Revista Ibero- Americana de Humanidades, Ciências e Educação- REASE

doi.org/10.51891/rease.v9i10.12254

A LEI GERAL DE PROTEÇÃO DE DADOS E SUA APLICAÇÃO NO COMBATE AOS CRIMES CIBERNÉTICOS: DESAFIOS E PERSPECTIVAS

THE GENERAL DATA PROTECTION LAW AND ITS APPLICATION IN COMBATING CYBER CRIMES: CHALLENGES AND PERSPECTIVES

Ronaldo Couto da Silva[1]
Thyara Gonçalves Novais[2]

RESUMO: Este trabalho tem como objetivo analisar a aplicabilidade da Lei Geral de Proteção de Dados (LGPD) na prevenção de crimes cibernéticos. Diante dos avanços tecnológicos da informática e dos meios de comunicação digitais, tornou se necessário se tutelar de forma mais particular os direitos inerentes a proteção de dados. Nesse novo cenário, os dados pessoais passam a ter grande valor econômico na sociedade contemporânea, assim como adquirir funções político-sociais, será demonstrado como a lei pode auxiliar na prevenção dessa criminalidade, e os seus possíveis impactos na proteção e privacidade de dados. Os crimes cibernéticos envolvem o uso de tecnologias e/ou dados digitais para obter vantagem indevida. A LGPD tem como objetivo regular o tratamento de dados pessoais, protegendo quem os detém para uso pessoal e/ou comercial. Por meio de uma análise histórica, foi possível observar que, no Brasil, a legislação ainda é deficiente em termos de prevenção a esses crimes. Diante das abordagens, pretende-se compreender como a lei tem se tornado uma ferramenta cada vez mais necessária na prevenção de crimes ocorridos no ambiente virtual com a aplicabilidade da LGPD. Por fim, foram realizadas discussões pertinentes ao avanço dessa valiosa legislação, devido ao adiantamento que ela trouxe, na perspectiva de segurança e prevenção de crimes cibernéticos. É possível concluir que a LGPD é fundamental para garantir a privacidade e segurança de dados pessoais, a prevenção de atos ilícitos e o combate a crimes cibernéticos.

Palavras-chave: Lei Geral de Proteção de Dados. Crimes Cibernéticos. Prevenção. Legislação. Dados Pessoais. Privacidade.

ABSTRACT: This work aims to analyze the applicability of the General Data Protection Law (LGPD) in preventing cybercrimes. In view of technological advances in information technology and digital media, it has become necessary to protect the rights inherent to data protection in a more particular way. In this new scenario, personal data begins to have great economic value in contemporary society, as well as acquiring political-social functions, it will be demonstrated how the law can help prevent this crime, and its possible impacts on data protection and privacy. Cybercrimes involve the use of digital technologies and/or data to obtain an undue advantage. The LGPD aims to regulate the processing of personal data, protecting those who hold it for personal and/or commercial use. Through a historical analysis, it was possible to observe that, in Brazil, legislation is still deficient in terms of preventing these crimes. Given the approaches, the aim is to understand how the law has become an increasingly necessary tool in preventing crimes occurring in the virtual environment with the applicability of the LGPD. Finally, discussions were held relevant to the advancement of this valuable legislation, due to the advancement it brought, from the perspective of security and prevention of cybercrimes. It is possible to conclude that the LGPD is essential to guarantee the privacy and security of personal data, the prevention of illicit acts and the fight against cybercrimes.

Keyword: General Data Protection Law. Cybercrime. Prevention. Legislation. Personal Data. Privacy.

[1]Discente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia.
[2]Docente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia.

1. INTRODUÇÃO

O aumento do cibercrime ao longo dos anos levou à necessidade de desenvolver soluções seguras para proteger os usuários contra possíveis ataques cibernéticos. Uma das formas mais eficazes de garantir a segurança dos usuários e evitar violações de dados e por meio da implementação de leis específicas que estabeleçam padrões de segurança e ofereçam orientações sobre o tratamento adequado das informações.

Neste contexto, é crucial examinar os desafios e perspectivas que envolvem a aplicação da LGPD no combate aos crimes cibernéticos. Isso inclui a necessidade de equilibrar a proteção da privacidade dos indivíduos com a investigação e a resistência dos crimes cibernéticos, a importância de mecanismos de supervisão e fiscalização eficientes para garantir o cumprimento da lei, e o papel da educação e conscientização na construção de uma sociedade digital mais seguro.

Por conseguinte, a LGPD desempenha um papel fundamental na busca por um ambiente digital mais seguro, bem como os desafios que ainda precisam ser superados e as perspectivas de aprimoramento nesse contexto

Diante da crescente ameaça de crimes cibernéticos, a Lei Geral de Proteção de Dados (LGPD) introduziu importantes regras e diretrizes para a coleta, armazenamento e uso adequado dos dados pessoais da população brasileira. Os principais objetivos da LGPD são aumentar a transparência, segurança e privacidade para o tratamento de dados pessoais, além de oferecer diretrizes para identificar os responsáveis pelos crimes cibernéticos. No entanto, o cumprimento adequado da LGPD pode encontrar desafios na sua aplicação, principalmente na identificação dos responsáveis e nos possíveis conflitos entre a LGPD e outras leis relacionadas a crimes cibernéticos.

Para garantia de privacidade e segurança, também é importante assegurar que os conceitos básicos da LGPD sejam usados com eficiência na aplicação das leis. Além disso, a atualização constante da LGPD e a adoção de novas tecnologias são fundamentais para manter a proteção de dados pessoais eficaz diante esse contexto. Para isso, é necessário adotar medidas que contemplem uma análise sistemática e voltada para a atualização contínua da lei para lidar com novas tecnologias, enquanto esclarece as dificuldades existentes na sua aplicação.

A Lei Geral de Proteção de Dados (LGPD) introduziu importantes diretrizes e previsões para a coleta, armazenamento e uso dos dados pessoais da população brasileira. Os conceitos básicos da LGPD podem ser usados para assegurar que os dados pessoais sejam

tratados com segurança, apego às leis e a ética. Os principais objetivos da LGPD, por sua vez, são fornecer maior transparência, segurança e privacidade para o tratamento de dados pessoais.

Os crimes cibernéticos também se tornaram uma ameaça crescente no que diz respeito à segurança de dados pessoais. Existem vários tipos de crimes cibernéticos, como vazamentos de dados, dinheiro clonado e roubo de identidade. Os impactos dos crimes cibernéticos na sociedade são sérios e podem causar grandes prejuízos.

Os desafios para aplicação adequada da LGPD no combate aos crimes cibernéticos são ainda maiores. Embora a LGPD contenha regras e diretrizes importantes para a proteção de dados pessoais, a identificação dos responsáveis pelos crimes cibernéticos é um grande desafio. Além disso, possíveis conflitos entre a LGPD e outras leis relacionadas a crimes cibernéticos tornam ainda mais complexa a tarefa de lutar contra esses crimes. Por fim, a atualização constante da LGPD e a adoção de novas tecnologias são fundamentais para que a proteção de dados pessoais se mantenha eficaz. No entanto, há desafios a serem superados na aplicação da LGPD no combate aos crimes cibernéticos

O presente trabalho tem como objetivo discutir sobre a Lei Geral de Proteção de Dados (LGPD), Conceitos básicos da LGPD, os Principais objetivos da LGPD, os Crimes cibernéticos.

Tipos de crimes cibernéticos, os Impactos dos crimes cibernéticos na sociedade, Desafios na aplicação da LGPD no combate a esses crimes, Dificuldades na identificação dos responsáveis pelos atos criminosos e Conflitos entre a LGPD e outras leis relacionadas a crimes cibernéticos. Também foi abortada a Importância da atualização constante da LGPD e Novas tecnologias e desafios para a proteção de dados pessoais.

As advertências para a evidência da LGPD devem ser aplicadas de forma eficaz para garantia de Privacidade e Segurança: Embora a LGPD visa proteger a privacidade dos indivíduos, também é importante garantir que a segurança dos dados não seja usada como pretexto para infringir direitos civis e individuais.

Analisar os conflitos entre a LGPD e outras leis relacionadas a crimes cibernéticos, assim como, a importância da atualização constante da LGPD e novas tecnologias e desafios para a proteção de dados pessoais com o crescimento exponencial de leis e regulamentações para garantir a privacidade e a segurança dos dados pessoais, discutir a LGPD, seus principais objetivos e como ela interfere no combate aos crimes cibernéticos se tornou ainda mais pertinente.

As advertências para a aplicação eficaz da LGPD e a garantia de Privacidade e Segurança são ainda mais relevantes diante do crescimento dos crimes cibernéticos. Para isso, é necessário adotar medidas que contemplem uma análise sistemática e voltada para a atualização contínua da lei para lidar com novas tecnologias, enquanto esclarece as dificuldades existentes na sua aplicação. O trabalho será realizado com base nas informações levantadas no âmbito da Lei Geral de Proteção de Dados, seus principais objetivos, assim como, a ameaças e os desafios na aplicação de seus ordenamentos para inibir os crimes cibernéticos.

Os crimes cibernéticos estão crescendo exponencialmente nos dias de hoje e, conforme a legislação brasileira, surgiram dúvidas quanto à aplicação da LGPD no combate a esses crimes.

O trabalho foi desenvolvido a partir de pesquisas direcionadas nos sites legislativos, artigos científicos e documentos que tratam da LGPD, crimes cibernéticos, as dificuldades na aplicação da LGPD no combate a esses crimes de forma colaborativa, dividido em modalidades de estudo: pesquisas bibliográficas, pesquisa documental, delinear o problema, levantar estatísticas e dados exatos sobre crimes cibernéticos, levantar dados sobre a aplica.

2.A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

À medida que o mundo se torna cada vez mais digital, a proteção dos dados pessoais tornou-se uma preocupação crítica tanto para indivíduos como para organizações. Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) no Brasil visa regulamentar o uso, o tratamento e a proteção de dados pessoais. Esse trabalho vem explorar alguns aspectos gerais da violação da LGPD.

A Lei Geral de Proteção de Dados representa um marco importante para a privacidade e a proteção de dados no Brasil, e tem como objetivo aumentar a transparência e a responsabilidade no tratamento de informações pessoais, promovendo a confiança dos cidadãos na relação com as organizações que lidam com seus dados

Além disso, a violação da LGPD pode trazer graves consequências jurídicas para as organizações. O não cumprimento da lei pode resultar em multas e penalidades substanciais. Em alguns casos, os infratores podem enfrentar acusações criminais, causando ainda mais danos à reputação e perdas financeiras. Portanto, é fundamental que as empresas entendam e cumpram os requisitos estabelecidos pela LGPD para mitigar o risco de violações e inclusive a Constituição Federal contempla em seu artigo 5º um extenso rol de direitos e

garantias fundamentais, dentre os quais a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurando ao lesado o direito a indenização pelo dano material ou moral decorrente de sua violação conforme, o Art 5 Constituição Federal, Inciso X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. (CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988)

Neste contexto a Constituição Federal reconhece e garante a todas as pessoas o direito à inviolabilidade da intimidade, da vida privada. Quando estas são violadas, a pessoa lesada tem direito a ser indenizada por dano material ou moral. Esta é uma preocupação ainda mais importante hoje, na era da informação, onde os dados e a reputação das pessoas estão cada vez mais vulneráveis.

Destaca a importância de promover a adesão à Lei Geral de Proteção de Dados (LGPD) no Brasil como um elemento fundamental para criar um ambiente digital que respeite a privacidade dos indivíduos. A LGPD é uma legislação que se baseia na proteção dos direitos dos cidadãos em relação ao tratamento de seus dados pessoais. Ela desempenha um papel crucial na mitigação das consequências legais e políticas decorrentes da observação da privacidade sofrida por esses cidadãos.

Além disso, a violação da LGPD pode ter implicações negativas para os direitos de privacidade dos indivíduos. A lei confere às pessoas singulares o direito de saber como estão a ser recolhidos e tratados os seus dados, bem como o direito de solicitar a sua eliminação ou correção. Porém, sem a devida adesão à LGPD, os indivíduos poderão ter seus dados coletados sem consentimento ou utilizados para fins além do legalmente permitido. Esta violação dos direitos de privacidade pode levar a uma quebra de confiança entre indivíduos e organizações, resultando numa reputação prejudicada para estas últimas.

Ademais, a violação da LGPD apresenta riscos e desafios significativos tanto para indivíduos quanto para organizações. O uso indevido de dados pessoais, as consequências legais e a violação dos direitos de privacidade são alguns dos aspectos gerais associados à violação desta lei. Para garantir a conformidade e proteger os dados pessoais, as organizações devem adotar medidas robustas de proteção de dados e priorizar a privacidade dos indivíduos. Em última análise, a implementação e aplicação adequadas da LGPD são essenciais para proteger as informações pessoais na era digital, A Lei LGPD trouxe uma nova era de responsabilidade no tratamento de dados pessoais, onde a violação dessa lei pode resultar em multas substanciais e danos irreparáveis à confiança da empresa.

Analisar as possíveis consequências legais do não cumprimento da LGPD (Lei Geral de Proteção de Dados) na prevenção de crimes cibernéticos é um tópico relevante, pois a LGPD estabelece regras rigorosas para a proteção de dados pessoais e tem implicações significativas para a segurança cibernética. Aqui estão quatro tópicos a serem considerados.

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que visa proteger a privacidade e os dados pessoais dos cidadãos. A violação da LGPD ocorre quando uma organização ou indivíduo não cumpre as disposições previstas na lei. Abaixo alguns aspectos gerais da violação da LGPD.

A LGPD prevê multas substanciais para empresas que não estejam em conformidade com suas disposições, que podem chegar a até 2% do faturamento da empresa, limitado a R$ 50 milhões por infração. Isso pode representar um impacto financeiro significativo para organizações que negligenciam a proteção de dados pessoais, especialmente em casos de crimes cibernéticos resultantes de uma violação de dados.

A LGPD tem como objetivo proteger a privacidade e a segurança dos dados pessoais, dando aos indivíduos maior controle sobre suas informações e incentivando as empresas a adotarem boas práticas de proteção de dados. Ela se aplica a todas as organizações que tratam dados pessoais no Brasil, sejam públicas ou privadas. A Autoridade Nacional de Proteção de Dados (ANPD) é a entidade responsável pela fiscalização e aplicação da LGPD.

Em conclusão, a LGPD criou diretrizes claras para o uso e a proteção correta de dados pessoais, com aplicação de sanções sérias para quem violar suas regras. É essencial que as organizações entendam e cumpram os requisitos estabelecidos pela lei a fim de assegurar que seus dados sejam tratados de forma segura e ética.

2.1. Conceitos Básicos da LGPD

A Lei Geral de Proteção de Dados (LGPD) criou normas para que as organizações possam garantir a proteção de dados de seus clientes e usuários. É importante entender os conceitos básicos dessa lei para começar a cumprir os requisitos.

O primeiro é sobre tratamento de dados. É a forma como os dados são coletados, armazenados, usados, compartilhados ou excluídos. A segunda é a responsabilidade dos agentes de dados. É o responsável pela coleta, armazenamento, manuseio, uso e divulgação dos dados.

Outro conceito é o consentimento. Antes de coletar qualquer dado, é preciso solicitar a autorização do usuário, com transparência e clareza.

Além disso, outros conceitos da LGPD são os princípios: finalidade, adequação, necessidade, transparência, segurança, qualidade dos dados, integridade e responsabilidade.

A LGPD também trata de transmissão de dados, fornecendo diretrizes sobre qualquer troca de dados entre agentes ou Provedores de Serviços de Dados (PSD).

Também existe o direito do usuário de acessar, corrigir ou excluir dados pessoais. Além disso, o usuário pode requerer a portabilidade de seus dados para outro serviço ou exercer seu direito de ser esquecido.

Esses são alguns dos conceitos básicos da LGPD. É fundamental que as organizações tenham conhecimento desses princípios e cumpram as obrigações aplicáveis pela lei para garantir a proteção dos dados pessoais dos indivíduos.

A partir dessas lições, podemos concluir que o tratamento de dados exige uma abordagem segura e responsável. É preciso se certificar de que todas as etapas envolvidas na coleta, armazenamento, uso, compartilhamento e exclusão dos dados são realizadas de forma adequada. Também é essencial que os usuários sejam informados sobre o que acontecerá com seus dados pessoais, e que possam dar seu consentimento antes de serem coletados. Além disso, os usuários têm o direito de acessar, corrigir ou excluir seus dados pessoais, bem como requerer a portabilidade de seus dados para outro serviço. É por isso que, para manter a confidencialidade dos usuários e seguir à risca as regulamentações da LGPD, é essencial que as empresas compreendam e sejam responsáveis em relação ao tratamento de dados.

Este conceito de LGPD contribui para a construção de um ambiente que contemple valores como liberdade, idoneidade e segurança no que diz respeito a dados pessoais. Esta lei estabelece a transparência como princípio fundamental, a fim de que sejam divulgadas políticas de privacidade claras e explícitas, de forma a informar os titulares dos dados sobre o que está acontecendo com eles e como serão tratados

Além disso, de acordo com o disposto na LGPD, o tratamento de dados pessoais dá-se somente com consentimento prévio dos titulares dos direitos, além de sua obrigação de informar ao titular sobre a resposta de dados, o armazenamento e a finalidade do tratamento.

A LGPD foi elaborada com o propósito de desenvolver uma cultura de respeito pelos dados pessoais no Brasil. Geralmente, os dados pessoais são tratados de forma segura, tendo em vista os seus direitos fundamentais e garantindo que eles tenham a devida proteção. O objetivo é estabelecer um pacto de proteção e responsabilidade entre as empresas e os titulares dos dados.

Portanto, a LGPD contribui para a construção de um ambiente de liberdade, idoneidade e segurança no que se refere aos dados pessoais. Essas são algumas das principais diretrizes da lei para garantir que as empresas tratem os dados de forma consciente e garanta um ambiente

seguro para os usuários. Assim, a LGPD deve ser porta-voz e aplicada como proteção de usuários online, empresas e da sociedade como um todo.

Assim, de acordo a carta da Unesco, A transparência é a qualidade de ser aberto, claro e acessível em relação a informações, ações, decisões e processos. É um princípio importante em muitos contextos, incluindo governança, negócios, organizações sem fins lucrativos e governos. (UNESCO),

A transparência não apenas promove a responsabilidade e a prestação de contas, mas também ajuda a evitar a corrupção, a desconfiança e os abusos de poder. Ela é um princípio fundamental para o funcionamento saudável de governos, organizações e sociedades em todo o mundo.

Esses são alguns dos conceitos básicos da LGPD. É fundamental que as organizações tenham conhecimento desses princípios e cumpram as obrigações aplicáveis pela lei para garantir a proteção dos dados pessoais dos indivíduos.

2.2. Principais Objetivos da LGPD

A Lei Geral de Proteção de Dados (LGPD) é o primeiro marco jurídico no Brasil que gera obrigações para tratamento de dados pessoais. Ela tem como principal objetivo tornar a proteção dos direitos de privacidade individuais mais eficaz, ajudando assim na prevenção de crimes cibernéticos.

Para que se alcance esse objetivo é necessário o uso de medidas de segurança cibernética, tais como criptografia, autenticação e controle de acesso. Essas medidas impedem o acesso não autorizado a dados pessoais importantes e ajudam a reduzir os riscos de vazamento de informações e possíveis fraudes.

A LGPD trata não só a questão de segurança, mas também a da responsabilidade, a Lei Geral de Proteção de Dados estipula que todos os agentes envolvidos no tratamento de dados pessoais sejam solidários na área de responsabilidade. Isso significa que eles devem se responsabilizar por qualquer dano ou perda causada aos titulares dos dados, o que incentiva a adoção das necessárias medidas de prevenção contra crimes cibernéticos.

Em relação à responsabilidade civil na Lei Geral de Proteção de Dados (LGPD), o artigo 42 estabelece a obrigação de o controlador ou o operador indenizar o titular de dados pessoais, caso tenha causado algum dano patrimonial, moral, individual ou coletivo, por meio de um tratamento ilegal de dados pessoais.

Tratamento ilícito de dados é aquela que não está de acordo com a LGPD, como enviar emails marketing sem o consentimento do titular, que requer como base legal de consentimento do mesmo, nos termos do Art7, inciso II da LGPD. Outro exemplo de tratamento ilegal é usar os dados do titular para finalidades diversas daquelas informadas, pois o tratamento dos dados deve ser realizado apenas com a finalidade informada ao titular. Nesse sentido, se houver o uso dos dados com alteração dos objetivos estipulados, caracteriza-se como um tratamento ilegal.

Portanto, a LGPD estabelece os direitos a serem seguidos para o uso da informação de titulares de dados pessoais. Quando esses direitos são infringidos, essas empresas serão obrigadas a indenizar os titulares. (LEI Nº 13.709, DE 14 DE AGOSTO DE 2018)

3.CRIMES CIBERNÉTICOS

Os crimes cibernéticos são cada vez mais comuns. Estes criminosos de alto-tecnologia têm a capacidade de violar direitos civis ao usar a tecnologia avançada. Estes criminosos atacam computadores e computação em todo o mundo.

Ataques cibernéticos, como o phishing, ransomware, hacking informático e o uso de malware, preocupam governos e cidadãos em todo o mundo. Os cidadãos devem tomar precauções e prevenção de segurança para evitar os efeitos destes perigos digitais.

Para proteger os direitos civis digitais, os governos precisam promulgar a legislação adequada e as autoridades governamentais devem garantir a sua aplicação adequada. Além disso, é importante que os cidadãos aprendam os principais riscos destes crimes cibernéticos e as melhores práticas para prevenir eficazmente estes tipos de ameaças. Como informa Pereira Otsu.

> O crime cibernético pode ser encarado como uma afronta a um sistema de informação. Os sistemas de informação podem ser definidos como um conjunto de componentes interligados que coletam, processam, armazenam e distribuem informações para apoiar a coordenação, o controle, e a tomada de decisões pelas organizações. (2023, p. 09)

O texto anterior demonstra a compreensão d sobre o crime cibernético enquanto afronta aos sistemas de informação, explorando seus componentes de modo a fornecer uma

base de conhecimento necessária para nortear na tomada de decisões efetivas para evitá-lo. É notável a coerência na construção lógica e textual e a clareza na condução do discurso, informando necessidades e desafios diante da ocorrência de um crime cibernético.

3.1 Tipos De Crimes Cibernéticos

Os crimes cibernéticos tornaram-se cada vez mais comuns nas últimas décadas. Afetam tanto indivíduos quanto empresas, tornando a segurança cibernética uma grande prioridade em todo o mundo. Os tipos de crimes cibernéticos podem variar de invasões à vulnerabilidades nas redes, passando por roubo de informações confidenciais.

Estes crimes podem incluir ações ilegais como invasão de computadores, roubo de informações confidenciais, violação da privacidade, criação de vírus de computador, fraude eletrônica e outras atividades fraudulentas e ilegais. Os crimes cibernéticos podem ter graves consequências econômicas e sociais para os indivíduos, empresas e governos a nível mundial. Muitos governos estão implementando leis e serviços para lidar com o crescimento destes tipos de crimes. Essas leis e serviços estão ajudando a detectar, investigar e punir os perpetradores destas ações ilegais e a prevenir e minimizar o risco de tais infrações serem cometidas.

A fraude é um exemplo de crime cibernético que se tornou muito comum ultimamente. Ela tem vários sub-tipos, incluindo phishing, golpes de cheque falso, roubo de identidade e roubo de cartão de crédito. Essas fraudes podem levar a vítimas a perder dinheiro e até mesmo dados confidenciais importantes, provocando grandes prejuízos financeiros e emocionais.

Outro crime cibernético comum é o ataque de negação de serviço (DDoS). Estes ataques usam robôs para sobrecarregar servidores de computador, possivelmente originando vírus, destruindo dados e criando atrasos nos serviços.

O roubo de informações confidenciais é outro tipo de crime cibernético. Os criminosos usam técnicas sofisticadas para acessar bases de dados privadas, a fim de roubarem informações confidenciais dos usuários. Os dados roubados podem ser usados para obter esses usuários em situações financeiras e emocionais desvantajosas.

Há também o uso indevido de um computador, um crime cibernético que envolve usar um computador para acometer outros crimes. Por exemplo, os criminosos podem usar computadores para monitorar os usuários sem o seu consentimento, fornecer informações a terceiros e até mesmo instalar vírus em outros computadores. Como observado por Rossini:

> O conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva omissiva, praticada por pessoa física ou jurídica, com o uso a informática, em ambiente de rede ou for dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade (ROSSINI, 2004,p.123).

Rossini sugere que esses crimes informáticos alcançam não apenas aqueles praticados no âmbito da internet, mas também são aplicáveis a todas as condutas relacionadas com o sistema informático. Isto inclui, inclusive, delitos em que o computador é usado como uma simples ferramenta, sem a conexão à rede mundial ou a qualquer outra ambiente telemático. Ou seja, as fraudes nos quais o computador é usado como meio delituoso, além da internet, também serão consideradas delitos informáticos.

Destacamos inicialmente que os crimes virtuais não se limitam apenas às práticas na Internet. São todas as ações ou omissões em que o computador é um meio ou instrumento para a prática delitiva, do mesmo modo que poderia ocorrer fora da rede. A Rede não é, portanto, indispensável para a configuração de tais delitos. Como observado por Rossini.

Perante isso, é notório que mesmo com toda a legislação vigente que coíbe os crimes virtuais, o número de denúncias está cada vez maior, e cada vez com novas práticas aperfeiçoadas.

Diante do que foi exposto, o usuário após identificar quaisquer atos abusivos, deverá ir até a delegacia de polícia para registrar um boletim de ocorrência e dependendo da gravidade da situação, começar uma investigação e identificar o autor do crime para que seja combatido os cibercrimes. Ademais, é essencial que o internauta fique atento no mundo virtual para que seja evitado tal tragédia.

Com isso, concluímos que os crimes cibernéticos são uma realidade atual com muitas formas variadas e potencialmente destrutivas. É importante para todos, desde indivíduos até empresas, manter a vigilância e tomar todas as medidas necessárias para proteger o seu meio de vida contra tais invasões.

3.2 Estelionato

É considerado um crime grave, uma vez que viola o direito à privacidade das pessoas. A Lei nº 9.296/1996, conhecida como Lei das Interceptações Telefônicas, prevê a punição para esse tipo de conduta, com pena de reclusão de 2 a 4 anos, além de multa. No entanto, com a expansão da internet, mais pessoas passaram a utilizá-la, aumentando, assim, a oportunidade para a prática de diferentes crimes.

Além dos crimes relacionados à invasão de sistemas e interceptação de dados, também é comum a prática de estelionato na internet. O estelionato é um crime que consiste em obter vantagem ilícita, para si ou para terceiros, induzindo alguém ao erro, por meio de artifício, fraude ou outro meio ardiloso.

O estelionato, tanto no ambiente virtual quanto no físico, consiste em enganar e ludibriar alguém para obter vantagens ilícitas. No contexto da criminalidade virtual, é cada vez mais comum a prática do estelionato por meio de meios digitais. Isso inclui desde a criação de sites fraudulentos de vendas, onde as pessoas são levadas a realizar compras de produtos que nunca receberão, até a criação de perfis falsos em redes sociais para solicitar doações ou empréstimos financeiros.

Desse modo, os crimes virtuais tiveram uma rápida evolução, saindo das práticas de sabotagens e passando a englobar outras práticas criminosas, como por exemplo, o estelionato virtual, roubo e exposição de informações e de imagens íntimas (Ferreira, Santos e Costa, 2019).

No âmbito digital, o estelionato é comumente praticado por meio de golpes online. Isso inclui desde a falsificação de sites e perfis em redes sociais para obter informações pessoais e financeiras das vítimas, até a venda de produtos ou serviços inexistentes. O Código Penal Brasileiro, em seu artigo 171, prevê pena de reclusão de um a cinco anos.

Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, .de 1 (um) a 5 (cinco) anos, e multa. (DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940)

Com o avanço da tecnologia e o aumento do acesso à internet, o estelionato tem se tornado cada vez mais comum nesse meio. A facilidade de comunicação e transações virtuais tem sido explorada por criminosos que se utilizam de artifícios para ludibriar suas vítimas e obter ganhos ilícitos.

Os estelionatários utilizam diversas estratégias para enganar as pessoas e conseguir informações confidenciais, como senhas bancárias e dados pessoais. Uma das principais modalidades de estelionato cometidas pela internet é o phishing, em que os criminosos enviam mensagens ou e-mails falsos, se passando por instituições legítimas, com o objetivo de obter informações sigilosas

3.3 Crimes Contra a Honra

O crime contra a honra consiste no ato de desonrar ou atentar contra a reputação, a dignidade, o bom-nome ou a imagem de outra pessoa – algo que, certamente, não deveria ser incentivado. Essa prática é considerada criminal em diversos países e, de acordo com a Constituição Federal e é conhecida como uma calunia, difamação ou injúria.

O crime de injúria caluniosa é grave, produzindo agressão a pessoas, e somente direitos, especialmente garantidos por meio da Constituição Federal, podem justificar a punição a tais condutas.

O Código Penal define as figuras mais graves de crimes contra a honra como a calúnia, a difamação e a injúria. A calúnia consiste em imputar, a outrem, um fato que o possa degradar socialmente, enquanto a difamação é a imputação de fato determinado que desonre a reputação alheia. A injúria, por sua vez, é a ofensa a reputação, ao crédito, aos bons costumes ou ao decoro ofendendo diretamente a pessoa – existindo de duas formas: a injúria pessoal e a injúria racial.

É interessante notar que as medidas judiciais não se limitam às mais graves formas de crime contra a honra. Em casos considerados menos graves, o Judiciário efetua uma espécie de tutela penal, através de uma retificação ou de uma indenização. Na prática, a pessoa que foi mencionada de forma imprópria em algum veículo de comunicação, por exemplo, não somente deve obter a retratação, como também ser indenizada pelo dano moral produzido, decorrente desta divulgação infeliz.

Não devemos nos esquecer que, não importando em que forma ocorrer, o crime contra a honra é algo absolutamente inaceitável, merecendo de nós um posicionamento sempre contrário a esta prática. Afinal, o bom-nome, a fama e a reputação de cada um de nós devem ser mantidos e não podem ser corroídos por qualquer meio nefasto.

3.4. Impactos dos Crimes Cibernéticos na Sociedade

No mundo atual, a tecnologia se tornou uma parte indispensável da nossa vida cotidiana. Com a evolução da internet e o crescimento exponencial dos meios digitais, também surgiram crimes virtuais, conhecidos como cibercrimes. Para coibir e punir essas condutas, há diversos tipos penais previstos na legislação brasileira. No mundo atual, a tecnologia se tornou uma parte indispensável da nossa vida cotidiana.

O crime cibernético é uma das maiores ameaças à segurança da informação. É uma ameaça que não conhece fronteiras, pois os criminosos estão cada vez mais habilidosos e espertos para elaborar ataques precisos e eficazes.

Os crimes cibernéticos estão cada vez mais presentes em nosso cotidiano, seja na usa de computadores, tablet ou smartphone. Os crimes cibernéticos podem ser definidos como ações ilegais cometidas com o objetivo de prejudicar organizações, usuários ou computadores, por meio da internet. É uma das principais ameaças identificadas atualmente.

Os crimes cibernéticos têm diferentes faces, podendo atingir desde pessoas individuais até grandes corporações. O aumento desses delitos tem um impacto direto sobre a segurança cibernética, pois qualquer ataque pode causar danos materiais ou imateriais, invasão de privacidade, interrupção de serviços, vandalismo e espalhar informação falsa ou notícias sensacionalistas.

Além disso, os crimes cibernéticos também podem afetar o ambiente econômico, uma vez que tendem a causar prejuízos astronômicos para empresas, indivíduos e governos. Por exemplo, os ataques cibernéticos, como o ransomware, que a pessoa infectada deve pagar um resgate ou perder acesso a seus dados, podem causar grandes prejuízos financeiros.

Os criminosos cibernéticos também podem usar as informações obtidas por meio desses ataques para realizar suas próprias atividades criminosas. Por isso, os ataques cibernéticos podem resultar em sérios problemas sociais, tirando dinheiro de bolsos dos cidadãos e gerando insegurança ao desviar bilhões de dólares em arrecadações ilícitas.

Portanto, é necessário desenvolver medidas para conter a prática de crimes cibernéticos. Desde crianças até adultos e idosos devem estar conscientes das ameaças cibernéticas e dos seus riscos, além de adotarem boas práticas para proteger seus bens eletrônicos. A segurança digital deve ser vista não como um custo, mas como um investimento e um hábito, pois é a única forma de nos proteger de inúmeros prejuízos e garantir a nossa segurança.

É importante observar que a legislação relacionada a crimes cibernéticos varia de país para país e pode ser atualizada para acompanhar a evolução das ameaças cibernéticas. Além disso, a complexidade das tecnologias e das táticas utilizadas pelos crimes cibernéticos torna a aplicação das leis e a investigação desses crimes um desafio constante para as autoridades de todo o mundo. Portanto, os elementos específicos dos crimes cibernéticos podem ser definidos de maneira mais específica e adaptados em conformidade com a legislação local.

Em resumo, os crimes cibernéticos têm um impacto abrangente na sociedade, abrangendo aspectos financeiros, de privacidade, segurança nacional, psicológicos e regulatórios. A prevenção e o combate a esses crimes são desafios contínuos que desativam os esforços colaborativos de governos.

4. DESAFIOS NA APLICAÇÃO DA LGPD NO COMBATE AOS CRIMES CIBERNÉTICOS

A LGPD (Lei Geral de Proteção de Dados) é um importante instrumento para assegurar a proteção dos dados no Brasil. Esta lei tem sido bem-vinda, pois requer mais rigor quanto ao manuseio, armazenamento e proteção de informações pessoais. Contudo, sua aplicação traz desafios no combate aos crimes cibernéticos. Consequente à aprovação da Lei Geral de Proteção de Dados (LGPD) no Brasil, trazemos novas exigências quanto à aplicação de conceitos legais e tecnológicos para lidar com questões relevantes de segurança de dados. Por meio desta lei, é possível estabelecer mecanismos de proteção relacionados à privacidade e informações sigilosas, visando a punição de crimes cibernéticos e a utilização indevida de informações confidenciais.

Todavia, diversos desafios interrelacionados a esse novo marco jurídico devem ser enfrentados para o adequado combate a essa espécie de infrações criminais. O primeiro passo a ser dado é o de sensibilização das partes interessadas, para que haja consciência das responsabilidades decorrentes e das diretrizes que a lei estabelece.

No entanto, é necessário salientar que tais desafios não reduzem o poder da LGPD. A lei estabelece regras para proteção de informações pessoais, trazendo um controle maior sobre a infraestrutura e os procedimentos de segurança. Isso significa que as empresas estão obrigadas a seguir a legislação, a fim de evitar prejuízos éticos, legais e financeiros.

Outro ponto relevante a ser destacado diz respeito à responsabilização. Embora a lei tenha trazido maior segurança às empresas, também introduz mecanismos de responsabilização que visam punir quem não cumprir devidamente as regras. Assim, a aplicação da LGPD não gera somente desafios, mas também é uma importante ferramenta para combatê-los.

Ainda de acordo com o Núcleo de Estudos de Segurança da Informação (NESI) da UnB, a LGPD também é um estímulo para que as empresas busquem formas cada vez mais seguras de lidar com seus dados. É um sinal para as companhias que devem elevar os

mecanismos de segurança cibernética, para que sejam capazes de lidar de forma cuidadosa e responsável com as informações de seus clientes.

De forma resumida, a LGDP é um instrumento importantíssimo na proteção de dados no Brasil. Sua aplicação, no entanto, apresenta desafios. Nessas circunstâncias, é necessário que as empresas busquem mecanismos cada vez mais eficazes para estimular a segurança. (ANPD): A busca por práticas seguras e criativas é a única forma de lidar com os constantes desafios da tecnologia.

De acordo com a LGPD, as empresas têm o direito de solicitar à ANPD a proteção de informações consideradas confidenciais, como segredos comerciais ou industriais, que, se divulgadas, podem trazer prejuízos financeiros ou competitivos.

O Projeto de Lei Geral de Proteção de Dados - PL 13.709/18 - (Lei nº 13.709/2018 ou LGPD) veio para mudar completamente o jeito que lidamos com a informação no ambiente digital. A segurança das informações dos usuários sempre foi prioridade para governos, empresas e serviços de tecnologia, sendo a criação de novos padrões e melhores práticas uma forma de evoluir a forma como as pessoas lidam, compartilham e confiam nas informações online. A LGPD é uma lei que foi elaborada para proteger e conceder maior segurança às informações dos usuários.

Assim, a LGPD traz consigo algumas medidas com o intuito de promover a segurança das informações. Em primeiro lugar, ela estabelece princípios e direitos ao consentimento de qualquer usuário antes do uso de seus dados. Estes princípios inere o direito do usuário de ter acesso a seus dados, receber informações claras sobre seu uso e possuir direitos como anonimato, correção, desativação ou interrupção. Em segundo lugar, a lei obriga as empresas a procederem com práticas íntegras na coleta dos dados dos usuários, estabelecendo o levantamento das informações com ética, honra e responsabilidade. Além disso, ela exige sigilo, confidencialidade e integridade desses dados. Por último, a lei solicita que os usuários sejam avisados quando houver violações ou roubo de informações, permitindo que tomem medidas de segurança apropriadas.

De acordo com o artigo 154-A do Código Penal, constitui crime informático invadir disciplinado computador ou sistema informático, mediante violação indevida de mecanismo de segurança e, com o intuito de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do proprietário. Além disso, segundo o artigo 154-B do Código Penal, Pune-se as condutas consistentes na utilização de dispositivo informático, microcomputadores, minicomputadores ou sistema de comunicação informática, para

divulgar mensagem, vídeo, fotografia, som, imagem ou qualquer outra forma de comunicação contendo dados pessoais e íntimos de outrem sem a devida autorização (LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012).

Para lidar com esses desafios, é importante que as autoridades e as empresas implementem políticas e práticas que garantam a conformidade com a LGPD, ao mesmo tempo em que possibilitem o combate eficaz aos crimes cibernéticos. Isso inclui investir em tecnologias de segurança cibernética, promover a cooperação internacional e adotar abordagens transparentes e responsáveis para o tratamento de dados pessoais no contexto de investigações criminais. Além disso, a legislação e as regulamentações podem precisar ser atualizadas para abordar as complexidades do cenário de crimes cibernéticos em constante evolução.

4.1. Dificuldades na Identificação dos Responsáveis Pelos Crimes Cibernéticos

O ciberespaço, nos dias de hoje, está repleto de vários perigos, principalmente quando se trata da segurança dos dados pessoais. Os cibercriminosos estão cada vez mais sofisticados e tecnologicamente espertos, desenvolvendo novas técnicas de violação de segurança para comprometer a privacidade das pessoas. É importante tomar medidas para melhorar a segurança dos dados pessoais e prevenir os crimes cibernéticos.

Uma maneira é se certificando de que todos os seus dispositivos estão sempre atualizados. Instalar todas as atualizações de segurança e sistema relacionadas é essencial para garantir que seu computador ou smartphone não tenham brechas. Outra opção é criar senhas únicas e fortes para todas suas contas. Os novos hackers cibernéticos são capazes de violar até as mais fracas senhas, portanto, é recomendado criar senhas únicas, complexas, e combiná-las com frases de segurança ou palavras-chave únicas.

Para máxima segurança, também seria recomendável gerar senhas aleatórias com caracteres especiais. Outra excelente precaução é habilitar a autenticação de dois fatores, como usar seu celular ou endereço de e-mail para verificação adicional da sua identidade. Além disso, seria sábio não clicar em links suspeitos ou descarregar aplicativos não oficiais a partir de fontes desconhecidas.

Além disso, os cidadãos precisam ficar atentos ao monitorar os cartões de crédito e extratos bancários. Verificar regularmente se houve alguma transação suspeita e notificar prontamente o banco ou empresa seria muito apropriado. Permanecer alerta seria outro mecanismo proativo para combater os crimes cibernéticos.

Em suma, a melhoria da segurança de dados pessoais é uma tarefa complicada, pois os cibercriminosos criam cada vez mais formas avançadas de violar os sistemas de proteção. Por isso, tomar as devidas precauções e se deter às atualizações e procedimentos de segurança de que acabamos de listar é tão importante para proteção de informações confidenciais.

A segurança dos dados pessoais é uma preocupação crítica na era digital, dada a frequência crescente de crimes cibernéticos. Para prevenir esses crimes e proteger os dados pessoais, foram adotadas diversas medidas em níveis individuais, organizacionais e governamentais. Aqui estão algumas das principais medidas tomadas para melhorar a segurança dos dados pessoais.

Discutir as medidas tomadas para melhorar a segurança dos dados pessoais para prevenir crimes cibernéticos. É importante notar que a segurança cibernética é uma responsabilidade compartilhada entre indivíduos, empresas e governos. A colaboração entre essas partes é essencial para prevenir crimes cibernéticos e proteger os dados pessoais. Além disso, as ameaças cibernéticas estão sempre evoluindo, portanto, é importante manter-se atualizado sobre as melhores práticas de segurança cibernética e estar preparado para se adaptar às novas ameaças à medida que surgem.

Segurança Cibernética é uma responsabilidade partilhada entre os indivíduos, empresas e governos. A colaboração entre essas partes é crucial para prevenir crimes cibernéticos e proteger os dados pessoais. Alinhar as atividades de cada parte neste trabalho em conjunto é necessário para evitar perdas financeiras e para preservar a confiança e a privacidade das pessoas. É fundamental acompanhar as melhores práticas de segurança cibernética e estar preparado para se adaptar às novas ameaças à medida que surgem. Desta forma, podemos criar um ambiente seguro para a transação de dados de forma eficaz e segura.

Para superar essas dificuldades, as autoridades e agências de aplicação da lei em todo o mundo precisam cooperar, compartilhar informações e usar técnicas de investigação avançadas.

4.2 Conflitos Entre a LGPD e Outras Leis Relacionadas a Crimes Cibernéticos

Os conflitos entre a LGPD e as leis brasileiras relacionadas à criminalização de crimes cibernéticos costumam surgir pelo fato de que os dados pessoais têm muitas vezes sido usados em delitos informáticos. Por exemplo, quando se trata de fraudes bancárias, ou

roubo de identidade, ou Lavagem de Dinheiro, os dados referentes a cada pessoa são utilizados para eles.

Isso gera crescentes preocupações quanto ao fato de que os dados possam ser usados como meios para a prática de crimes cibernéticos.

Com efeito, a pesquisa já cientificamente comprovou que divergências entre a LGPD e o direito a segurança das informações devem ser enfrentadas de forma que haja uma busca por normas protetivas de dados financeiros e de outras informações e documentos privados, assim como garantir a segurança jurídica para os usos legítimos destes dados.

É necessário encontrar uma equação que equilibre os direitos previstos na LGPD com a necessidade de prevenção dos crimes cibernéticos, além de assegurar que as datas estão sendo usadas de forma adequada e que os usuários têm acesso seguro e livre de preocupações. Isso permitirá que o Brasil alcance todo o seu potencial como nação digital, atendendo às necessidades de todos os cidadãos.

Um exemplo claro dessa tensão ocorre no contexto da investigação de crimes cibernéticos. Enquanto a LGPD estabelece padrões rígidos para a coleta, armazenamento e processamento de dados pessoais, as leis de combate a crimes cibernéticos muitas vezes exigem a coleta e análise de dados para rastrear crimes digitais. Isso levanta questões sobre como conciliar a necessidade de investigações com o direito à privacidade dos indivíduos.

Nesse sentido, é vital que os legisladores se esforcem para equilibrar a proteção de dados explícita e generalizada fornecida pela LGPD e os meios essenciais de segurança para proteger os cidadãos contra a metamorfose incessante destinada à criminalidade informática.

A LGPD faz parte de um marco geral de direitos privacidade reconhecido no país e, embora desafiante, é necessário alinhar o direito fundamental à privacidade com o bom exercício das atividades de polícia e inteligência da Autoridade Nacional, de forma a proporcionar a segurança necessária para seus cidadãos por isso ABIN tem trabalhado arduamente para garantir a proteção da privacidade das informações confiadas à autoridade e estabelecer um quadro nacional que garanta essa proteção aos cidadãos.

Assim, ao aderir à LGPD, espera-se que o estado use os direitos dos cidadãos à proteção dos dados pessoais como uma ferramenta para prevenir ou pelo menos reduzir os conflitos com outras leis relacionadas a crimes cibernéticos.

No geral, há uma necessidade de encontrar um equilíbrio que permita simplesmente punir os infratores, mas também corrigir o problema de proteção de dados pessoais existente

no Brasil. A LGPD, ao propor um caderno de boas práticas a serem seguidas pelos titulares dos dados pessoais, ajudará a melhorar as condições de segurança relacionadas à proteção dos mesmos. De acordo com o art. 14 da Lei Geral de Proteção de Dados (LGPD) falar sobre o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. Portanto a coleta de informações está dentro dos limites aceitáveis. Com isso, a mãe fica mais tranquila, sabendo que seus dados pessoais estão sendo tratados de forma adequada. (LEI Nº 13.709, DE 14 DE AGOSTO DE 2018)

Nesse contexto, é essencial que o poder legislativo e o judiciário trabalhem em conjunto para criar uma estrutura legal que harmonize a LGPD com as leis relacionadas aos crimes cibernéticos, garantindo que as investigações sejam incluídas de maneira eficaz e ao mesmo tempo respeitando os direitos de privacidade dos cidadãos. A colaboração entre as partes interessadas, incluindo a sociedade civil e especialistas em tecnologia, é fundamental para encontrar soluções equilibradas que protejam tanto os dados pessoais quanto a segurança digital.

4.3 A Importância da Atualização Constante da LGPD e Novas Tecnologias e Desafios Para a Proteção de Dados Pessoais

Atualmente, a Lei Geral de Proteção de Dados (LGPD) é o tema mais relevante quando se trata de garantir proteção às informações pessoais. Seu objetivo é definir regras capazes de orientar empresas, governos e organizações na coleta, tratamento e proteção de dados pessoais. Assim, a atualização constante, em razão da evolução tecnológica, torna-se fundamental para garantir a eficácia da lei.

De acordo com a LGPD, as informações pessoais de - quer sejam cidadãos, trabalhadores, clientes - devem ser tratadas adequadamente de forma que se assegure a segurança destes dados e o respeito a eles. No entanto, inclusive a aplicação desta lei possibilita novos desafios devido a constante evolução tecnológica.

Por isso a atualização da LGPD tornou-se tão importante, uma vez que é necessário acompanhar o ritmo das novas tecnologias e as suas possibilidades para garantir a proteção dos dados.

Um exemplo disso é a inteligência artificial. De acordo com um estudo realizado pela IBM, a Inteligência Artificial poderá gerar $ 2,+ trilhões em aplicações em todo o mundo a partir da idade e engenhosidade como forma de tratamento de informações pessoais.

Nesse sentido, o desafio é criar mecanismos capazes de assegurar a segurança de todas essas informações, a fim de que não haja abusos ou explorações indevidas.

A inteligência artificial tem tudo a ver e, portanto, para garantir o cumprimento da LGPD, é necessário que sejam construídas medidas de segurança que contemplem e regulamentem os tratamentos de dados.

De forma geral, a atualização regular da Lei Geral de Proteção de Dados, além da implementação de sistemas e processos de segurança avançados são medidas fundamentais para o cumprimento dessa norma, assim como para garantir a proteção de dados pessoais.

A tecnologia é um dos mais importantes investimentos que as empresas, governos e organizações podem fazer para a garantia de segurança das informações pessoais. Segundo defende Kaio Alves:

> A cada acesso à internet, o usuário deixa registrado vários dados pessoais, o que se torna informação. A informação passou a ser um ativo de grande relevância no ambiente virtual e despertou grande interesse por parte das instituições. Mas o que é feito com essas informações despertou na sociedade a necessidade de proteção aos seus dados. E de uma lei que regulamentasse seus direitos à privacidade e a proteção de dados. (2023, p. 6)

Assim, em relação à proteção de dados pessoais, investir e aprimorar continuamente é uma questão fundamenta. Isso porque garantir que as informações estejam em locais seguros possibilita a segurança na navegação na internet e também a ampliação da confiança dos usuários.

Segundo Art.1° da Lei n° 13.709/2018, cita que Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. (LEI N° 13.709/2018)

A melhor solução para que as organizações trabalhem de forma segura e dentro da LGPD é a adoção de uma cultura de conformidade contínua. Isso significa que as equipes devem estar sempre atualizadas e conscientes das mudanças ocorridas, e que as ferramentas e processos devem ser avaliados e atualizados constantemente, para que não haja conformidades potenciais. Além disso, é importante que os usuários da empresa se sintam responsáveis e comprometidos em identificar e notificar o gerenciamento de sua equipe quando identificarem prazos de implementação não cumpridos ou outras formas de não conformidade.

Conforme defende o Auto Kaio Alves (2023, p.30) de acordo com o art. 50, § 1º da LGPD, a ANPD poderá levar em conta, quando aplicar multas, mecanismos para

minimização de dano, boas práticas e governança e medidas corretivas. Dessa forma, argumenta-se que a responsabilização e a prestação de contas previstas na lei podem servir de parâmetro também para ações judiciais.

Nesse sentido, a internet desempenha um papel crucial na promoção da cidadania, buscando assegurar tanto a liberdade de expressão quanto a privacidade. Só assim será possível alcançar um ambiente onde os direitos fundamentais sejam respeitados.

Contar com sistemas avançados de segurança da informação o e a atualização contínua da LGPD é fundamental para aumentar a confiança dos usuários e para garantir a segurança de suas informações pessoais. Pode-se dizer que é indispensável o investimento adequado para garantir a segurança dos dados.

CONSIDERAÇÕES FINAIS

Ao longo deste trabalho, explorei a aplicabilidade da Lei Geral de Proteção de Dados (LGPD) na prevenção de crimes cibernéticos. A LGPD, que entrou em vigor no Brasil em setembro de 2020, trouxe importantes mudanças no cenário da proteção de dados pessoais e privacidade dos indivíduos.

Ficou claro ao longo da pesquisa que a LGPD desempenha um papel crucial na prevenção de crimes cibernéticos. Ao estabelecer diretrizes rígidas para a coleta, armazenamento e tratamento de dados pessoais, a lei cria uma base sólida para a segurança cibernética. Além disso, a LGPD estabelece a obrigação de notificação de violações de dados, o que é fundamental para identificar e responder rapidamente a ataques cibernéticos.

No entanto, também foi evidente que a aplicação eficaz da LGPD requer esforços conjuntos do governo, empresas e cidadãos. É necessário um investimento contínuo em conscientização, capacitação e tecnologias de segurança cibernética para garantir o cumprimento da lei e a proteção dos dados pessoais.

Além disso, a cooperação internacional desempenha um papel crucial na prevenção de crimes cibernéticos, dada a natureza transnacional desses delitos. O compartilhamento de informações e a colaboração entre países são essenciais para enfrentar ameaças cibernéticas globais.

Portanto, concluímos que a LGPD é uma ferramenta poderosa na luta contra os crimes cibernéticos, mas seu sucesso depende da ação coletiva e da vigilância constante. À medida que o cenário da segurança cibernética continua a evoluir, é fundamental que o Brasil

e outros países adaptem suas leis e estratégias para proteger eficazmente os dados pessoais e enfrentar as ameaças cibernéticas em constante evolução.

Este TCC é apenas um passo inicial na exploração desse tema complexo e em constante mudança. Espero que esta pesquisa inspire futuros estudos e discussões sobre como a LGPD pode ser ainda mais eficaz na prevenção de crimes cibernéticos e na proteção da privacidade dos indivíduos.

Mais uma vez, agradeço a todos que contribuíram para este trabalho e estou ansioso para futuras investigações e avanços na área da segurança cibernética e proteção de dados.

REFERÊNCIAS

BRASIL. Brasília, DF: Presidência da República. **Lei nº 12.527, de 18 de novembro de 2011**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm#art1> Acesso em: 25 out. 2023.

BRASIL, Brasília, DF: **Presidência da República**, Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 12 de outubro de 2023

BRASIL, Brasília, DF: Constituição (1988). Constituição da República Federativa do Brasil. **Art 5 - X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação**; Brasília, DF: Senado Federal, 2016. Disponível em 2016 <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 12 de outubro de 2023

BRASIL, Brasília, DF: Presidência da República. Lei nº 13.709, de 14 de agosto de 2018. **Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses**: II - para o cumprimento de obrigação legal ou regulatória pelo controlador; Presidência da República Secretária-geral, 2019.Disponível em<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 02 de novembro de 2023

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Vigência. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências**. Brasília, DF: Presidência da República Disponível em: 7 dezembro 1940< https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 25 de setembro 2023

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências**. Brasília, DF: Presidência da República. Brasília, DF: Presidência

da República,2012. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 02 de nov.2023.

BRASIL. Decreto-Lei no 2.848, de 7 de dezembro de 1940. **Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento**:
Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. Brasília, DF: Presidência da República. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm > Acessado em 10 de nov de 2023

BRASIL. **Lei Geral de Proteção de Dados Pessoais, Lei 13.709/2018**. Diário Oficial da União, Brasília, DF. 14 de agosto de 2018, seção I, p. 1-6. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/l13709.htm>Acesso em: 07 de SETEMBRO 2023

BRASIL. Lei n° 13.709/2018, de 14 de agosto 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)** Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais. Brasília, DF: Presidência da República. Brasília, DF: Presidência da República,2012. Disponível em:< https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em 02 de nov.2023

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal**; e dá outras providências. Brasília, DF: Presidência da República. Brasília, DF: Presidência da República,2012. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 02 de nov.2023.

Brasília, DF: Presidente da República, **LEI N° 13.709/2018**. Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/l13709.htm#:~:text=Art.%201%C2%BA%20Esta%20Lei%20disp%C3%B5e,da%20personalidade%20da%20pessoa%20natural.> . Acesso em: 02 out. 2023

CABETTE, Eduardo Luiz Santos. **Artigo 1º, parágrafo único, da lei nº 9.296/1996 e a questão da constitucionalidade**. Disponível em:
https://repositorio.idp.edu.br/bitstream/123456789/577/1/Direito%20Publico%20n212008_Eduardo%20Luiz%20Santos%20Cabette.pdf> Acesso em agosto de 2023
CAIRES, Kaio Alves. **A proteção dos dados e a LGPD: desafios na implementação da LGPD**. e - Publica - Pontifícia Universidade Católica de Goiás, Goiás 2023. Disponível em: 31-Mai-2023. <
https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/6439/1/KAIO%20ALVES%20CAIRES.pdf> Acesso em: 10 de setembro 2023

DANIEL, Maycon Antônio et al. **A evolução e aplicação da segurança da informação por meio da lei geral de proteção de dados pessoais (lgpd)**: um estudo de caso em uma instituição financeira. Foco. Disponível em:<https://repositorio.ufsc.br/bitstream/handle/123456789/233375/TCC%20MAYCON.pdf?sequence=1&isAllowed=y> Acesso em agosto de 2023

Declaração universal da UNESCO sobre a diversidade cultural. **UNESCO**. Disponível em: 2002<http://unesdoc.unesco.org/images/0012/001271/127160por.pdf>. Acesso em: 15 de outubro de 2023

DENISE, Pereira Otsu. **Crimes cibernéticos e os limites da liberdade de expressão nas redes**. e - Publica - Centro Universitário São Judas Tadeu Campus Mooca, São Paulo, 2023. Disponível em:<https://repositorio.animaeducacao.com.br/bitstream/ANIMA/35166/1/CRIMES%20CIBERNE%CC%81TICOS%20%281%29.pdf> Acesso em: 15 de out 2023

FRAZÃO, Ana. Nova LGPD: **principais repercussões para a atividade empresarial**. Disponível em: <www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial-29082018>. Acesso em: 10.02.2023

IZIDRO, Augusto. **Crimes Cibernéticos. 2023, delito informático**, f6. Disponível em:https://repositorio.animaeducacao.com.br/bitstream/ANIMA/35156/1/CRIMES%20CIBERN%c3%89TICOS%20%20.pdf>. Acesso em 02 de nov. 2023

MALDONADO, Viviane; BLUM, Renato. Seção II. Do Tratamento de Dados Pessoais Sensíveis In: Maldonado, Viviane; BLUM, Renato. Lgpd - **Lei Geral de Proteção de Dados Pessoais Comentada**. São Paulo (SP): Editora Revistados Tribunais.2021. Disponível em: <https://www.jusbrasil.com.br/doutrina/lgpd-lei-geral-de-proteção-de-dados-pessoais-comentada/1198081131>. Acesso em: 12 de novembro de 2023.>

Marra, Fabiane. (2019**). Desafios do Direito na Era da Internet: uma breve análise sobre os crimes cibernéticos**. Journal of Law and Sustainable Development. 7. 145-167. 10.37497/sdgs.v7i2.51. f8. Disponível em: 12/12/2019< https://ojs.journalsdg.org/jlss/article/view/51 > Acesso em : 15 de setembro 2023

MPF et al. MPF: Lei Geral de Proteção de Dados. In: LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) : **Lei Geral de Proteção de Dados**. [S. l.], 2023. Disponível em:<https://www.mpf.mp.br/servicos/lgpd>. Acesso em: 10 out. 2023.

SILVA, Hemili Oliveira Fernandes da. Lei geral de proteção de dados**: uma análise da evolução do direito frente ao desenvolvimento da sociedade**. 2022. Disponível em: <http://repositorio.unitau.br/jspui/bitstream/20.500.11874/6201/1/TG%20Hemili%20Oliveira%20Fernandes%20da%20Silva.pdf>. Acesso em: 02 de nov.2023