Compliance e proteção de dados: estudo comparado das leis de proteção de dados do Brasil, da União Europeia e da China

Rafael Coelho Camacho, Direito, Faculdade Integrado, Brasil, rcamachocm@gmail.com

Dânia Vanessa de Mello, Direito, Faculdade Integrado, Brasil, mello@grupointegrado.br

RESUMO: Este artigo realiza uma análise comparativa entre três das principais legislações de proteção de dados pessoais em vigor no cenário global: a Lei Geral de Proteção de Dados (LGPD) do Brasil, o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia e a Lei de Proteção de Informações Pessoais (PIPL) da China. Essas regulamentações têm como objetivo garantir a privacidade e a segurança das informações pessoais, mas apresentam abordagens e exigências distintas, refletindo as particularidades culturais e jurídicas de cada região. O estudo destaca as semelhanças e diferenças fundamentais entre as legislações, como os direitos dos titulares de dados, os requisitos de consentimento e as obrigações das empresas em termos de transparência e segurança. Além disso, são analisadas as implicações dessas leis nas práticas de compliance das empresas, com foco nos desafios enfrentados ao tentar cumprir com diferentes normas em um ambiente globalizado. Para ilustrar esses desafios, são apresentados três estudos de caso, cada um exemplificando a aplicação prática de uma dessas regulamentações em empresas de diferentes setores. A análise fornece uma visão abrangente sobre as questões de governança de dados pessoais e como as empresas podem se adaptar a essas complexas exigências legais.

Palavra Chave: Proteção de Dados. Compliance. Privacidade. Segurança da Informação. Leis de Proteção de Dados.

Abstract: This article provides a comparative analysis of three major data protection regulations in effect worldwide: Brazil's General Data Protection Law (LGPD), the European Union's General Data Protection Regulation (GDPR), and China's Personal Information Protection Law (PIPL). These regulations aim to ensure the privacy and security of personal information but present distinct approaches and requirements, reflecting the cultural and legal peculiarities of each region. The study highlights the key similarities and differences between the regulations, such as the rights of data subjects, consent requirements, and the obligations of companies regarding transparency and security. Furthermore, the implications of these laws on corporate compliance practices are analyzed, focusing on the challenges faced when attempting to comply with different standards in a globalized environment. To illustrate these challenges, three case studies are presented, each showcasing the practical application of one of these regulations in companies from various sectors. The analysis offers a comprehensive view of personal data governance issues and how companies can adapt to these complex legal requirements.

Keywords: Data Protection. Compliance. Privacy. Information Security. Data Protection Laws.

INTRODUÇÃO

A proteção de dados pessoais emergiu como uma questão central em um mundo cada vez mais digital e interconectado. À medida que a tecnologia avança e as empresas expandem suas operações globalmente, o tratamento e a segurança das informações pessoais tornam-se questões cruciais para garantir a confiança dos consumidores e o cumprimento das normas regulatórias. As preocupações com a privacidade e a proteção de dados são especialmente intensificadas por uma crescente incidência de vazamentos e abusos de informações sensíveis, o que tem gerado um aumento nas demandas por legislações rigorosas em todo o mundo. Nesse contexto, diversas regulamentações têm sido implementadas para proteger os dados dos cidadãos, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, e a Lei de Proteção de Informação Pessoal (PIPL) na China. Este artigo tem como objetivo comparar essas três regulamentações, analisando suas principais semelhanças e diferenças, bem como as implicações de cada uma para as práticas de compliance corporativo. A análise busca identificar os desafios enfrentados pelas empresas ao lidar com diferentes regimes legais e como essas regulamentações impactam a conformidade e a governança de dados nas organizações.

MÉTODO

Este artigo adota o método do estudo comparado para analisar três importantes regulamentações de proteção de dados: a Lei Geral de Proteção de Dados (LGPD) do Brasil, o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia e a Lei de Proteção de Informações Pessoais (PIPL) da China. O estudo comparativo busca identificar as semelhanças e diferenças entre essas legislações, considerando seus contextos culturais, econômicos e jurídicos. Ao contrastar as disposições legais de cada sistema, este método permite uma análise mais profunda das implicações práticas para as empresas no que diz respeito à conformidade regulatória e às práticas de governança de dados.

Além disso, o artigo faz uso do método dedutivo para examinar como princípios gerais de proteção de dados. A partir de premissas amplas sobre a proteção da privacidade e os requisitos de compliance, são deduzidas conclusões práticas que ajudam a entender os desafios enfrentados pelas empresas ao implementar as regulamentações em diferentes cenários. Dessa forma, o estudo parte de conceitos universais sobre a proteção de dados e, por meio de análise dedutiva, aplica esses conceitos às situações concretas apresentadas nos estudos de caso.

Para complementar essa análise, três estudos de caso são apresentados, ilustrando a aplicação prática de cada legislação em diferentes cenários empresariais e os desafios enfrentados na implementação de medidas de compliance em distintas jurisdições.

RESULTADO E DISCUSSÃO

1 CONTEXTO HISTÓRICO LEGAL

Apesar de ser um assunto atual e com aspecto de modernidade, o tratamento de dados já vem sendo estudado e aplicado há décadas. Porém, assim como ocorre em todas as áreas da legislação, as adaptações são necessárias para enfrentar novos problemas que surgem.

A construção jurídica da proteção de dados tem grande influência de movimentos europeus, iniciados pela Alemanha e seguido pela França, que em 1970 sofriam forte intervenção estatal na vida privada dos cidadãos, por sua vez os civis se movimentavam, pois, estavam fartos de governos totalitários causado pelo sentimento pós guerra mundial(OECD, 2013).

Mas foi em 1980 que o assunto chegou no âmbito internacional, onde a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) adotou as Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, vigente até os dias de hoje. Esse documento, sem caráter vinculativo, estabeleceu princípios para guiar o tratamento de dados pessoais e inspirou diversos textos legais pelo mundo(OECD, 2013).

No ano seguinte, em 1981, o Conselho da Europa, por meio da Convenção 108, com possibilidade de adesão de países europeus e não europeus, afirmou que a proteção à privacidade e aos dados pessoais são fundamentais para a manutenção dos direitos do homem. Foi o primeiro texto legal internacional com caráter vinculante. Até o ano de 2023 contava com 55 países assinantes, sendo 9 não europeus, um destes o Brasil (COUNCIL OF EUROPE, 1981).

Anos depois, por meio da Diretiva 95/46/CE da União Europeia (1995), apareceu a primeira regulamentação sobre os tratamentos dos dados pessoais e a livre circulação destes. Mas, apenas no ano 2000 que a União Europeia realmente reconheceu o caráter de direito fundamental da proteção de dados pessoais, por meio do artigo 8 da Carta de Direitos Fundamentais da União Europeia, integralizando a Diretiva ao sistema jurídico de cada Estado membro da União Europeia(União Europeia, 2000).

Por muito tempo, a Diretiva foi tratada como o principal texto regulador do tema na União Europeia, sendo substituída em 2018 pelo atual Regulamento Geral de Proteção de Dados (GDPR) da União Europeia (União Europeia, 2016).

Com início dos movimentos europeus, a chegada do século XXI até os dias atuais, está sendo marcadas pela adoção mundial de legislações relacionadas ao tema, Segundo o mapa mundial das legislações de dados ao redor do mundo, disponibilizado pela Conferência das Nações Unidas Sobre Comércio e Desenvolvimento (UNCTAD), 71% dos países já possuíam legislação, 9% estavam em desenvolvimento, 15% ainda não tratam do assunto, e 5% não possuem dados(UNCTAD, 2024).

Embora o Brasil tenha assinado a Convenção 108 apenas no dia 8 de outubro de 2021, a Constituição Federal, em seu artigo 5º, já garantia o direito

fundamental à intimidade, vida privada, honra e imagem desde sua promulgação em 1988 (Brasil, 1988).

No sentido de firmar esse direito, algumas leis foram precursoras no sistema jurídico brasileiro. Uma delas é o Código de Defesa do Consumidor (Lei nº 8.078/1990), que implementou defesas de informação pessoal em seção sobre cadastro e banco de dados, garantindo o direito à correção (Brasil, 1990). Outra lei importante foi a Lei nº 9.296 de 1996, que tornou inviolável o sigilo de correspondência, comunicações telegráficas, de dados e das comunicações telefônicas, salvo por ordem judicial (Brasil, 1996).

No ano de 2013, uma importante movimentação legislativa acontecia no Brasil, gerando a implementação do Marco Civil da Internet (Lei nº 12.965/2014), onde foram introduzidos conceitos de liberdade de expressão e responsabilidade de empresas e usuários no ambiente digital (Brasil, 2014).

E, finalmente, em 2018, foi sancionada a Lei Federal nº 13.709, que entrou em vigor em 2020, conhecida como a Lei Geral de Proteção de Dados do Brasil (LGPD), surgindo em resposta à crescente demanda global por regulamentação de dados pessoais (Brasil, 2018).

Inspirada principalmente pela Europa, a Lei Geral de Proteção de Dados brasileira visa proteger os direitos dos cidadãos no que diz respeito ao tratamento de seus dados pessoais. A lei impõe obrigações às empresas que processam esses dados, exigindo, entre outras coisas, o consentimento explícito para certas atividades de processamento.

Já no continente asiático, com a inserção da China no mercado global e a recente era capitalista, fez o país superar problemas de terceiro mundo e avançar no setor tecnológico, esse grande crescimento veio acompanhado da necessidade de se adequar aos parâmetros internacionais sem afetar sua própria soberania(Zhang, 2004).

A criação da Lei de Proteção de Informações Pessoais (PIPL) da China é mais recente, aprovada em novembro de 2021, e marca o esforço da China para regular de forma abrangente o uso de dados pessoais e se firmar no mundo globalizado.

Importante mencionar que o avanço do tema na China segue uma linha de aplicação de controle, moldando algumas políticas de censura, como no caso do Great Firewall que tem o objetivo de bloquear o acesso a sites estrangeiros selecionados e diminuir o tráfego de internet transnacional, ao mesmo tempo em que tenta avançar internacionalmente sua própria tecnologia como o caso da Huawei, Xiaomi, BYD, TikTok entre outros (Gisonna, 2024).

Portanto, embora a PIPL se inspire em regulamentações estrangeiras, como o GDPR, também reflete as necessidades internas do país, como o foco no controle estatal e na proteção da soberania digital.

Cada uma dessas leis foi motivada por fatores distintos. Enquanto a Europa teve forte influência histórica e global, incluindo a própria criação da Lei brasileira, esta também é fruto de vários fatores internos que personalizam a norma, já a China reflete uma abordagem um pouco diferente, combinando proteção de dados com controle governamental. As influências culturais e

jurídicas de cada região se refletem nas diferenças específicas de cada legislação.

2 A NECESSIDADE DE COMPLIANCE

Como se depreende do tópico acima, estar dentro das normas no mundo empresarial é de total importância, não apenas na área de proteção de dados, mas diversas outras como segurança do trabalho e gestão de risco. Razão pela qual cada caso empresarial deve ter seu programa de Compliance estudado separadamente, evitando problemas futuros que podem comprometer a vida da empresa.

Para claro entendimento, o Programa de Compliance é um conjunto de práticas adotadas por uma organização para garantir que suas atividades estejam em conformidade com as leis, regulamentos, normas e políticas internas aplicáveis.

O termo vem do inglês "to comply", que significa "cumprir" ou "estar em conformidade". O objetivo principal de Compliance é assegurar que a empresa ou instituição atue de maneira ética, transparente e dentro dos parâmetros legais, evitando riscos legais, financeiros e de reputação.

Com a crescente necessidade das empresas se adequarem ao cenário atual, a área de Compliance se tornou algo essencial no corpo das grandes companhias, com a função de criar um conjunto de práticas que devem ser adotadas para garantir que as operações estejam em conformidade com as regulações legais, evitando multas e sanções, protegendo o direito das pessoas, mitigando os riscos operacionais entre outros benefícios(Rakha, 2023).

Como é o caso da Volkswagen após o escândalo do "Dieselgate" em 2015, situação em que resultados de testes de emissão de carbono eram fraudados, a Volkswagen reformulou profundamente sua área de compliance, introduzindo um programa global para garantir conformidade com normas ambientais, regulatórias e éticas. A empresa passou a adotar um código de conduta rígido e reforçou seus controles internos para evitar manipulações e fraudes (BBC, 2015).

O compliance em proteção de dados não é apenas uma exigência legal, mas uma estratégia essencial para o sucesso e a sustentabilidade das empresas no cenário global. Ele garante a conformidade com as diversas legislações internacionais, protege os direitos dos indivíduos e promove a segurança operacional, ao mesmo tempo em que fortalece a reputação e a competitividade no mercado global (Kuner, 2017).

Analisar a similaridade e diferença entre as legislações de proteção de dados entre blocos distintos é fundamental para entender como seguem e seguirão na regulação dos tratamentos de dados e garantir a conformidade legal em contexto internacional. Isso tem impacto direto na operação de empresas multinacionais, para os direitos dos cidadãos e no desenvolvimento de políticas globais sobre o tema.

3 AS PRINCIPAIS SEMELHANÇAS ENTRE AS NORMAS

Estudar a semelhança entre as legislações é tão importante quanto estudar as diferenças, podendo se estabelecer uma base comum e concreta para empresas e governos aplicarem em casos específicos, podendo simplificar o processo garantindo celeridade, economia de recursos, conformidade internacional com possibilidade de atuação em várias regiões globais e melhorando a cooperação internacional.

Uma das semelhanças entre as legislações está na garantia de direitos essenciais aos indivíduos, incluindo o direito de acesso de sua informação, correção, exclusão e portabilidade dos dados. Essas proteções visam empoderar os cidadãos, proporcionando maior controle sobre suas informações pessoais, embora não sejam direitos absolutos.

Essas similaridades estão descritas nos próprios regulamentos da União Europeia, especificamente nos artigos 15 a 22 do Regulamento (UE) 2016/679, que cobrem os direitos dos titulares, como acesso, retificação, apagamento ("direito ao esquecimento"), portabilidade e objeção ao tratamento (União Europeia, 2016).

A Lei Brasileira (Lei nº 13.709, de 14 de agosto de 2018) em seu artigo 18, por exemplo, garante aos titulares dos dados os direitos de acesso, correção, eliminação e oposição ao tratamento, entre outros (Brasil, 2018).

Já a Lei Chinesa (Lei nº 13.709, de 14 de agosto de 2018) estabelece nos artigos 44 a 49 direitos semelhantes para os titulares dos dados, tais como o direito à correção, exclusão e oposição ao tratamento (China, 2021).

Lembrando que nas três leis os direitos não são absolutos, cedendo perante direitos de liberdade de expressão e de informação, quando o tratamento dos dados decorre de uma obrigação de Direito da União ou de um Estado-Membro, por motivos de interesse público, ou quando o tratamento dos dados é relevante no âmbito de um processo judicial(União Europeia, 2016; Brasil, 2018; China, 2021).

Outra semelhança das normas que deve ser destacada está nas bases legais para tratamento de dados, estabelecendo requisitos legais claros para a autorização desse tratamento, podendo ser o consentimento da pessoa, execução de contratos, interesse público e outros. Embora existam estas similaridades, as abordagens específicas de cada legislação podem variar dependendo do contexto.

Por exemplo, no Brasil, o artigo 7 da Lei nº 13.709/2018 define as bases legais para o tratamento de dados pessoais, como consentimento, cumprimento de obrigação legal, execução de contrato, exercício regular de direitos e legítimo interesse (Brasil, 2018).

Já na União Europeia, no artigo 6 do Regulamento 2016/679, e na China, no artigo 13 da Lei de Proteção de Informações Pessoais, ambos mantêm a redação e acrescentam interesses vitais, interesse público ou exercício de autoridade oficial, entre outros (União Europeia, 2016; China, 2021)

Outra paridade entre as normas é encontrada em um tema muito relevante na proteção aos dados, que são as Responsabilidades dos Controladores e

Processadores, as três regulamentações impõem fortes responsabilidades sobre eles, especialmente no que tange à segurança e à proteção contra violações.

O Brasil e a União Europeia tratam da responsabilidade do controlador de manter registros das operações, além da obrigatoriedade de nomeação de encarregado de proteção de dados, o Data Protection Officer (DPO) (União Europeia, 2016; Brasil, 2018).

A Lei de Proteção de Informações Pessoais da China também detalha as obrigações de controladores e processadores, incluindo a nomeação de um responsável pela proteção de dados e a necessidade específica de análise de órgãos governamentais correspondentes a cada situação (China, 2021).

As diferenças provenientes desse tema também são muito relevantes e serão tratadas no tópico correspondente.

As normas reguladoras de proteção de dados do Brasil, da União Europeia e da China compartilham a responsabilidade de atribuir a supervisão das operações de tratamento de dados a uma figura legalmente designada, como o encarregado de proteção de dados (DPO) (União Europeia, 2016; Brasil, 2018; China, 2021). A personificação dessas responsabilidades demonstra que as normas seguem a responsabilização direta de uma pessoa ou equipe específica para as aplicações legais.

Mesmo que as normas determinem a personificação de um responsável sobre as operações, elas ainda acrescentam as Autoridades de Supervisão. Cada jurisdição possui uma autoridade responsável pela supervisão e aplicação das leis de proteção de dados. Essas autoridades possuem amplos poderes para fiscalizar, investigar e sancionar violações, embora a independência e o alcance desses poderes variem.

No Brasil, a Lei define a Autoridade Nacional de Proteção de Dados (ANPD) como a entidade responsável pela fiscalização, regulação e aplicação de sanções referentes à proteção de dados no Brasil (Brasil, 2018).

A União Europeia estabelece as Autoridades de Proteção de Dados em cada Estado-Membro da União Europeia, com poderes de monitoramento, investigação e aplicação de sanções (União Europeia, 2016). Cada país da União Europeia possui uma autoridade independente, como o ICO no Reino Unido ou o CNIL na França (Reino Unido, 2024; França, 2024).

A China designa as autoridades responsáveis pela supervisão e aplicação da norma, como a Administração do Ciberespaço da China (CAC), que tem poderes de fiscalização, regulação e imposição de penalidades em caso de violações (China, 2021).

Dessa forma pode se concluir que as semelhanças entre as normas demonstram uma tendência global de convergência em relação à proteção de dados pessoais, estabelecendo princípios comuns que facilitam a conformidade para empresas que operam em diversas jurisdições.

Esses pontos em comum, como os direitos dos titulares de dados, as bases legais para o tratamento e a exigência de nomeação de um responsável pela proteção de dados, mostram que, apesar das diferenças culturais e

regulatórias, as três legislações têm como objetivo central garantir a segurança, privacidade e transparência no tratamento de dados.

Isso contribui para o fortalecimento da cooperação internacional e para a criação de padrões globais mais robustos na proteção de dados.

4 AS PRINCIPAIS DIFERENÇAS ENTRE AS NORMAS

Em um mundo onde a proteção de dados é cada vez mais relevante e as comunicações evoluem rapidamente, é crucial que empresas, governos e cidadãos estejam atentos às nuances das regulamentações para garantir a segurança e privacidade das informações, evitando sanções legais e danos à reputação(Rakha, 2023).

Estudar as diferenças entre as legislações de proteção de dados, como a brasileira LGPD (Lei Geral de Proteção de Dados n° 13.709/2018) (Brasil, 2018), a europeia GDPR (General Data Protection Regulation - Regulamento (UE) 2016/679) (União Europeia, 2016) e a chinesa PIPL (Personal Information Protection Law) (China, 2021), é fundamental por diversas razões, sejam elas adaptação às exigências locais, mitigação de riscos legais, desenvolvimento de estratégia de compliance, acompanhamento de mudanças regulatórias, entre outras.

Com o avanço da tecnologia, surgem novas ameaças, como fraudes e ciberataques, e leis como essas exigem que as empresas adotem medidas proativas de conformidade. Isso não apenas previne multas, mas também fortalece a confiança com clientes e parceiros, promovendo uma cultura de ética e transparência. A conformidade com essas normas, tanto no âmbito local quanto internacional, é essencial para a segurança das operações e a proteção do indivíduo.

De início, uma das importantes diferenças entre as normas que deve ser mencionada é o escopo territorial, material e pessoal de cada uma delas. A lei europeia é amplamente aplicável a qualquer entidade que processe dados de cidadãos da União Europeia. O GDPR é reconhecido como uma das leis mais expansivas e rigorosas. Seu alcance extraterritorial visa diretamente influenciar qualquer organização que interaja com quaisquer dados pessoais, seja para uso comercial ou não, de residentes da UE, independentemente de onde esteja localizada. Ou seja, empresas estrangeiras que coletam ou monitoram dados de europeus são obrigadas a cumprir o GDPR (União Europeia, 2016).

A LGPD, no Brasil, aplica-se a qualquer tratamento de dados pessoais realizado no território brasileiro. Além disso, também abrange operações feitas fora do Brasil que tenham como objetivo oferecer ou fornecer bens ou serviços a indivíduos no Brasil ou que tratem dados de pessoas localizadas no país. Dessa forma, ela possui um alcance extraterritorial em casos específicos, o que reflete uma preocupação com a proteção de dados dos cidadãos brasileiros mesmo em transações internacionais (Brasil, 2018).

A PIPL também se aplica extraterritorialmente, mas com uma ênfase mais forte na segurança nacional e pública. A lei abrange o tratamento de dados de cidadãos chineses fora do país se isso afetar a segurança nacional ou pública

ou os direitos dos cidadãos chineses. As restrições da China incluem regras de transferência de dados para fora do país, exigindo até que dados sensíveis sejam armazenados em território chinês (China, 2021).

A norma europeia aplica-se amplamente, com foco na proteção da privacidade e nos direitos dos indivíduos, a lei brasileira protege dados pessoais de brasileiros, mas seu alcance extraterritorial é mais restrito, voltado a interesses comerciais, já a PIPL dá um enfoque adicional à soberania digital chinesa, incluindo um maior controle sobre os dados de seus cidadãos, mesmo quando processados fora do país (União Europeia, 2016; Brasil, 2018; China, 2021).

Já outra distinção está nas penalidades e sanções, embora todas as leis prevejam sanções severas, o Brasil é o mais brando. As multas sob a União Europeia são notoriamente altas, enquanto a China impõe sanções robustas (Brasil, 2018; União Europeia, 2016; China, 2021).

A norma brasileira estabelece sanções administrativas que incluem advertência, multa de até 2% do faturamento da empresa, limitada a 50 milhões de reais por infração, e suspensão ou proibição do exercício de atividades relacionadas ao tratamento de dados (Brasil, 2018).

O regulamento da União Europeia impõe multas de até 20 milhões de euros ou 4% do faturamento global anual da empresa, o que for maior, além de outras medidas, como restrição do tratamento de dados (União Europeia, 2016).

Já a China estabelece multas de até 50 milhões de yuans ou 5% da receita anual da empresa, e pode suspender ou encerrar operações. Também prevê penalidades criminais para violações graves (China, 2021).

Em síntese, embora Brasil, União Europeia e China compartilhem o objetivo de proteger os dados pessoais, suas abordagens em termos de sanções refletem diferentes graus de severidade. Enquanto a legislação brasileira é relativamente mais branda, a União Europeia aplica penalidades financeiras mais severas e a China vai além, incorporando sanções robustas que incluem até penalidades criminais, reforçando sua postura rígida em relação à proteção de dados e soberania digital (Brasil, 2018; União Europeia, 2016; China, 2021).

Outra distinção entre as leis está na Transferência Internacional de Dados, o GDPR europeu e a LGPD brasileira possuem mecanismos rigorosos para a transferência internacional de dados, incluindo a necessidade de garantias adequadas para a proteção dos dados. A PIPL chinesa, por outro lado, coloca um foco maior na soberania digital chinesa, com restrições mais rígidas para a transferência de dados para o exterior (União Europeia, 2016; Brasil, 2018; China, 2021).

A União Europeia impõe requisitos rigorosos para a transferência internacional de dados, exigindo que os dados sejam transferidos para países que ofereçam um nível de proteção adequado ou com base em salvaguardas apropriadas, como cláusulas contratuais padrão ou regras corporativas vinculativas (União Europeia, 2016).

No mesmo sentido, a norma brasileira define que transferências internacionais de dados só podem ocorrer para países que garantam um nível

adequado de proteção de dados ou em situações específicas, como o consentimento explícito ou acordos contratuais entre as partes. (Brasil, 2018).

Já a China impõe restrições ainda mais rígidas para a transferência internacional de dados, incluindo a necessidade de aprovação do governo chinês e a realização de avaliações de impacto sobre a segurança dos dados, com ênfase na proteção da soberania digital da China (China, 2021).

É evidente que tanto a União Europeia, quanto o Brasil e a China adotam abordagens rigorosas para a transferência internacional de dados, refletindo a crescente preocupação global com a proteção da privacidade e a segurança das informações pessoais.

Apesar de seguirem princípios comuns, como a exigência de um nível adequado de proteção nos países destinatários, cada jurisdição possui particularidades que reforçam seus interesses específicos, seja pela proteção dos direitos dos titulares de dados, como no caso europeu e brasileiro, ou pela ênfase na soberania digital, como destaca a legislação chinesa.

5 ESTUDO DE CASOS

5.1 A IMPORTÂNCIA DO ESTUDO DE CASOS

O estudo de casos é uma metodologia essencial em pesquisas jurídicas, especialmente no campo da segurança de dados. Esta abordagem oferece análises práticas sobre a aplicação de regulamentações e permite uma análise detalhada dos desafios e soluções encontradas por empresas e órgãos reguladores ao longo de processos reais de conformidade com leis. Em vez de focar apenas nas diretrizes teóricas e normativas.

O estudo de casos fornece uma visão contextualizada, que facilita a compreensão dos impactos e nuances das leis de proteção de dados na prática, Kathleen Eisenhardt, uma referência em estudos de caso no contexto de administração e negócios, escreveu:

> Estudos de caso são uma estratégia de pesquisa que permite aos pesquisadores obter insights e construir teorias a partir de dados empíricos da vida real. Eles são particularmente úteis na exploração de novas áreas onde há pouca base teórica. (EISENHARDT, 1989, p. 534)

Mostra-se que um dos principais benefícios do estudo de casos é a sua capacidade de ilustrar desafios reais e as estratégias adotadas para solucioná-los, possibilitando uma análise mais profunda e concreta do que as exigências legais significam no dia a dia das organizações.

Por meio de casos específicos, é possível observar como diferentes empresas lidam com questões como coleta e armazenamento de dados, transferências internacionais e respostas a violações de segurança. Isso também revela como as regulamentações podem ser interpretadas e aplicadas em contextos específicos, considerando fatores culturais, econômicos e tecnológicos locais.

Além disso, o estudo de casos permite que pesquisadores e profissionais do direito identifiquem padrões e melhores práticas, contribuindo para o desenvolvimento de soluções mais eficazes e aplicáveis em cenários semelhantes. Por exemplo, analisar como grandes empresas de tecnologia enfrentam investigações e implementaram programas de compliance robustos pode ajudar outras organizações a antecipar desafios e estruturar seus próprios mecanismos de proteção de dados de maneira mais sólida. No mesmo sentido segue o entendimento de Kathleen Eisenhardt:

> Os estudos de caso são particularmente valiosos em ambientes de alta velocidade, onde a complexidade e a rapidez das mudanças tornam difícil tirar conclusões a partir dos métodos tradicionais de coleta de dados. (Eisenhardt, 1997, p. 573)

Outro ponto relevante é que o estudo de casos possibilita uma análise comparativa prática entre diferentes jurisdições, destacando como cada uma delas lida com a proteção de dados em situações concretas. Isso é especialmente útil para entender as áreas onde as regulamentações divergem ou convergem e como essas diferenças influenciam as decisões das empresas em nível global.

Em suma, o estudo de casos em segurança de dados proporciona uma abordagem prática e detalhada que complementa a teoria, oferecendo uma base sólida para compreender a eficácia e os desafios da aplicação das leis de proteção de dados. Ele promove uma análise prática e contextualizada, fundamental para o desenvolvimento de políticas, a formação de melhores práticas e a construção de um ambiente jurídico mais acessível e informativo.

5.2 BRASIL: CASO DO BANCO INTER

Em 2018, o Banco Inter, um dos pioneiros em oferecer contas digitais no país, registrou um vazamento de dados que comprometeu clientes da empresa. Supostamente um hacker teria acessado conteúdos como senhas, códigos de verificação, cheques, declarações de imposto de renda e dados pessoais dos clientes do banco. A empresa fechou um acordo com o Ministério Público e pagou uma multa de R$1 milhão, que foi destinada a instituições públicas de caridade e a organizações que trabalham combatendo o crime cibernético (MPDF, 2018).

Com a entrada em vigor da Lei Geral de Proteção de Dados em 2020, o Banco Inter, uma instituição financeira digital no Brasil, precisou adaptar suas práticas de tratamento de dados. O banco lidava com uma grande quantidade de dados sensíveis, como informações financeiras e pessoais de clientes. Com isso, foi necessário garantir que as práticas de coleta, armazenamento e processamento estivessem em conformidade com a LGPD (BANCO INTER, 2024).

Não foi registrado um processo judicial específico, pois o caso foi resolvido extrajudicialmente por meio de um Termo de Ajustamento de Conduta (TAC) junto ao Ministério Público do Distrito Federal e Territórios. Esse TAC impôs ao banco obrigações de aprimorar suas práticas de segurança. A empresa

implementou um programa de governança de dados constituindo a criação de um Encarregado de Proteção de Dados (DPO); o mapeamento dos dados pessoais tratados pelo banco; a reavaliação de bases legais para tratamento de dados e obtenção de consentimento; e, a revisão de contratos com fornecedores que também tratavam dados pessoais.

O fato de o caso ter sido resolvido por meio de um Termo de Ajustamento de Conduta (TAC) indica a importância de acordos extrajudiciais no Brasil para resolver questões relacionadas à proteção de dados pessoais. Isso foi possível, pois o Ministério Público entendeu que o Banco Inter demonstrou boa-fé ao cooperar para implementar mudanças significativas em suas políticas de segurança de dados.

Com a adaptação o Banco Inter se posicionou como uma empresa que respeita a privacidade de seus clientes, além de evitar penalidades futuras da Agência Nacional de Proteção de Dados (FEBRABAN, 2018).

Mesmo com a implementação dessas medidas corretivas, o Banco Inter, como outras empresas que lidam com dados sensíveis, devem continuar monitorando constantemente suas práticas de segurança e compliance. A LGPD impõe um regime de auditorias regulares e reportes de incidentes de segurança, além de exigir atualizações contínuas nos sistemas de proteção de dados, para que as empresas possam responder rapidamente a novas ameaças cibernéticas.

Outra medida foi a criação de um Encarregado de Proteção de Dados (DPO), responsável por garantir que a empresa esteja em conformidade com as normas de privacidade e segurança, foi uma medida importante implementada após o incidente.

Além disso, o crescente volume de transações digitais e a evolução das técnicas de ataque cibernético exigem que o Banco Inter e outras instituições financeiras invistam continuamente em tecnologias de proteção de dados, como encriptação de dados, monitoramento de redes e treinamento de equipes internas para lidar com questões de segurança cibernética.

5.3 UNIÃO EUROPEIA: CASO DA EMPRESA GOOGLE

A Google enfrentou um dos maiores desafios de conformidade com a norma da Europa. Em 2019, a empresa foi multada em 50 milhões de euros pela autoridade de proteção de dados da França (CNIL) por não fornecer informações claras e acessíveis aos usuários sobre como seus dados pessoais estavam sendo processados. A multa foi aplicada devido a violações relacionadas à falta de transparência e consentimento inadequado para anúncios personalizados (EUROPEAN DATA PROTECTION BOARD, 2019).

O regulamento foi amplamente aplicado à Google devido às suas operações na União Europeia, particularmente na coleta e uso de dados pessoais para anúncios personalizados.

O principal problema identificado pela CNIL foi que a Google não forneceu informações suficientes e claras aos usuários sobre como seus dados pessoais eram processados, particularmente no que se refere à personalização de

anúncios, uma área central de seus serviços. De acordo com a CNIL, as informações eram apresentadas de maneira difusa e de difícil acesso, o que dificultava para os usuários entenderem e consentirem de forma explícita sobre o uso de seus dados (EUROPEAN DATA PROTECTION BOARD, 2019)..

Após o incidente, a Google ajustou suas práticas, incluindo a criação de controles mais claros para os usuários gerenciarem suas preferências de privacidade e o uso de dados, além de atualizações nos termos de serviço e políticas de privacidade (CNIL, 2023).

O Google atualizou suas políticas de privacidade, proporcionando maior clareza sobre como os dados dos usuários eram coletados e usados, implementou notificações pop-up detalhadas, caixas de seleção para garantir que o consentimento fosse dado de forma explícita, e estabeleceu um Data Protection Officer (DPO) para supervisionar as práticas de proteção de dados.

Apesar das medidas corretivas implementadas, a Google enfrentou desafios em garantir que todas as suas práticas de tratamento de dados atendessem aos rigorosos requisitos do GDPR. A principal dificuldade foi em relação ao consentimento informado, um dos pilares da legislação.

Apesar dessas medidas, o Google foi multado em €50 milhões no ano de 2019 pela CNIL, a autoridade francesa de proteção de dados, por não ter fornecido informações claras e facilmente acessíveis sobre suas políticas de consentimento. Esse caso é um exemplo de como mesmo grandes multinacionais enfrentam desafios significativos para se adequar aos ordenamentos mundiais (GOOGLE, 2024).

A complexidade dos serviços da Google e o grande volume de dados pessoais que ela coleta complicam a tarefa de garantir que cada aspecto do processo de coleta e uso de dados esteja completamente em conformidade com a legislação. Além disso, o caso da Google demonstra como empresas de grande porte podem enfrentar dificuldades práticas ao se adaptar a um regulamento tão detalhado e abrangente como o GDPR.

5.4 CHINA CASO DA EMPRESA DIDI

A DiDi, maior empresa de transporte por aplicativo da China, foi uma das primeiras grandes companhias a enfrentar as exigências da Lei de Proteção de Informações Pessoais (PIPL), que entrou em vigor em 2021.

A empresa atraiu a atenção das autoridades chinesas após sua decisão de abrir o capital nos Estados Unidos, em 2021, em vez de fazer a oferta pública de ações (IPO) na China. Isso gerou uma reação negativa do governo chinês, que considerou essa movimentação uma afronta à segurança nacional e à soberania digital da China. A decisão da DiDi de listar suas ações nos EUA, sem consultar as autoridades regulatórias chinesas, foi vista como uma tentativa de evitar o controle governamental sobre seus dados. Esse incidente desencadeou uma investigação de cibersegurança e proteção de dados, liderada pela Cyberspace Administration of China (CAC), órgão responsável pela segurança cibernética no país (XIONG; REGISTER; HE, 2024).

Em julho de 2022, as autoridades chinesas impuseram à DiDi Global uma multa de US$1,2 bilhão após uma investigação de cibersegurança que apontou "abusos desprezíveis" de dados. A DiDi foi acusada de coleta e uso excessivo e desprotegido de informações pessoais e de dados sensíveis, que incluíam detalhes sobre a localização em tempo real dos usuários, informações de reconhecimento facial e dados dos veículos. Essas práticas foram vistas como risco à segurança nacional. Esse caso, um dos maiores até então, marcou o rigor da China contra empresas de tecnologia que violam a regulamentação de dados, conforme as novas exigências da Lei de Proteção de Informação Pessoal (PIPL)(WEBSTER, 2024).

Além da multa substancial, os executivos da DiDi, incluindo Zhang Bo e Cheng Wei, foram multados em 1 milhão de yuans (aproximadamente US$ 150 mil) cada um, em um claro sinal de que a responsabilidade pela proteção de dados não recai apenas sobre a empresa, mas também sobre seus líderes executivos.

Como parte das exigências regulatórias para retomar as operações, a DiDi precisou revisar profundamente seus protocolos de coleta e armazenamento de dados para atender aos critérios de segurança e privacidade estabelecidos pela PIPL. A empresa foi obrigada a implementar controles mais rigorosos para a transferência de dados internacionais, exigindo avaliações de impacto sempre que dados pessoais fossem enviados para fora da China (DIDI, 2023).

A CAC também determinou que a DiDi realizasse auditorias periódicas e fornecesse relatórios de conformidade, além de restringir temporariamente o download do aplicativo em lojas online chinesas, uma medida que impactou consideravelmente a empresa e seus serviços no país. Somente após a adequação de suas práticas à PIPL, a DiDi conseguiu retomar a operação do aplicativo, embora continue sob forte monitoramento regulatório.

O impacto do incidente foi significativo para a DiDi, não só em termos financeiros, mas também em sua capacidade de operar dentro da China. A empresa enfrentou restrições temporárias no download de seu aplicativo nas lojas de aplicativos chinesas e perdeu acesso a alguns dados essenciais para suas operações.

O caso da DiDi serve como um forte aviso para empresas globais sobre os riscos e as penalidades associadas ao não cumprimento de regulamentações de proteção de dados em mercados onde essas leis são rigorosamente aplicadas. Com a PIPL estabelecendo padrões altos para a coleta e o tratamento de dados pessoais, a DiDi precisou adotar uma série de mudanças significativas para garantir a continuidade de suas operações e evitar penalidades adicionais. Este caso também destaca como o governo chinês está se tornando cada vez mais ativo na regulação e monitoramento das empresas de tecnologia em relação à segurança de dados e à privacidade.

Esses casos também reforçam a tendência de um aumento na regulação global em relação à proteção de dados pessoais, refletindo uma crescente conscientização sobre a privacidade e segurança dos dados no contexto de um mundo cada vez mais digitalizado.

6 IMPLICAÇÕES PARA A PRÁTICA DE COMPLIANCE

Esses casos, Banco Inter, Google e DiDi, demonstram a diversidade e complexidade dos desafios enfrentados por empresas ao lidar com questões de proteção de dados pessoais em diferentes partes do mundo. Eles ilustram como as empresas precisam não apenas investir em tecnologias de segurança e compliance, mas também compreender profundamente as regulamentações locais e globais sobre proteção de dados. Além disso, as penalidades severas e as consequências para a reputação das empresas destacam a importância de uma governança de dados robusta e da conscientização contínua sobre os riscos cibernéticos. Esses casos também reforçam a tendência de um aumento na regulação global em relação à proteção de dados pessoais, refletindo uma crescente conscientização sobre a privacidade e segurança dos dados no contexto de um mundo cada vez mais digitalizado. Com o surgimento e desenvolvimento das regulamentações de proteção de dados em diferentes partes do mundo, as empresas se deparam com a necessidade crescente de adaptar seus programas de compliance para cumprir leis locais e internacionais, como o GDPR na União Europeia, a LGPD no Brasil e a PIPL na China. Essas regulamentações impõem exigências rigorosas para o tratamento, segurança e transferência de dados pessoais, que demandam investimentos em tecnologia, processos internos robustos e equipes especializadas (ABRAPP, 2021).

Outro fator que impulsionou as regulamentações foi a pandemia de COVID-19, com base nas informações do Deloitte Global Risk Management Survey – 12ª edição (Deloitte, 2021), pode se observar que a pandemia não apenas impactou as operações das empresas, mas também acelerou a transformação digital e redefiniu as prioridades na gestão de riscos. As mudanças trazidas pela crise sanitária revelaram a necessidade urgente de adaptação dos programas de compliance e gestão de riscos às novas realidades operacionais e tecnológicas, estabelecendo novos desafios e oportunidades para as organizações. Empresas que operam globalmente precisam ajustar seus processos de conformidade para atender às exigências específicas de cada jurisdição. A União Europeia, o Brasil e a China, por exemplo, compartilham semelhanças, como a garantia dos direitos dos titulares de dados e a necessidade de nomeação de um DPO em determinadas situações. Contudo, cada uma dessas regulamentações possui nuances distintas, especialmente em questões como sanções, escopo territorial e a proteção da soberania digital, especialmente evidente na legislação chinesa. A adaptação a esses diferentes regimes implica a necessidade de monitoramento contínuo, criação de políticas abrangentes e treinamento das equipes (LORENZON, 2021).

O Deloitte Global Risk Management Survey (2021) também revela que, em um ambiente cada vez mais regulamentado, as empresas passaram a focar mais intensamente em garantir conformidade com normas globais como o GDPR na Europa, a LGPD no Brasil e outras legislações relacionadas à proteção de dados pessoais. De acordo com o relatório, 72% das empresas relataram que a conformidade regulatória e a gestão de riscos relacionados a dados são agora prioridades estratégicas para suas equipes de gestão de risco. Isso reflete uma mudança de postura no mercado, em que as

organizações não apenas buscam evitar multas e penalidades, mas também desejam fortalecer sua imagem e relação com os consumidores por meio de práticas éticas e transparentes no tratamento de dados (DELOITTE, 2021).

Além disso, programas de compliance de dados robustos também devem incluir avaliações regulares de conformidade e auditorias internas. Assim como uma revisão periódica pode identificar falhas na estrutura de um prédio, auditorias de conformidade garantem que o sistema de proteção de dados esteja sólido, corrigindo vulnerabilidades antes que elas se tornem problemas legais (ANPD, 2020). Deve-se destacar a importância de uma cultura organizacional sólida em relação à gestão de riscos. As empresas que promovem uma cultura de transparência, ética e responsabilidade tendem a ser mais eficazes na mitigação de riscos e na implementação de programas de compliance. Além disso, o Deloitte Global Risk Management Survey destaca a importância do compromisso da liderança no fortalecimento da gestão de riscos. Organizações com líderes que apoiam ativamente os programas de compliance e incentivam uma cultura organizacional de risco são mais bem preparadas para enfrentar os desafios regulatórios e as crises emergentes, como as causadas pela pandemia (DELOITTE, 2021).

Para aumentar a eficiência, muitas empresas têm adotado ferramentas de automação e inteligência artificial (IA), que ajudam no monitoramento de grandes volumes de dados e na execução de auditorias automáticas de segurança. Essas ferramentas atuam como uma camada extra de proteção, analisando os dados em tempo real para detectar possíveis violações antes que elas ocorram (EUROPA, 2023). O que por muitas vezes passa despercebido são as relações com terceiros e com sua cadeia de fornecimento. Assim como uma corrente é tão forte quanto o seu elo mais fraco, o compliance de dados também depende da conformidade de fornecedores e parceiros. Isso exige contratos bem definidos e auditorias periódicas para assegurar que todas as partes estão em conformidade com as regulamentações de proteção de dados (FARIA; WANDER; NASCIMENTO, 2020).

Também é de suma importância, em situações de incidentes de segurança, ter planos de resposta e recuperação. Esses planos são essenciais para mitigar rapidamente os danos e garantir a comunicação adequada às autoridades e aos titulares de dados. Isso age como um seguro contra incêndio, minimizando o impacto de uma violação e preservando a confiança dos clientes, demonstrando transparência e agilidade na resposta (ABRAPP, 2021). O Deloitte Global Risk Management Survey (2021) sugere que a integração de programas de compliance na governança corporativa e na gestão de riscos empresariais é uma tendência crescente. Programas de compliance não devem ser vistos apenas como ferramentas para evitar penalidades, mas como uma parte essencial da estratégia geral de negócios, fortalecendo a resiliência corporativa e melhorando a capacidade das organizações de se adaptarem a mudanças regulatórias e crises imprevistas. Empresas que alinham suas estratégias de compliance com a gestão de riscos têm maior capacidade de antecipar e responder rapidamente a desafios regulatórios, além de aumentar sua competitividade no mercado global (DELOITTE, 2021).

A nomeação de um DPO e o treinamento contínuo das equipes também são fundamentais. O DPO atua não só como ponto de contato com as autoridades e titulares de dados, mas supervisiona políticas internas e prevenção de riscos. Um programa de treinamento contínuo ajuda a reforçar a cultura de compliance, incentivando os colaboradores a praticarem a proteção de dados no dia a dia, transformando o compliance em um compromisso ético de toda a empresa (ANPD, 2020). Empresas que necessitam transferir dados entre fronteiras enfrentam desafios para garantir que os países destinatários oferecem níveis adequados de proteção. Esse aspecto exige que os programas de compliance incluam políticas específicas para transferências internacionais e que estabeleçam contratos e outras garantias, como cláusulas de proteção de dados, compatíveis com as exigências de cada jurisdição (ABRAPP, 2021).

Em suma, as regulamentações de proteção de dados exigem que os programas de compliance das empresas estejam bem estruturados, alinhados com as leis locais e internacionais e continuamente atualizados para responder a um ambiente legal em rápida evolução. Ao fazer isso, as organizações não só evitam sanções, mas também promovem uma cultura de transparência, ética e responsabilidade, fortalecendo sua competitividade e resiliência no mercado global.

CONSIDERAÇÕES FINAIS

Em um mundo cada vez mais globalizado e digitalizado, a proteção de dados emergiu como um imperativo global. Com as fronteiras digitais nos aproximando, a harmonização das legislações e a salvaguarda dos direitos individuais tornam-se mais urgentes do que nunca.

As empresas, como agentes fundamentais no tratamento de dados pessoais, têm um papel crucial na proteção da privacidade. A adoção de práticas robustas de segurança e a implementação de programas de compliance são essenciais para garantir a confiança dos consumidores e mitigar sanções legais. Nesse contexto, é imprescindível que as empresas busquem o acompanhamento jurídico especializado, a fim de garantir a conformidade com as legislações locais e internacionais, evitando riscos legais e danos à sua reputação.

Além disso, é imperativo estudar as legislações de diferentes blocos territoriais, pois cada região possui suas particularidades e abordagens sobre a proteção de dados. A realização de estudos comparados de casos permite não apenas compreender essas diferenças, mas também identificar melhores práticas e soluções que podem ser adaptadas a diferentes contextos, enriquecendo o debate e a eficácia das políticas de privacidade.

O futuro da privacidade é complexo e repleto de desafios. A crescente coleta e utilização de dados pessoais demandam uma reavaliação dos nossos conceitos de privacidade e a busca por soluções inovadoras para proteger nossos direitos. A implementação de programas de compliance não deve ser vista apenas como uma obrigação legal, mas como um investimento estratégico na confiança do cliente e na segurança da operação empresarial.

A proteção de dados exige atenção contínua e adaptação às novas realidades. É vital que empresas, governos e a sociedade civil colaborem para assegurar a privacidade e a segurança das informações pessoais. O futuro da privacidade depende das ações do presente.

REFERÊNCIAS

ABRAPP. Código de autorregulação em governança corporativa. 2019. Disponível em: https://www.abrapp.org.br/wp-content/uploads/2021/01/manualautorregulacaocorporativa.pdf. Acesso em: 29 jun. 2024.

ALLAH RAKHA, N. (2023). *Navigating the Legal Landscape: Corporate Governance and Anti-Corruption Compliance in the Digital Age*. *International Journal of Management and Finance*. Acessado em: https://irshadjournals.com/index.php/ijmf/article/view/39.

BANCO INTER, Privacidade de Dados, 2024. Disponível em: https://inter.co/privacidade-de-dados/. Acesso em: 20 de outubro de 2024.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Brasília, 2020. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/guia-orientativo-para-definicoes-dos-agentes-de-tratamento-de-dados-pessoais-e-do-encarregado. Acesso em: 20 out. 2024.

BRASIL. (1988). Constituição da República Federativa do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. (1990). Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm.

BRASIL. (1996). Lei nº 9.296, de 24 de julho de 1996. Dispõe sobre a interceptação de comunicações telefônicas e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm.

BRASIL. (2014). Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l12965.htm.

BRASIL. (2018). Lei nº 13.709, de 14 de agosto de 2018. Estabelece a proteção de dados pessoais e regula a utilização desses dados. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l13709.htm.

CNIL (Commission Nationale de l'Informatique et des Libertés). Closure of the injunction issued against GOOGLE. Agosto 2023. Disponível em: https://www.cnil.fr/en/closure-injunction-issued-against-google. Acesso em: 22 de outubro de 2024.

COUNCIL OF EUROPE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Treaty Office, União Europeia. Disponível em:

https://www.coe.int/en/web/data-protection/convention108/parties. Acesso em: 14 de outubro de 2024.

DELOITTE. Global Risk Management Survey 12th edition. 2021. Disponível em: https://www2.deloitte.com/global/en/pages/risk/articles/global-risk-management-survey.html. Acesso em: 14 nov. 2024.

DIDI. Política de Privacidade. Atualizado em 05 de abril de 2023. Disponível em: https://privacycenter.didiglobal.com/BR/privacy-notice/3f9ccfec294a7fd662b43fbc5036124b?id=315. Acesso em: 22 de outubro de 2024.

EISENHARDT, K. M. (1989), *Building Theories from Case Study Research*, *Academy of Management Review*. Disponível em: https://www.jstor.org/stable/258557. Acesso em: 20 de outubro de 2024.

EISENHARDT, K. M. (1997), *Making Fast Strategic Decisions in High-Velocity Environments*, *Academy of Management Journal*. Disponível em: https://gmdconsulting.eu/nykerk/wp-content/uploads/2020/02/Making-high-quality-decisions-in-high-velocity-environments-_-Eisenhardt.pdf. Acesso em: 20 de outubro de 2024.

EUROPEAN DATA PROTECTION BOARD, The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. Disponível em: https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en. Acesso em: 22 de outubro de 2024.

EUROPA. Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI. European Parliament, 6 dez. 2023. Disponível em: https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai. Acesso em: 14 out. 2024.

FEBRAN (Federação Brasileira de Bancos), Guia | Boas Práticas de Compliance, Edição revista e atualizada 2018. Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/febraban_manual_compliance_2018_2web.pdf. Acesso em: 20 de outubro de 2024.

GISONNA, Nicholas. The Great Firewall of China. *Encyclopaedia Britannica*. Disponível em: https://www.britannica.com/topic/Great-Firewall. Acesso em 16 de outubro de 2024.

GOOGLE. Política de Privacidade do Google. 16 de setembro de 2024. Disponível em: https://policies.google.com/privacy?hl=pt-BR. Acesso em: 22 de outubro de 2024.

HOTTEN, Russell. BBC. Dezembro de 2015. Disponível em: https://www.bbc.com/news/business-34324772. Acesso em 12 de outubro de 2024.

KUNER, C. (2017). *The General Data Protection Regulation: A commentary*. Oxford University Press. Disponível em: https://academic.oup.com/book/41324. Acesso em: 20 de outubro de 2024.

LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos

instrumentos de enforcement. *Revista do Programa de Direito da União Europeia*, Rio de Janeiro, v. 1, pp. 39-52, 2021. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rpdue/article/view/83423. Acesso em: 6 abr. 2021.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL. MPDFT ajuíza ação contra o Banco Inter por vazamento de dados pessoais. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10211-mpdft-ajuiza-acao-contra-o-banco-inter-por-vazamento-de-dados-pessoais. Acesso em: 20 de outubro de 2024.

OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Disponível em: https://www.oecd-ilibrary.org/docserver/9789264196391-sum-pt.pdf?expires=1731592289&id=id&accname=guest&checksum=1ADD83CFBFD29619F45E656C2ED4F6C6. Acesso em: 14 outubro 2024.

UNIÃO EUROPEIA. Diretiva 95/46/CE, de 24 de outubro de 1995. Relativa à proteção das pessoas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 14 outubro 2024.

UNIÃO EUROPEIA. (2000). Carta dos Direitos Fundamentais da União Europeia. Artigo 8. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32000X1219%2801%29. Acesso em 14 de outubro de 2024.

UNIÃO EUROPEIA. (2016). Regulamento (UE)