGPD adaptado às suas necessidades específicas. O plano deve incluir uma etapa de extensa avaliação do cenário atual, além de um plano de adequação e implementação da lei, que seja realizado de forma contínua.

É necessário que as empresas compreendam que investir tempo e recursos para atender às exigências da lei é imprescindível para alcançar o sucesso de uma organização e a confiança dos clientes. Com um planejamento adequado, as empresas podem superar os desafios da implementação da LGPD e garantir a proteção dos dados pessoais de seus clientes e colaboradores.

7 CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados apresenta-se em estado promissor, as empresas estão se adequando à legislação ao passo que essa discussão alcança a população. Todavia, verifica-se a necessidade de uma cultura organizacional que valorize a privacidade e a conformidade. No entanto, como em qualquer empreendimento desafiador, a jornada rumo à conformidade não está isenta de obstáculos significativos, todavia, se as organizações mantiveram um planejamento de adequação e mudanças contínuas, essa jornada torna-se mais simples.

A capacitação dos colaboradores revelou-se um pilar fundamental na busca pela efetiva implementação das diretrizes da lei, capacitando a equipe para lidar com as questões relacionadas à manipulação de dados e desenvolvimento de software.

O futuro da LGPD no Brasil é promissor. A lei está ainda em fase de implementação, mas já está tendo um impacto positivo na proteção dos dados pessoais no país. No futuro, é provável que a LGPD seja ainda mais aprimorada para atender às necessidades da sociedade. Também é provável que a lei seja aplicada de forma mais rigorosa, com o objetivo de garantir a conformidade das empresas. As empresas que se prepararem adequadamente para o futuro da LGPD estarão mais bem posicionadas para enfrentar os desafios e aproveitar as oportunidades que a lei oferece.

Para superar esses desafios, as empresas precisam desenvolver um plano de adequação à LGPD que seja adequado às suas necessidades específicas, que vão desde o planejamento da implementação, avaliação da comunidade até chegar na implementação da LGPD de fato dentro da organização.

A implementação da LGPD é um processo complexo e contínuo. As empresas precisam estar preparadas para investir tempo e recursos para atender às exigências da lei. Com uma estratégia bem pensada, as empresas podem vencer os obstáculos e assegurar a proteção dos dados pessoais dos profissionais envolvidos no processo e também dos clientes da organização.

O papel do profissional de TI é de suma importância para a aplicação efetiva da lei, uma vez que ele pode ser o responsável por boa parte do processo ou até ele todo, em que se inicia desde o desenvolvimento do software e a coleta dos dados até o seu tratamento para os devidos fins.

Outro papel importante é o do Encarregado de Proteção de Dados, uma vez que sua existência dentro de uma empresa deve ser obrigatória em alguns casos. E

para evitar conflito de interesses, este não deve ter outra ocupação dentro da empresa, a fim de desempenhar o seu papel de mediador entre o controlador, o titular dos dados e a ANPD a contento.

Sabe-se que o caminho é árduo e o processo de efetivação da privacidade dos dados é lento, todavia, é necessário compreender que as empresas que primeiro alcancem a implementação da LGPD nas suas práticas, terão vantagens em relação às organizações que não dão a devida importância para a lei. A cada dia, as pessoas passam a se preocupar mais com o que fazem com seus dados na *web* e a proteção de dados particulares vem se tornando cada vez mais prioridade na hora de escolher um serviço ou produto a ser contratado.

REFERÊNCIAS

BENTO MUNIZ ADVOCACIA. **Somente 16% das empresas aderiram a LGPD, revela pesquisa**. [*Online*], 2022. Disponível em: https://bentomuniz.com.br/somente-16-das-empresas-aderiram-a-lgpd-revela-pesquisa/#:~:text=No%20ano%20de%202020%2C%20foi,maior%20seguran%C3%A7a%20jur%C3%ADdica%20aos%20envolvidos. Acesso em: 6 dez. 2023.

BEZERRA, M. R. B. Autoridade Nacional de Proteção de Dados Pessoais: a importância do modelo institucional independente para a efetividade da Lei. **Caderno Virtual**, [S. l.], v. 2, n. 44, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3828. Acesso em: 3 dez. 2023.

BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento, 2. ed. Rio de Janeiro: Forense, 2020. E-book.

BRASIL. **Lei nº 14.460, de 25 de outubro de 2022**. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019. Brasília: Congresso Nacional, 25 out. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm#art7. Acesso em: 21 nov. 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 República Federativa do Brasil, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 9 dez. 2023.

CALIFORNIA. **Title nº 1.81.5., de 16 de dezembro de 2018**. California Consumer Privacy Act of 2018. [S. l.], 16 dez. 2020. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: 4 dez. 2023.

CETIC. CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros**. [Online]: CETIC, 2023. Disponível em: https://data.cetic.br/explore/?pesquisa_id=1&unidade=Domic%C3%ADlios. Acesso em: 01 dez. 2023.

CUNHA, B. E. de M. *et al*. As dificuldade da implementação da LGPD no Brasil. **Revista Projetos Extensionistas**, Pará de Minas, v. 1, ed. 2, 10 dez. 2021. Disponível em: https://periodicos.fapam.edu.br/index.php/RPE/article/view/391/249. Acesso em: 2 dez. 2023.

DUARTE, N. M. S. **A compreensão dos profissionais de TI quanto à lei geral de proteção de dados pessoais e suas implicações nas organizações - estudo de caso SENAC**. Orientador: Albuquerque Junior, Antonio Eduardo de. 2021. 178 p. Dissertação (Pós-Graduação em Administração Profissional) - Universidade Federal da Bahia, Salvador, 2021. Disponível em: https://repositorio.ufba.br/handle/ri/35435. Acesso em: 4 dez. 2023.

FACCIONI FILHO, M. **Internet das coisas**. Palhoça: UnisulVirtual, 2016. E-book (56 p.). Disponível em: https://www.researchgate.net/profile/Mauro-Fazion-Filho/publication/319881659_Internet_das_Coisas_Internet_of_Things/links/59c038d5458515e9cfd54ff9/Internet-das-Coisas-Internet-of-Things.pdf. Acesso em: 20 nov. 2023.

FERNANDES, M. A. de S. **Repositório seguro e o impacto gerado pela Lei Geral de Proteção de Dados Pessoais (LGPD)**. 2022. Dissertação (Mestre em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2022. Disponível em: https://repositorio.unb.br/handle/10482/45357. Acesso em: 9 nov. 2023.

FERREIRA, L.; OKANO, M. T. **Um panorama da implementação da LGPD no Brasil**: uma pesquisa exploratória com 216 profissionais. In: SIMPÓSIO DOS PROGRAMAS DE MESTRADO PROFISSIONAL UNIDADE DE PÓS-GRADUAÇÃO, EXTENSÃO E PESQUISA, 16., 2021, São Paulo. Anais [...]. São Paulo: [s. n.], 2021. Disponível em: https://www.researchgate.net/profile/Marcelo-Okano-2/publication/356555146_Um_panorama_da_implementacao_da_LGPD_no_Brasil_uma_pesquisa_exploratoria_com_216_profissionais/links/61a05cb83068c54fa51db117/Um-panorama-da-implementacao-da-LGPD-no-Brasil-uma-pesquisa-exploratoria-com-216-profissionais.pdf. Acesso em: 10 nov. 2023.

FREITAS, C. **Como elaborar uma política de privacidade aderente à LGPD?**. In: SERPRO. Serpro e LGPD: segurança e inovação. [online], 11 out. 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2019/elabora-politica-privacidade-aderente-lgpd-dados-pessoais. Acesso em: 7 dez. 2023.

GIL, A. C. Como classificar as pesquisas? *In:* GIL, A. C.**Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010. 4. cap. p. 25-44.

KANAGUSKU, A. R. A.; LAHR, M. V. **Impactos da LGPD na Tecnologia da Informação: Desafios para os Profissionais da Área**. FatecSeg - Congresso de Segurança da Informação, [S. l.], v. 1, n. 2, 2022. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/69. Acesso em: 11 jun. 2023.

MARCONI, M. de A; LAKATOS, E. M. **Fundamentos de Metodologia Científica**. 5. ed. São Paulo: Atlas, 2003. 311 p.

MATOS, V. S.; MARQUES JUNIOR, W. P. Os brasileiros não conhecem a Lei Geral de Proteção de Dados. **Encontros Universitários da UFC**, [*s. l.*], v. 6, n. 11, ed.

2021, 1 jan. 2021. Disponível em: http://periodicos.ufc.br/eu/article/view/73668. Acesso em: 1 dez. 2023.

MEDEIROS, R. M. **LGPD | Desafios e impactos na TI**. 2022. Trabalho de conclusão de curso (Bacharelado em Sistemas de Computação) - Universidade Federal Fluminense, Niterói, 2022. Disponível em: https://app.uff.br/riuff/bitstream/handle/1/31091/TCC_RODRIGO_MOREIRA_MEDEIROS.pdf?sequence=1&isAllowed=y. Acesso em: 5 dez. 2023.

OLIVEIRA, L. P. de. **Proteção de dados pessoais na era da tecnologia**: Análise do impacto da LGPD na coleta, uso e armazenamento de informações pessoais na internet. 2023. Trabalho de Conclusão de Curso ([Bacharel em Direito]) - [Ânima, S. l.], 2023. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/35115. Acesso em: 10 jul. 2023.

ONETRUSH. **Solicite uma Demonstração OneTrust Cookie Consent**: Gestão de Consentimento de Cookies. [S. l.], 2023. Disponível em: https://www.onetrust.com/br/formularios/demo-consentimento-de-cookies/. Acesso em: 6 dez. 2023.

PERSONAL INFORMATION PROTECTION COMMISSION. Amended Act on the Protection of Personal Information. **Act on the Protection of Personal Information** (Tentative Translation). [S. l.], dez. 2016. Disponível em: https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf. Acesso em: 6 dez. 2023.

PWC. **Global Digital Trust Insights Survey 2022**: Simplificar para reduzir riscos cibernéticos. [S. l.], 2021. Disponível em: https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2021/global-digital-trust-insights-survey-2022.html. Acesso em: 4 dez. 2023.

ROSA, R. de O.; CASAGRANDA, Y. G.; SPINELLI, F. E. A importância do marketing digital utilizando a influência do comportamento do consumidor. **Revista de Tecnologia Aplicada**, [s. l.], v. 6, n. 2, 2017. Disponível em: http://www.cc.faccamp.br/ojs-2.4.8-2/index.php/RTA/article/view/1044. Acesso em: 8 jul. 2023.

SANTI, L. **Lei nº 13.709/2018**: análise à Lei Geral de Proteção de Dados (LGPD). 2020. Monografia (Bacharel em Direito) - Universidade do Sul de Santa Catarina, Tubarão, 2020.

SANTOS, M. F. C. de S.. Porque não há mais escapatória: a vigência dos princípios norteadores da proteção de dados pessoais no Brasil e sua aplicação nas relações de consumo, bem como no tratamento desses dados. **Revista Jurídica da Seção Judiciária de Pernambuco**, n. 13, v. 1, p. 217-255, 2021. Disponível em: https://revista.jfpe.jus.br/index.php/RJSJPE/article/view/231. Acesso em: 02 dez. 2023.

TEFFÉ, C. S. DE; VIOLA, M. **Tratamento de dados pessoais na LGPD**: estudo sobre as bases legais. civilistica.com, v. 9, n. 1, p. 1-38, 9 maio 2020.

THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. **Regulation nº 679, de 27 de abril de 2016**. On the protection of natural persons with regard to the processing of personal data anOn the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [*S. l.*], 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 4 dez. 2023.

ZAEEM, R. N.; BARBER, K. S. **The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise**. ACM Transactions on Management Information Systems, n.1, v. 12, 2021. Disponível em: https://www.researchgate.net/publication/343681934_The_Effect_of_the_GDPR_on_Privacy_Policies_Recent_Progress_and_Future_Promise. Acesso em: 30 nov. 2023.