INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO

NICOLLY PEREIRA ROMÃO

IMPACTO DA LGPD NA SEGURANÇA CIBERNÉTICA: UMA ANÁLISE DAS VIOLAÇÕES DE DADOS E CRIMES DIGITAIS

Cubatão
2023

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO

NICOLLY PEREIRA ROMÃO

IMPACTO DA LGPD NA SEGURANÇA CIBERNÉTICA: UMA ANÁLISE DAS VIOLAÇÕES DE DADOS E CRIMES DIGITAIS

Projeto apresentado ao Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – Campus Cubatão como parte dos requisitos necessários para a avaliação do componente Projeto de Sistemas do curso Técnico em Informática Integrado ao Ensino Médio, sob a orientação do professor Mauricio Neves Asenjo.

Cubatão
2023

AGRADECIMENTOS

Agradeço a todos os que me ajudaram na elaboração deste trabalho, mesmo quando decidi realizá-lo sozinha, vocês não soltaram minha mão e confiaram no meu projeto, em especial agradeço à minha mãe, que sempre me apoiou e incentivou, meu orientador Thiago Silva Augusto da Fonseca, com muitas dicas e sempre me passando confiança, e também ao meu orientador de pesquisa científica, Artarxerxes Tiago Tácito Modesto que estava do meu lado durante todo o ano acadêmico, não poderia deixar de incluir as profissionais da Coordenadoria Sócio-Pedagógica do campus, Maria das Neves Farias Dantas Bergamaschi, Waldísia Rodrigues de Lima, e Gisele Assunção de Andrade, que nunca me deixaram desistir.

RESUMO

Este Trabalho de Conclusão de Curso (TCC) visa analisar a apropriação indevida de dados em meio à era digital, com um enfoque especial nas implicações da Lei Geral de Proteção de Dados (LGPD). A rápida evolução tecnológica tem elevado a frequência e complexidade das violações de dados, exigindo uma abordagem jurídica e técnica mais refinada para garantir a segurança e privacidade das informações pessoais. Este estudo busca explorar casos emblemáticos nos quais a LGPD foi invocada, examinando como essa legislação impactou a resposta legal e a prevenção desses incidentes. Além disso, pretende-se avaliar o papel crucial da LGPD na promoção de uma cultura de proteção de dados e segurança cibernética, proporcionando insights para um ambiente digital mais seguro e responsável.

Palavras-chave: Apropriação Indevida de Dados, LGPD, Privacidade, Segurança Cibernética, Violação de Dados, Lei Geral de Proteção de Dados.

ABSTRACT

This Course Completion Work (TCC) aims to analyze the misappropriation of data in the digital era, with a special focus on the implications of the General Data Protection Law (LGPD). Rapid technological evolution has increased the frequency and complexity of data breaches, requiring a more refined legal and technical approach to guarantee the security and privacy of personal information. This study seeks to explore emblematic cases in which the LGPD was invoked, examining how this legislation impacted the legal response and prevention of these incidents. Furthermore, we intend to evaluate the crucial role of LGPD in promoting a culture of data protection and cybersecurity, providing insights for a safer and more responsible digital environment.

Key-words: Misappropriation of Data, LGPD, Privacy, Cybersecurity, Data Breach, General Data Protection Law.

SUMÁRIO

INTRODUÇÃO

Nos dias atuais, o cenário digital desempenha um papel cada vez mais central em nossas vidas, moldando a forma como nos comunicamos, fazemos compras, acessamos informações e interagimos com o mundo ao nosso redor. No entanto, junto com essa revolução tecnológica, emergem desafios complexos, dos quais os crimes digitais e a apropriação indevida de dados surgem como ameaças significativas.

Os crimes digitais abrangem um vasto espectro de atividades ilegais realizadas através de meios eletrônicos. Isso pode incluir desde a disseminação de malware e ataques cibernéticos até fraudes online, phishing e apropriação indevida de dados. A apropriação indevida de dados refere-se à prática criminosa de adquirir, acessar, compartilhar ou manipular informações confidenciais, pessoais ou sensíveis, sem o consentimento do proprietário desses dados. Essa ação criminosa é facilitada pelas inúmeras oportunidades oferecidas pelo ambiente digital. A vasta quantidade de informações pessoais armazenadas em bancos de dados online, redes sociais, contas de e-mail e outros serviços digitais se tornou um alvo valioso para criminosos cibernéticos. Através de técnicas como invasões de sistemas, phishing e engenharia social, esses atores maliciosos conseguem explorar vulnerabilidades para obter acesso a informações preciosas.

Os prejuízos decorrentes da apropriação indevida de dados são extensos e podem ter impactos devastadores em vários níveis. Em escala individual, a vítima pode enfrentar roubo de identidade, perda financeira, invasão de privacidade e comprometimento de informações pessoais sensíveis. Além disso, a divulgação não autorizada de informações pessoais pode levar a ataques de chantagem, assédio online e até mesmo danos à reputação.

Em um âmbito mais amplo, os prejuízos se estendem à sociedade como um todo. Grandes vazamentos de dados podem resultar em perdas econômicas significativas para as empresas, danificando sua reputação e levando a litígios legais. Além disso, a disseminação de informações falsas ou manipuladas provenientes de apropriação indevida pode minar a confiança nas instituições, afetando a credibilidade de fontes de notícias e governos.

Para combater eficazmente a apropriação indevida de dados nos crimes digitais, são necessários esforços coordenados de governos, empresas e indivíduos. Medidas de segurança cibernética robustas, educação sobre segurança digital e conscientização pública são componentes-chave na mitigação desses riscos. Tal apropriação indevida de dados nos crimes digitais destacam a importância de regulamentações como a Lei Geral de Proteção de Dados (LGPD). À medida que nossa sociedade continua a se adaptar à era digital, a proteção dos dados pessoais e a prevenção de crimes cibernéticos devem permanecer como prioridades cruciais para garantir um ambiente online seguro e confiável.

A LGPD

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que entrou em vigor no Brasil em agosto de 2020 e estabelece regras e diretrizes para o uso, coleta, armazenamento e compartilhamento de dados pessoais por organizações públicas e privadas.

A LGPD se aplica a qualquer empresa, organização ou entidade que realize atividades de tratamento de dados pessoais dentro do território brasileiro ou que ofereça bens ou serviços para indivíduos localizados no Brasil. Ela abrange uma ampla gama de situações em que ocorre o tratamento de dados pessoais, incluindo a coleta, armazenamento, uso, compartilhamento, transferência e exclusão de informações que possam identificar uma pessoa física.

Alguns dos principais princípios e regulamentos da LGPD incluem:

Consentimento: O tratamento de dados pessoais só é permitido mediante o consentimento livre, informado e inequívoco do titular dos dados ou de seu representante legal.

Finalidade: Os dados pessoais devem ser coletados para finalidades específicas, explícitas e legítimas, devendo ser utilizado apenas para os propósitos informados ao titular.

Necessidade: O tratamento de dados pessoais deve ser limitado ao mínimo necessário para atingir a finalidade pretendida, evitando-se a coleta excessiva de informações.

Transparência: As organizações devem fornecer informações claras e acessíveis aos titulares dos dados sobre como seus dados pessoais são coletados, usados, armazenados e compartilhados.
Segurança: Deve-se garantir a proteção adequada dos dados pessoais, adotando medidas técnicas e organizacionais para prevenir vazamentos, perdas ou acessos não autorizados.
Direitos dos titulares: A LGPD concede aos titulares dos dados uma série de direitos, como o acesso aos dados, a correção de informações incorretas, a exclusão de dados desnecessários ou tratados em desconformidade, entre outros.
Responsabilidade: As organizações são responsáveis por garantir o cumprimento da LGPD e devem adotar medidas internas para promover a conformidade, incluindo a designação de um encarregado de proteção de dados (DPO) e a realização de avaliações de impacto à privacidade.

A LGPD estabelece também a Autoridade Nacional de Proteção de Dados (ANPD) como órgão responsável por supervisionar, orientar e aplicar sanções em caso de descumprimento da lei.

A ANPD

A ANPD (Autoridade Nacional de Proteção de Dados) é o órgão responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados (LGPD) no Brasil. Ela foi criada pela própria LGPD e tem papel fundamental na aplicação da lei. A ANPD é uma entidade autônoma, vinculada à Presidência da República, e possui autonomia técnica, decisória e independência no exercício de suas atribuições. Suas principais responsabilidades incluem em orientação, normatização e cooperação internacional,

É importante ressaltar que a ANPD atua de forma complementar aos demais órgãos reguladores e fiscalizadores existentes, como o Ministério Público, a Secretaria Nacional do Consumidor e a Agência Nacional de Proteção de Dados. Essa cooperação entre as instituições fortalece a proteção dos dados pessoais no Brasil e promove a conformidade com a LGPD.

A ANPD possui autoridade para fiscalizar e aplicar sanções em caso de descumprimento da LGPD. Isso significa que ela tem poder para investigar denúncias de violações à privacidade e proteção de dados pessoais, solicitar informações e documentos às organizações, aplicar sanções administrativas e impor medidas corretivas. Dentre as sanções previstas pela LGPD, a ANPD pode aplicar advertências, multas, bloqueio ou eliminação de dados pessoais, além de outras medidas que visem à conformidade das organizações com a lei. O valor das multas pode chegar a 2% do faturamento da empresa, limitado a R$ 50 milhões por infração.

Além da fiscalização e aplicação de sanções, a ANPD também desenvolve um papel essencial na orientação e capacitação das organizações e dos cidadãos sobre as melhores práticas de proteção de dados pessoais. Ela emite diretrizes, normas e orientações para auxiliar na interpretação da LGPD e na implementação de medidas adequadas de segurança e privacidade.

No entanto, é válido mencionar que a aplicação da LGPD não é exclusiva da ANPD. Outros órgãos reguladores, como o Ministério Público e a Secretaria Nacional do Consumidor, também têm competência para fiscalizar e aplicar penalidades em casos de descumprimento da lei. A atuação conjunta desses órgãos é essencial para assegurar o cumprimento e a efetividade da LGPD no Brasil.

PENALIDADES

A Lei Geral de Proteção de Dados (LGPD) estabelece uma série de penalidades que podem ser aplicadas em caso de descumprimento das disposições da lei. As penalidades podem variar de acordo com a gravidade da infração e a natureza dos dados pessoais envolvidos. Algumas das possíveis penalidades incluem:

Advertência: A ANPD (Autoridade Nacional de Proteção de Dados) pode emitir uma advertência formal à organização infratora, informando sobre a irregularidade e recomendando medidas corretivas.

Multa simples: A ANPD pode aplicar multas simples, que podem chegar a 2% do faturamento da organização infratora no último exercício, limitado a um total de R$ 50 milhões por infração.

Multa diária: Em casos de infrações continuadas, a ANPD pode impor multas diárias à organização infratora até que a irregularidade seja corrigida.
Publicização da infração: A ANPD pode determinar a publicização da infração, divulgando publicamente os detalhes da violação e da penalidade aplicada, de forma a informar o público sobre o descumprimento da lei.
Bloqueio ou eliminação de dados pessoais: A ANPD pode determinar o bloqueio dos dados pessoais envolvidos na infração, impedindo o seu acesso e uso, ou exigir a eliminação dos dados que tenham sido coletados e/ou tratados de forma irregular.

Além das penalidades administrativas, a LGPD também prevê a possibilidade de reparação de danos pelos titulares dos dados afetados. Isso significa que os indivíduos que tiverem seus direitos violados em relação à proteção de seus dados pessoais podem buscar indenizações e compensações por eventuais danos morais ou materiais sofridos.
É importante ressaltar que a aplicação das penalidades é de responsabilidade da ANPD e de outros órgãos competentes, como o Ministério Público e a Secretaria Nacional do Consumidor. A gravidade da infração, a reincidência, o porte da organização e outros fatores podem ser considerados na determinação das penalidades aplicadas

STJ SUPERIOR TRIBUNAL DE JUSTIÇA

O art. 2º da Lei Geral de Proteção de Dados Pessoais - LGPD, expressa os seguintes fundamentos:

I – o respeito à privacidade;

II - a autodeterminação informativa;

III – a liberdade de expressão, de informação, de comunicação e de opinião;

IV – à inviolabilidade da intimidade, da honra e da imagem;

V – o desenvolvimento econômico e tecnológico e a inovação;

VI – a livre-iniciativa, a livre concorrência e a defesa do consumidor;

VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A LGPD é aplicável a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país no qual estejam localizados os dados, desde que a operação de tratamento de dados seja realizada no Brasil; a atividade de tratamento tenha por objetivo a oferta de bens ou serviços ou o manejo de dados de indivíduos localizados no país; ou, ainda, que os dados pessoais objeto do tratamento tenham sido coletados em território nacional.

Entretanto, estão excluídos da aplicação da lei alguns meios de tratamentos de dados, a exemplo daqueles realizados para fins exclusivamente jornalísticos, artísticos e acadêmicos, além de informações relacionadas exclusivamente à segurança pública, defesa nacional, segurança do Estado e a atividades de investigação e repressão de infrações penais.

A LGPD e o STJ

Leia o relatório da auditoria do TCU sobre as ações implementadas pelo STJ

Iniciativas do STJ para garantir o cumprimento das disposições da Lei Geral de Proteção de Dados e do CNJ:

Instituição de Comitê Gestor de Proteção de Dados Pessoais (LGPD), responsável pelo processo de implementação da LGPD no Tribunal: Portaria STJ/GDG 178/2021 e alterações. (art. 1º, I, "a", da Res. CNJ 363/2021);

Realização de ações de capacitação: cursos básicos de proteção de dados pessoais, a LGPD e o Serviço Público, Transferência Internacional de Dados Pessoais na LGPD e no RGPD.[1]

[1] O Regulamento Geral sobre a Proteção de Dados 2016/679 é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Económico Europeu que foi criado em 2018. Regulamenta também a exportação de dados pessoais para fora da UE e EEE.

Publicação do Aviso de cookies no portal do STJ. (art. 1º, VI, “a”, da Res. CNJ 363/2021);

Publicação da Política de privacidade para navegação (art. 1º, VI, “b”, da Res. CNJ 363/2021);

Publicação da Política de Proteção de Dados Pessoais: Portaria STJ/GP N. 197 (art. 1º, VI, “c”, da Res. CNJ 363/2021)

Registro de Operações (inventário) de tratamento de dados pessoais por meio do aplicativo desenvolvido pelos servidores do STJ (art. 1º, XII e art. 2º, I, ambos da Res. CNJ 363/2021);

OBJETIVOS

OBJETIVO

O objetivo deste Trabalho de Conclusão de Curso (TCC) é analisar de forma abrangente as implicações da Lei Geral de Proteção de Dados (LGPD) no contexto das violações de dados e crimes digitais. A pesquisa visa compreender como a implementação da LGPD influencia a prevenção, detecção e combate a incidentes de segurança cibernética, incluindo a apropriação indevida de dados, ataques de phishing, roubo de informações pessoais e outras atividades criminosas relacionadas à esfera digital.

MOTIVAÇÃO

A crescente digitalização de informações e transações trouxe consigo uma série de benefícios e facilidades à sociedade moderna. No entanto, essa evolução tecnológica também gerou novos desafios, especialmente no que diz respeito à segurança dos dados pessoais e à ocorrência de crimes digitais. A Lei Geral de Proteção de Dados (LGPD) surge como uma resposta crucial a essas preocupações, estabelecendo diretrizes rigorosas para a coleta, o processamento e a proteção de informações pessoais.

A motivação para este Trabalho de Conclusão de Curso (TCC) reside na necessidade de compreender profundamente os impactos da LGPD no contexto das violações de dados e crimes digitais. A entrada em vigor da LGPD gerou uma mudança significativa na forma como organizações coletam e utilizam informações pessoais, bem como nas medidas de segurança cibernética que precisam ser implementadas para proteger esses dados. Essas mudanças têm implicações tanto para empresas quanto para indivíduos, uma vez que a violação de dados pessoais pode levar a danos financeiros, perda de privacidade e até mesmo a situações de chantagem ou extorsão.

Além disso, a LGPD também busca trazer mais responsabilidade e transparência para o tratamento de dados pessoais, permitindo que os indivíduos tenham maior controle sobre suas informações e saibam como elas estão sendo usadas. Entender como a aplicação da LGPD afeta a prevenção, detecção e reação a violações de dados e crimes digitais é crucial para avaliar a eficácia dessa legislação na proteção da sociedade em um mundo cada vez mais digital e interconectado.

Por conseguinte, este estudo busca não apenas explorar as implicações legais e técnicas da LGPD no contexto da segurança cibernética, mas também contribuir para a conscientização sobre a importância da proteção de dados e boas práticas de segurança cibernética. A motivação subjacente é fornecer informações valiosas para a tomada de decisões informadas por parte de empresas, indivíduos e legisladores, visando a um ambiente digital mais seguro e resiliente diante dos desafios do cenário tecnológico contemporâneo.

JUSTIFICATIVA

A justificativa para a realização deste Trabalho de Conclusão de Curso (TCC) repousa na importância inegável da Lei Geral de Proteção de Dados (LGPD) como uma ferramenta crucial para a proteção dos dados pessoais em um mundo digital em constante evolução. Com a crescente frequência de violações de dados e crimes digitais, é fundamental investigar como a implementação da LGPD tem influenciado a prevenção, detecção e resposta a esses incidentes, a fim de compreender seus impactos e contribuições para a sociedade e o setor empresarial.

A proteção dos dados pessoais tornou-se uma prioridade global, uma vez que informações confidenciais são frequentemente compartilhadas e armazenadas digitalmente, aumentando as oportunidades para cibercriminosos e violadores de dados. A LGPD busca remediar essa preocupação, estabelecendo um conjunto de diretrizes destinadas a garantir a privacidade e a segurança dessas informações. No entanto, é essencial avaliar até que ponto essas diretrizes têm sido eficazes na mitigação dos riscos associados às violações de dados e aos crimes digitais.

Além disso, este estudo encontra relevância no contexto de um ambiente corporativo altamente competitivo, onde a confiança do consumidor é um ativo valioso. Organizações que adotam medidas proativas para garantir a segurança dos dados pessoais de seus clientes podem ganhar uma vantagem competitiva significativa, fortalecendo a confiança do público em suas operações e serviços.

Outra justificativa reside no fato de que o avanço tecnológico não mostra sinais de desaceleração, tornando necessário o aprimoramento constante das medidas de segurança cibernética. Uma investigação aprofundada sobre a relação entre a LGPD e a

mitigação de crimes digitais contribuirá para o conhecimento geral sobre como as regulamentações podem ser adaptadas para enfrentar os desafios em constante mutação do cenário cibernético.

Portanto, este TCC visa preencher uma lacuna de conhecimento ao explorar os efeitos da LGPD nas violações de dados e crimes digitais. A pesquisa realizada terá o potencial de oferecer insights valiosos para profissionais de segurança cibernética, empresas, legisladores e indivíduos, ao mesmo tempo em que contribui para um debate informado e direcionado a um ambiente online mais seguro e confiável.

REFERENCIAL TEÓRICO

Ao detalharmos casos de apropriação indevida de dados, nos deparamos com situações em que a LGPD entrou em jogo, demonstrando seu impacto no âmbito legal e suas implicações na resposta a esses incidentes. Esta análise oferece insights valiosos sobre como a regulamentação pode afetar diretamente a abordagem das organizações diante de violações de dados e crimes digitais, buscando mitigar os prejuízos e fortalecer a proteção dos direitos individuais.

British Airways

O caso envolvendo a British Airways está relacionado a um vazamento massivo de dados pessoais. Em setembro de 2018, a British Airways anunciou que havia sofrido um ataque cibernético que resultou no vazamento de dados pessoais de cerca de 500.000 clientes. Os dados comprometidos incluíam informações como nomes, endereços de email, números de cartão de crédito e detalhes de pagamento.

O ataque ocorreu por meio de um skimming de dados em seu site e aplicativo móvel, no qual os invasores conseguiram redirecionar os clientes para um site falso e capturar suas informações de pagamento durante o processo de reserva de voos.

Após a descoberta do vazamento, a British Airways prontamente informou às autoridades competentes e tomou medidas para conter o incidente, reforçar sua segurança e auxiliar os clientes afetados. O caso foi investigado pelas autoridades competentes, resultando em uma multa proposta pela Autoridade de Proteção de Dados do Reino Unido (ICO, na sigla em inglês) no valor de £20 milhões em 2020, embora esse valor possa ter sido alterado em atualizações posteriores.

É importante notar que, além das multas impostas por reguladores, a British Airways também enfrentou ações judiciais movidas por clientes afetados em busca de compensação pelos danos sofridos em decorrência do vazamento de dados.

A LGPD é uma legislação brasileira que entrou em vigor em 2020, e a British Airways é uma empresa do Reino Unido. Portanto, a LGPD não se aplica diretamente ao caso da British Airways. No entanto, é importante observar que a LGPD estabelece

princípios e diretrizes para a proteção de dados pessoais no Brasil, buscando garantir a privacidade e a segurança das informações dos indivíduos. Embora a LGPD seja específica para o Brasil, muitos países têm leis semelhantes que visam proteger os dados pessoais dos cidadãos.

No caso da British Airways, foram acionadas as regulamentações de proteção de dados vigentes no Reino Unido e na União Europeia, como o Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês), que é uma legislação abrangente que se aplica a empresas que processam dados de cidadãos da UE.

O GDPR compartilha muitos princípios semelhantes à LGPD, incluindo a necessidade de obter consentimento adequado para o processamento de dados pessoais, a adoção de medidas de segurança para proteção dos dados e a obrigação de notificar as autoridades competentes e os indivíduos afetados em caso de violação de dados.
Portanto, embora o caso da British Airways não esteja diretamente relacionado à LGPD, ele está relacionado às questões mais amplas de proteção de dados e privacidade, nas quais várias legislações, como a LGPD e o GDPR, buscam abordar.

Facebook / Cambridge Analytica

Em 2018, veio à tona um escândalo envolvendo a empresa de consultoria política Cambridge Analytica e o Facebook. A empresa coletou dados pessoais de aproximadamente 87 milhões de usuários do Facebook sem o consentimento adequado. Os dados foram obtidos por meio de um aplicativo de teste de personalidade chamado "This Is Your Digital Life", que foi instalado por cerca de 270.000 pessoas, mas também acessou dados dos amigos desses usuários sem seu conhecimento.

A Cambridge Analytica usou esses dados para criar perfis psicográficos e direcionar mensagens personalizadas para influenciar eleições e campanhas políticas, incluindo a eleição presidencial dos Estados Unidos em 2016. O caso gerou preocupações significativas em relação à privacidade e à manipulação de dados em massa, levando a um amplo debate sobre a regulamentação e a proteção dos dados pessoais.

> "A Cambridge Analytica teria comprado acesso a informações pessoais de usuários do Facebook e usado esses dados para criar um sistema que permitiu predizer e influenciar as escolhas dos eleitores nas urnas, segundo a investigação dos jornais The Guardian e The New York Times."[...] (BBC NEWS, 2018).

O caso não está diretamente relacionado à LGPD, pois a Cambridge Analytica é uma empresa de consultoria política sediada no Reino Unido e o incidente ocorreu antes da entrada em vigor da LGPD em 2020. No entanto, é importante destacar que o caso teve um impacto significativo no debate global sobre a proteção de dados pessoais e a necessidade de regulamentação nessa área. O escândalo revelou as vulnerabilidades e os abusos relacionados à coleta e ao uso indevido de dados pessoais de usuários do Facebook.

A LGPD, por sua vez, é uma legislação brasileira que busca proteger a privacidade e os direitos dos indivíduos em relação aos seus dados pessoais. Embora a LGPD não tenha sido diretamente aplicada no caso Cambridge Analytica, ela compartilha objetivos semelhantes aos esforços internacionais para proteger a privacidade dos dados e o controle dos indivíduos sobre suas informações pessoais. Apesar de não estar diretamente relacionado ao caso Cambridge Analytica, esse incidente reforçou a importância de leis de proteção de dados, como a LGPD, para garantir a privacidade dos indivíduos e regular as práticas de coleta e uso de dados pessoais pelas empresas.

Uber

Em 2016, foi revelado que a empresa de transporte Uber sofreu um vazamento massivo de dados que ocorreu em 2014. Os dados de aproximadamente 57 milhões de usuários e motoristas da Uber em todo o mundo foram comprometidos, incluindo nomes, endereços de e-mail, números de telefone e, em alguns casos, informações de carteira de motorista.

O vazamento ocorreu devido a uma violação dos sistemas de segurança da Uber, que permitiu que os hackers acessassem e baixassem as informações dos usuários. Além disso, a Uber foi criticada por não revelar o incidente imediatamente, ocultando o

vazamento por mais de um ano. O caso resultou em multas e ações legais em vários países, incluindo o Brasil, onde a LGPD entrou em vigor posteriormente.

No Brasil, a Uber revelou que dados pessoais de aproximadamente 196 mil usuários brasileiros foram acessados por hackers durante o incidente. As informações comprometidas incluíam nomes completos, endereços de email, números de telefone e informações relacionadas a viagens.

Após a descoberta do incidente, a Uber notificou as autoridades competentes e os usuários afetados no Brasil, em conformidade com as obrigações previstas na LGPD. A empresa também informou sobre a violação por meio de comunicados públicos, demonstrando transparência sobre o ocorrido.

A Autoridade Nacional de Proteção de Dados (ANPD) do Brasil iniciou uma investigação sobre o incidente da Uber à luz da LGPD. Em agosto de 2021, a ANPD aplicou uma multa de R$1,5 milhão à Uber por violações à proteção de dados, considerando o tempo de resposta ao incidente, a comunicação aos usuários afetados e a implementação de medidas de segurança após a violação.

Além da multa, a Uber foi instruída pela ANPD a adotar medidas para aprimorar a segurança e proteção dos dados pessoais dos usuários, implementando melhores práticas de governança e conformidade com a LGPD.

Esse caso envolvendo a Uber destaca a aplicação da LGPD em um incidente de vazamento de dados pessoais. A empresa foi responsabilizada pela violação, notificou as autoridades e os usuários afetados, e recebeu uma sanção da ANPD. Essas ações demonstram como a LGPD busca proteger os direitos dos indivíduos e garantir a segurança e a privacidade dos dados pessoais no Brasil.

Equifax

O vazamento de dados da Equifax, ocorrido em 2017, foi um dos maiores incidentes de violação de dados já registrados, resultando na exposição de informações pessoais confidenciais de milhões de consumidores nos Estados Unidos. O caso comprometeu dados pessoais de aproximadamente 147 milhões de consumidores. Essas

informações incluíam nomes completos, números de Seguro Social, datas de nascimento, endereços residenciais e, em alguns casos, números de cartões de crédito.

Os hackers aproveitaram uma vulnerabilidade em um aplicativo de software utilizado pela Equifax. Essa falha de segurança permitiu que eles obtivessem acesso não autorizado aos sistemas da empresa, expondo uma quantidade massiva de dados pessoais. O vazamento ocorreu entre maio e julho de 2017. No entanto, a Equifax só tornou o incidente público em setembro de 2017, meses após a violação ter ocorrido. Esse atraso na divulgação gerou críticas significativas à empresa por não agir prontamente para proteger os dados e informar os consumidores afetados.

O vazamento de dados da Equifax teve repercussões graves. Além do comprometimento das informações pessoais de milhões de consumidores, o incidente levou a um aumento no risco de fraudes, roubo de identidade e ataques cibernéticos direcionados. Os consumidores afetados enfrentaram a necessidade de monitorar suas contas e históricos de crédito, enquanto a Equifax enfrentou múltiplas ações judiciais, investigações regulatórias e multas significativas.

O caso de vazamento de dados pode ser relacionado aos princípios e à apropriação indevida de dados pessoais tratados pela LGPD. Embora a LGPD não tenha sido diretamente aplicada no caso da Equifax, ela compartilha objetivos semelhantes de proteção de dados pessoais e privacidade.

A LGPD estabelece que o tratamento de dados pessoais requer o consentimento adequado dos titulares dos dados. No caso da Equifax, os dados pessoais dos consumidores foram coletados e tratados sem o consentimento explícito desses indivíduos, o que pode ser considerado uma apropriação indevida de dados pessoais. A Lei também impõe a responsabilidade às empresas de adotar medidas de segurança para proteger os dados pessoais que possuem. Com a Equifax, a violação ocorreu devido a uma falha de segurança, o que pode ser interpretado como uma falha em cumprir essa obrigação de proteção dos dados pessoais. Outra exigência é que as empresas notifiquem os indivíduos e as autoridades competentes em caso de violação de dados. A Equifax, com o atraso na comunicação e divulgação pública do vazamento levantou preocupações sobre a falta de transparência e a demora em informar os consumidores afetados sobre a violação e seus potenciais riscos.

A Lei Geral de Proteção de Dados prevê sanções e penalidades para empresas que não cumprem suas obrigações em relação à proteção de dados pessoais. No contexto da empresa Equifax, as consequências legais e financeiras incluíram ações judiciais, investigações regulatórias e multas significativas.

Embora esse cenário não esteja diretamente ligado à LGPD, ele destaca a importância dos princípios de consentimento, segurança, transparência e responsabilização presentes na LGPD. Esses princípios visam prevenir a apropriação indevida de dados pessoais e garantir que os titulares dos dados tenham controle sobre suas informações, além de responsabilizar as empresas por violações de segurança e proteção de dados.

RESULTADOS E DISCUSSÕES

Caso Uber

Este caso envolveu um vazamento massivo de dados pessoais da empresa de transporte Uber, ocorrido em 2014, mas revelado apenas em 2016. Cerca de 57 milhões de usuários e motoristas da Uber tiveram suas informações comprometidas, incluindo nomes, endereços de e-mail, números de telefone e, em alguns casos, informações de carteira de motorista.

A LGPD FOI IMPLEMENTADA:

A Uber comunicou oficialmente as autoridades e os usuários afetados no Brasil, conforme exigido pela LGPD. A empresa também divulgou a violação em comunicados públicos, demonstrando transparência. A Autoridade Nacional de Proteção de Dados (ANPD) do Brasil está investigando o incidente da Uber à luz da LGPD. Em agosto de 2021, a ANPD impôs uma multa de R$1,5 milhão à Uber por violações à proteção de dados, considerando o tempo de resposta, a comunicação aos usuários afetados e a implementação de medidas de segurança. Além da multa, a ANPD instruiu a Uber a reforçar a segurança e a proteção dos dados pessoais dos usuários, implementando melhores práticas de governança e conformidade com a LGPD.

•

A Lei Geral de Proteção de Dados (LGPD) representa um marco crucial no Brasil em relação à segurança cibernética e à proteção da privacidade dos cidadãos. Desde sua implementação, a LGPD tem sido uma ferramenta fundamental para garantir a integridade e a segurança dos dados pessoais em um ambiente digital em constante evolução.

Outros inúmeros casos exemplificam a aplicação efetiva da LGPD em território brasileiro, destacando seu papel na garantia de uma proteção robusta dos dados e no estabelecimento de responsabilidade por parte das organizações. Empresas de diversos setores têm sido chamadas à responsabilidade, enfrentando penalidades significativas

por violações à proteção de dados. Esses casos variam em sua natureza, abrangendo desde vazamentos massivos de informações pessoais até o uso indevido de dados sem consentimento explícito. Em todos esses cenários, a Lei mostrou sua relevância ao impor penalidades proporcionais à gravidade da violação, estimulando uma cultura de conformidade e segurança cibernética.

A LGPD não apenas assegura a privacidade dos indivíduos, mas também promove a transparência nas práticas de tratamento de dados. Empresas são obrigadas a informar claramente como os dados são utilizados e a obter consentimento adequado. A lei impõe a necessidade de medidas de segurança robustas, garantindo que as organizações protejam os dados dos cidadãos de forma eficaz contra ameaças cibernéticas.

Além disso, ela incentiva a rápida notificação de violações de dados, permitindo uma resposta mais eficaz e a proteção imediata dos indivíduos afetados. Essa abordagem proativa é essencial para minimizar danos e garantir que os indivíduos possam tomar medidas para proteger suas informações.

Em síntese, a LGPD é uma ferramenta vital que fortalece a segurança cibernética e a proteção da privacidade no Brasil. Sua aplicação efetiva não apenas protege os dados pessoais, mas também contribui para um ambiente digital mais seguro e responsável, beneficiando tanto as organizações quanto os cidadãos.

•

Ao analisarmos casos ocorridos em outros países, destacam-se incidentes marcantes de violações de dados, já mencionados e detalhados anteriormente, que resultaram na exposição em larga escala de informações pessoais sensíveis. Estes casos envolveram grandes empresas e instituições, onde dados críticos foram comprometidos, colocando em risco a privacidade e a segurança de milhões de indivíduos.

Em um desses casos, uma violação de segurança significativa levou à exposição massiva de dados pessoais de consumidores. As informações vazadas incluíam nomes, números de identificação, endereços e, em alguns casos, detalhes financeiros. Essa

situação gerou uma série de problemas, desde riscos de fraudes até a necessidade de monitoramento constante das contas dos afetados.

Em outro cenário, uma empresa foi alvo de uma violação de seus sistemas de segurança, resultando na obtenção não autorizada de dados de usuários. Essa exposição comprometeu informações confidenciais, como nomes completos, datas de nascimento e detalhes de identificação. A divulgação tardia da violação gerou críticas sobre a falta de prontidão da empresa em proteger os dados e informar os afetados.

É relevante considerar como a aplicação da Lei Geral de Proteção de Dados (LGPD) poderia ter influenciado esses casos. A LGPD, com seus princípios de consentimento, segurança, transparência e responsabilização, busca proteger a privacidade e os direitos dos indivíduos em relação aos seus dados pessoais. Caso estivesse em vigor durante esses incidentes, a LGPD teria exigido a notificação imediata das autoridades e dos afetados, bem como a obtenção prévia de consentimento para o tratamento dos dados. Além disso, a imposição de medidas de segurança robustas seria mandatória para garantir a proteção dos dados pessoais.

Esses casos ressaltam a importância das leis de proteção de dados e evidenciam a necessidade de regulamentações como a LGPD para prevenir a apropriação indevida de dados pessoais e garantir a responsabilidade das empresas diante de violações de segurança e proteção de dados.

CONSIDERAÇÕES FINAIS

Diante da análise aprofundada dos casos de violação de dados e da contextualização da Lei Geral de Proteção de Dados (LGPD), torna-se evidente a necessidade imperativa de salvaguardar os dados pessoais dos indivíduos em um mundo digital interconectado. Os eventos de vazamentos massivos de informações e a exploração indevida de dados sensíveis demonstram as vulnerabilidades presentes na atual infraestrutura digital e a urgência em estabelecer medidas eficazes para sua proteção.

A LGPD se destaca como uma legislação progressiva, introduzindo princípios sólidos que visam à proteção dos direitos dos indivíduos sobre suas informações pessoais. Ao requerer o consentimento explícito para o tratamento de dados e ao impor responsabilidades claras às organizações, a LGPD estabelece um novo padrão para a gestão de dados pessoais, alinhado com as melhores práticas globais.

A aplicação da LGPD em casos concretos evidencia sua eficácia e relevância na proteção dos cidadãos brasileiros. As penalidades substanciais aplicadas a empresas por violações à segurança de dados não só servem como uma dissuasão eficaz, mas também demonstram o compromisso em garantir a conformidade e a proteção efetiva dos dados pessoais. Contudo, é crucial ressaltar que a segurança cibernética é um campo dinâmico, sujeito a constantes evoluções tecnológicas e estratégicas. À medida que novas ameaças emergem, a legislação deve continuar sendo adaptada para enfrentar os desafios contemporâneos e futuros de forma eficaz.

Portanto, insta-se à contínua revisão e aprimoramento da LGPD, sempre em consonância com as necessidades da sociedade e as tendências tecnológicas. A educação e conscientização sobre os direitos de privacidade e a importância da segurança dos dados devem ser fomentadas, promovendo uma sociedade digital mais informada e protegida.

Em síntese, a Lei Geral de Proteção de Dados representa um passo significativo rumo à proteção da privacidade e segurança cibernética, mas requer um compromisso coletivo para garantir sua eficácia contínua e a proteção dos cidadãos em um mundo digital em constante transformação.

REFERÊNCIAS BIBLIOGRÁFICAS

LIMA RAPÔSO, C. F.; MELO DE LIMA, H.; DE OLIVEIRA JUNIOR, W. F.; FERREIRA SILVA, P. A. .; ELAINE DE SOUZA BARROS, E. . LGPD - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM TECNOLOGIA DA INFORMAÇÃO: Revisão Sistemática. RACE **- Revista de Administração do Cesmac,** [S. l.], v. 4, p. 58–67, 2019. DOI: 10.3131/race.v4i0.1035. Disponível em: <https://revistas.cesmac.edu.br/administracao/article/view/1035 > . Acesso em: 21 jun. 2023.

VIEIRA, V. R. N. **Lei Geral de Proteção de Dados:**Uma análise da tutela dos dados pessoais em casos de transferência internacional. 2019. 77 f. Trabalho de Conclusão de Curso (Graduação em Direito) –Universidade Federal de Uberlândia, Uberlândia, 2019. Disponível em: <https://repositorio.ufu.br/handle/123456789/26233 > Acesso em: 09 set. 2023.

AGOSTINELLI, Joice. **A importância da lei geral de proteção de dados pessoais no ambiente online. Etic-encontro de iniciação científica**-ISSN 21-76-8498, v. 14, n. 14, 2018. Disponível em: <http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7025 > Acesso em: 09 set. 2023.

Brasil. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm >. Acesso em: 14 ago. 2023.

G1 ECONOMIA. **British Airways é multada em US$ 230 milhões por caso de roubo de dados de passageiros.** Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/07/08/british-airways-e-multada-em-us-230-milhoes-por-caso-de-roubo-de-dados-de-passageiros.ghtml> Acesso em: 09 jun. 2023.

JORNAL JURID. **Caso de vazamento de dados da British Airways é resolvido em termos confidenciais.** Disponível em: <https://www.jornaljurid.com.br/noticias/caso-de-vazamento-de-dados-da-british-airways-e-resolvido-em-termos-confidenciais> Acesso em: 09 jun. 2023.

TECMUNDO. **British Airways vaza dados e é multada em R$ 145 milhões.** Disponível em: <https://www.tecmundo.com.br/seguranca/205363-british-airways-vaza-dados-multada-r-145-milhoes.htm> Acesso em: 09 jun. 2023.

BBC NEWS BRASIL. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades.** Disponível em: <https://www.bbc.com/portuguese/internacional-43461751 > Acesso em: 10 jun. 2023.

G1 ECONOMIA. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades.** Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml> Acesso em: 10 jun. 2023.

CNN BRASIL. **Meta faz acordo de US$ 725 milhões para encerrar caso sobre Cambridge Analytica.** Disponível em: < https://www.cnnbrasil.com.br/economia/meta-faz-acordo-de-us-725-milhoes-para-encerrar-caso-sobre-cambridge-analytica/ > Acesso em: 10 jun. 2023.

O GLOBO ECONOMIA. **Vazamento de dados da Uber em 2016 afetou 196 mil brasileiros.** Disponível em: < https://oglobo.globo.com/economia/vazamento-de-dados-da-uber-em-2016-afetou-196-mil-brasileiros-22584512 > Acesso em: 10 jun. 2023.

CANALTECH. **Uber sofre vazamento de dados internos em ataque cibernético.** Disponível em: <https://canaltech.com.br/seguranca/uber-sofre-vazamento-de-dados-internos-em-ataque-cibernetico-225474/ > Acesso em: 10 jun. 2023.

TECMUNDO. **Uber admite ter escondido vazamento de dados de 57 milhões de usuários**. Disponível em: <https://www.tecmundo.com.br/seguranca/242206-uber-admite-ter-escondido-vazamento-dados-57-milhoes-de-usuarios.htm > Acesso em: 10 jun. 2023.

G1 ECONOMIA. **Equifax faz acordo para pagar R$ 2,6 bi por vazamento de dados de clientes nos EUA.** Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/07/22/equifax-faz-acordo-para-pagar-r-26-bi-por-vazamento-de-dados-de-clientes-nos-eua.ghtml > Acesso em: 11 jun. 2023.

EXAME. **Equifax pagará até US$ 700 milhões por vazamento de dados pessoais.** Disponível em: <https://exame.com/negocios/equifax-pagara-ate-us-700-milhoes-por-vazamento-de-dados-pessoais/ > Acesso em: 11 jun. 2023.