PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NUCLEO DE PRATICA JURIDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

ARTIGO CIENTÍFICO

A LEI GERAL DE PROTEÇÃO DE DADOS E SUA APLICABILIDADE PERANTE AS EMPRESAS BRASILEIRAS

ORIENTANDO (A): GUILHERME SILVA DOS REIS

ORIENTADOR (A): Prof.ª. ME ADRIANA DA CUNHA BORGES

GOIÂNIA – GO

2024

GUILHERME SILVA DOS REIS

A LEI GERAL DE PROTEÇÃO DE DADOS E SUA APLICABILIDADE PERANTE AS EMPRESAS BRASILEIRAS

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Comunicação e Negócios, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS). Profª. Orientadora: Me. Adriana da Cunha Borges

GOIÂNIA

2024

GUILHERME SILVA DOS REIS

A LEI GERAL DE PROTEÇÃO DE DADOS E SUA APLICABILIDADE PERANTE AS EMPRESAS BRASILEIRAS

Data da defesa: 27 de novembro de 2024

BANCA EXAMINADORA

_____

Orientador: Profª. Me. Adriana da Cunha Borges Nota

_____

Examinador Convidado: Profª. Drª. Fernanda de Paula Ferreira Moi Nota

SUMÁRIO

SIGLAS:

LGPD - Lei Geral de Proteção de Dados

GDPR – Regulamento Geral de Proteção de Dados

ANPD – Autoridade Nacional de Proteção de Dados

DPO - Data Protection Officer (Responsável pela proteção de Dados)

A LEI GERAL DE PROTEÇÃO DE DADOS E SUA APLICABILIDADE PERANTE AS EMPRESAS BRASILEIRAS

Guilherme Silva dos Reis

RESUMO

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), é um marco legal no Brasil que visa proteger a privacidade e segurança dos dados pessoais dos cidadãos. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD estabelece regras para o tratamento de dados por organizações públicas e privadas no Brasil, aplicando-se a atividades realizadas no país ou relacionadas a serviços e bens oferecidos a pessoas no Brasil. A lei exige que as empresas adotem práticas transparentes e responsáveis na gestão de dados, dando maior controle aos indivíduos sobre suas informações, para fortalecer a confiança nas relações comerciais e proteger os direitos individuais. Assim como a importância de um especialista em LGPD atuando em uma empresa. O estudo destaca os desafios enfrentados pelas empresas para se adequarem à LGPD, que, apesar das dificuldades, é de cumprimento obrigatório. O artigo também aborda a transição do setor empresarial diante das exigências impostas pela lei. Para elaboração do presente artigo científico, a fim de analisar a temática da Lei Geral de Proteção de Dados, e sua aplicabilidade no ordenamento jurídico brasileiro. Contudo, foram utilizadas pesquisas teóricas a respeito do assunto, visando analisar toda a problemática e gerar uma discussão acerca do tema em comento, além da pesquisa bibliográfica, bem como da utilização do método dedutivo. Para este efeito foi utilizada a metodologia de estudo e pesquisas aprofundadas nas dificuldades das empresas com a implementação da LGPD, com análises doutrinarias e legislativas sobre o direito da privacidade de dados pessoais.

Palavras chave: Tratamento. Dificuldades. Implementação. DPO - ANPD. Privacidade.

INTRODUÇÃO

A Lei nº 13.709/2018, cujo nome é Lei Geral de Proteção de Dados (LGPD) representa um marco significativo no cenário legal brasileiro, introduzindo normas e diretrizes destinadas a proteger a privacidade e a segurança das informações pessoais dos cidadãos. Promulgada em 2018 e inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD estabelece princípios e regras específicos para o tratamento de dados pessoais por organizações públicas e privadas no Brasil.

Este tema é de relevância tanto do ponto de vista acadêmico quanto prático, uma vez que a privacidade de dados visa proteger os direitos dos indivíduos protegendo dados sensíveis como origem racial, convicção religiosa, opinião politica, filiação sindical, saúde, vida sexual, genética e biometria, evitando assim riscos jurídicos para as empresas.

A legislação surge em resposta à proteção da privacidade, reconhecendo a importância de resguardar a privacidade dos indivíduos em um ambiente em que a coleta, armazenamento e processamento de dados tornaram-se práticas comuns. A LGPD se aplica a qualquer operação de tratamento de dados pessoais realizada por organizações, independentemente do setor em que atuam, desde que essas atividades ocorram no território brasileiro ou estejam relacionadas a bens ou serviços oferecidos a pessoas localizadas no Brasil.

A implementação da LGPD exige que as empresas brasileiras adotem práticas mais transparentes e responsáveis no que diz respeito à gestão de dados pessoais, fornecendo aos titulares das informações maior controle sobre suas próprias informações. Essa abordagem orientada pela privacidade visa promover a confiança nas relações comerciais e, ao mesmo tempo, fortalecer a proteção dos direitos individuais.

Esse estudo tem como finalidade explicar o que é a LGPD, como, onde e quando ela se aplica, trazendo também as dificuldades em que as empresas obtêm ao implementar a mesma em sua realidade, uma vez que em período anterior, os direitos ao sigilo das pessoas eram totalmente quebrados e não existia amparo legal para que essa exigência se cumprisse. Para isso foram

utilizadas pesquisas teóricas a respeito do assunto, visando analisar toda a problemática. A pesquisa bibliográfica foi de suma importância para o desenvolvimento teórico, com a finalidade de aprofundar o conhecimento. Ao decorrer do artigo serão desenvolvidos em capítulos e subcapítulos sendo eles a definição e princípios importantes da LGPD, os entraves legislativos para a implementação dela nas empresas, o treinamento para profissionais atuarem nas nelas e as barreiras possíveis que as mesmas colocam para a implementação da LGPD.

Ainda neste artigo, será demonstrado a transição que o meio empresarial teve e tem que enfrentar, uma vez que uma série de exigências tornaram essa mudança muito difícil, porém, por ser obrigatória, teve de ser abraçada. Para isso, serão empregadas pesquisas teóricas sobre o tema, com o objetivo de analisar a problemática e fomentar uma discussão a respeito do assunto em questão, além de uma revisão bibliográfica e da aplicação do método dedutivo.

1 DEFINIÇÃO LEI GERAL DE PROTEÇÃO DE DADOS

A Lei nº 13.709/2018 conhecida como Lei Geral de Proteção de Dados (LGPD) é a legislação brasileira que trata da proteção, coleta, tratamento, armazenamento e compartilhamento de dados pessoais por organizações públicas e privadas. Aprovada em 2018, ela entrou em vigor em setembro de 2020, estabelecendo um conjunto de regras e princípios para o manuseio de informações pessoais no Brasil.

Em seu 1º artigo a LGPD afirma que seu propósito é regular o tratamento de dados pessoais no Brasil, com o objetivo de garantir o respeito à privacidade das pessoas, a proteção de seus direitos fundamentais e o livre desenvolvimento da personalidade.

Ele contém a seguinte redação:

> Art. 1° Esta Lei dispõe sobre o tratamento de dados pessoais inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Em resumo, o artigo 1° da LGPD estabelece a abrangência da lei, indicando quem está sujeito a ela pessoas naturais e jurídicas e o seu propósito primordial é proteger os direitos fundamentais relacionados à liberdade, privacidade e desenvolvimento pessoal no contexto do tratamento de dados.

Na doutrina Comentários ao GDPR (Regulamento Geral de Proteção de Dados), Maldonato et al (2019), assevera que:

> Naturalmente, o foco é a proteção de direitos e garantias fundamentais dos cidadãos, com o objetivo de mitigar os riscos, em relação ao que pode ser levado a efeito, a partir da coleta e do futuro uso, compartilhamento, armazenamento, entre outros, desses dados. (MALDONADO et al., 2019, p.20).

A expressão "mitigar os riscos" sugere que a legislação busca reduzir ou evitar possíveis ameaças ou danos relacionados à coleta e ao uso futuro dos dados pessoais. Em outras palavras, a intenção é minimizar os perigos ou impactos negativos que podem surgir quando dados pessoais são coletados, processados, compartilhados, armazenados, ou sujeitos a outras formas de

manipulação. A menção a "coleta e futuro uso, compartilhamento, armazenamento, entre outros" indica que a lei não se concentra apenas na fase inicial de obtenção de dados, mas abrange todo o ciclo de vida da informação pessoal. Isso significa que as organizações e entidades que lidam com dados pessoais devem considerar não apenas como coletam esses dados, mas também como os utilizam posteriormente, compartilham com terceiros, armazenam e realizam outras operações relacionadas.

Essa abordagem ampla visa assegurar que a privacidade e os direitos dos cidadãos sejam respeitados ao longo de todo o processo de manipulação de dados pessoais, desde a sua coleta até o seu descarte ou eliminação. Em resumo, o objetivo principal é criar um ambiente regulatório que proteja os indivíduos contra possíveis abusos ou violações de privacidade que possam ocorrer no contexto da coleta e do tratamento de seus dados pessoais.

Na Lei Geral de Proteção de Dados do Brasil, os “dados sensíveis” são uma categoria especial de dados pessoais que, devido à sua natureza, exigem um nível maior de proteção. De acordo com a LGPD, os dados sensíveis são aqueles que se referem a origem racial ou étnica, a convicção religiosa, a opinião política, a filiação a sindicato ou a organização de caráter religioso, filosófico ou político, os dados de saúde ou vida sexual, os dados genéticos e biométricos. Esses dados são considerados sensíveis porque podem ser usados para discriminar ou violar a privacidade e a liberdade individual das pessoas. A LGPD impõe regras mais rígidas para o tratamento desses dados, restringindo a coleta, o processamento e o compartilhamento deles. Em geral, o tratamento de dados sensíveis só é permitido com o consentimento explícito do titular, ou em situações excepcionais previstas na lei, como para o cumprimento de obrigações legais ou para a proteção da vida do titular ou de terceiros.

Além disso, a LGPD prevê que as empresas devem adotar medidas de segurança apropriadas para proteger esses dados, visando reduzir os riscos de vazamentos e acessos não autorizados.

1.1 PRINCÍPIOS FUNDAMENTAIS DA LGPD

A LGPD baseia-se em princípios fundamentais para o tratamento de dados pessoais, como o princípio da finalidade (os dados devem ser utilizados para propósitos legítimos e específicos), o princípio da necessidade (limitação do tratamento ao mínimo necessário) e o princípio da transparência (informar claramente os titulares dos dados sobre o tratamento). Esses princípios orientam a coleta, uso, armazenamento e compartilhamento de dados pessoais, garantindo a proteção da privacidade e dos direitos dos indivíduos.

O Regulamento Geral de Proteção de Dados, em seu artigo 1º. estabelece que os dados pessoais devem ser tratados de forma lícita, justa e transparente em relação ao titular. Isso nos leva ao princípio da licitude, indicando que os dados só podem ser tratados conforme o que o regulamento determina expressamente, com especial destaque para o artigo 6º, que define as condições de licitude do tratamento.

Conforme podemos ver em, MALDONADO et al (2019, p.47):

> Assim, pelo princípio da Licitude, os responsáveis somente poderão tratar dados dos titulares quando houver uma permissão e fundamentação legal para tal finalidade, notadamente com base no GDPR, para aqueles que estiverem dentro da aplicabilidade desse Regulamento, mas também mediante a análise de outras normas possivelmente aplicáveis de acordo com áreas específicas potencialmente reguladas de forma especial, como saúde, relações trabalhistas, questões tributárias, proteção ao crédito, entre outras. (MALDONADO et al., 2019, p.47).

O tratamento de dados pessoais só pode ser feito quando há uma base legal que permita e justifique essa atividade. Isso significa que os responsáveis por coletar e processar dados só podem fazê-lo se estiverem de acordo com leis e regulamentos que protejam os direitos dos titulares desses dados.

Quando o artigo citado estabelece que os dados pessoais devem ser tratados de forma justa, isso nos remete diretamente ao princípio de equidade que deve ser inerente e inseparável do tratamento de dados. Os responsáveis pelo tratamento têm o dever de informar os titulares sobre a coleta, o armazenamento, o uso e o descarte de seus dados, levando em conta todas as circunstâncias e mecanismos adequados. Dessa forma, os titulares poderão

tomar uma decisão consciente sobre a concordância com o tratamento de seus dados e, ao mesmo tempo, conhecer seus direitos.

Por fim, o artigo trata do princípio da transparência, que deve estar diretamente relacionado à extensão do poder sobre o tratamento de dados pessoais e à capacidade dos titulares de compreender os novos e dinâmicos produtos e serviços oferecidos para seu uso.

É importante observar na doutrina MALDONADO et al (2019) que:

> Os controllers devem considerar sempre os titulares vulneráveis quanto ao entendimento das infinitas possibilidades de tratamento, notadamente quando ocorrer por meios digitais, em uma "conduta silenciosa", pois o déficit informacional ganha relevância no ambiente digital, diante da velocidade das mutações do tratamento de acordo com o avanço tecnológico, aumentando, portanto, a necessidade de informações claras, completas e ostensivas aos titulares, que aceitam determinadas transações ao confiar voluntariamente nas informações concedidas pelos responsáveis. (MALDONADO et al., 2019, p.49).

Os *controllers* (controladores de dados) devem prestar especial atenção aos titulares vulneráveis de dados, que podem ter dificuldades em compreender todas as formas de tratamento de seus dados, especialmente quando esse tratamento ocorre de maneira digital e não explícita, ou seja, de forma "silenciosa".

No ambiente digital, esse problema se agrava devido ao déficit informacional – ou seja, a falta de informações claras e compreensíveis para os titulares – já que as tecnologias e as formas de tratamento de dados mudam rapidamente. Isso exige que os controladores forneçam informações claras, completas e visíveis aos titulares. Muitos indivíduos aceitam transações e o uso de seus dados confiando nas informações que recebem dos responsáveis (controllers), o que torna ainda mais importante que essas informações sejam precisas e transparentes.

O tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Deve ser compatível com as finalidades informadas ao titular, conforme o contexto do tratamento.

A coleta e o tratamento de dados pessoais devem se limitar ao mínimo necessário para a realização das finalidades pretendidas, evitando excessos. Os titulares têm direito a acessar livremente as informações sobre a forma e a duração do tratamento de seus dados pessoais.

Os dados pessoais devem ser exatos, claros, relevantes e atualizados, conforme a necessidade e para o cumprimento da finalidade do tratamento. Os titulares devem ser informados de forma clara, adequada e acessível sobre o tratamento de seus dados e sobre os agentes de tratamento envolvidos. Com isso devem ser adotadas medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Medidas devem ser tomadas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Esses dados pessoais não podem ser utilizados para fins discriminatórios, ilícitos ou abusivos. Sendo assim os agentes de tratamento devem demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

Esses princípios servem como base para garantir a proteção dos dados pessoais dos indivíduos e a responsabilidade dos agentes que tratam esses dados.

2 ENTRAVES LEGISLATIVOS PARA A IMPLEMENTAÇÃO DA LGPD NAS EMPRESAS

A implementação da Lei Geral de Proteção de Dados (LGPD) nas empresas enfrenta alguns entraves legislativos que podem dificultar o processo de adequação.

A lei define dados pessoais como informações relacionadas a uma pessoa identificada ou identificável. Inclui desde informações óbvias, como nome e CPF, até dados mais sensíveis, como opiniões políticas e orientação sexual.

O tratamento de dados pessoais requer o consentimento do titular, exceto em situações específicas previstas na legislação. O consentimento deve ser livre, informado e inequívoco. A LGPD concede aos titulares dos dados uma série de direitos, incluindo o direito de acessar suas informações, corrigi-las, solicitar a exclusão, entre outros.

As organizações são responsáveis por adotar medidas técnicas e administrativas para garantir a proteção dos dados pessoais. Além disso, devem manter registros das operações de tratamento de dados e estar preparadas para prestar contas à Autoridade Nacional de Proteção de Dados (ANPD);

Em alguns casos, as organizações precisam nomear um Encarregado de Proteção de Dados, uma figura responsável por assegurar a conformidade com a LGPD.

A LGPD prevê sanções em caso de descumprimento das suas disposições, incluindo advertências, multas e a suspensão parcial ou total do banco de dados.

A ANPD (Autoridade Nacional de Proteção de Dados). É o órgão responsável pela fiscalização, regulamentação e aplicação da LGPD no Brasil. A ANPD atua para garantir que as empresas e instituições cumpram as normas relacionadas à coleta, tratamento, armazenamento e compartilhamento de dados pessoais, protegendo os direitos dos titulares desses dados e promovendo a privacidade e a segurança das informações.

Ela realiza o controle de infrações relacionadas à proteção de dados pessoais por meio de um processo que envolve monitoramento, fiscalização, e aplicação de sanções. Pode realizar auditorias e inspeções para verificar se as organizações estão cumprindo as exigências da LGPD.

Titulares de dados, consumidores ou outras partes interessadas podem relatar possíveis infrações. A ANPD, então, investiga as denúncias recebidas. Pode trabalhar em conjunto com outros órgãos reguladores e entidades governamentais para monitorar o cumprimento das normas de proteção de dados.

A ANPD possui um processo administrativo estruturado para lidar com infrações. Quando a ANPD identifica uma possível infração, ela notifica a organização envolvida para que apresente esclarecimentos e adote medidas corretivas, se necessário. Ela analisa as evidências e investiga a extensão e a gravidade da infração, avaliando o impacto nos direitos dos titulares de dados. A organização tem direito de defesa e pode apresentar justificativas e evidências para contestar a infração. Se a ANPD constatar que houve violação da LGPD, ela pode aplicar sanções, dependendo da gravidade e da reincidência.

A Advertência pode ser emitida com indicação de prazos para a adoção de medidas corretivas. Pode aplicar multas, que chegam a até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração. Em casos mais graves, a ANPD pode determinar o bloqueio ou a eliminação dos dados pessoais envolvidos na infração. E em situações extremas, a ANPD pode suspender temporariamente ou de forma definitiva as atividades de tratamento de dados da empresa.

Além de fiscalizar e penalizar, a ANPD também promove ações educativas e orienta as empresas e organizações sobre como se adequar às exigências da LGPD, prevenindo infrações e promovendo boas práticas de proteção de dados pessoais.

Como podemos observar no Art. 24 da Resolução CD/ANPD Nº 4, de 24 de fevereiro de 2023:

> Art. 24. A ANPD poderá aplicar ao infrator a sanção de suspensão parcial do funcionamento do banco de dados a que se refere a infração.
> § 1º A sanção de que trata o caput tem o fim de suspender o funcionamento de banco de dados em desacordo com a legislação de proteção de dados pessoais.

Caso a empresa não cumpra as exigências da LGPD, a ANPD pode interromper o uso de parte do banco de dados envolvido na infração. O objetivo dessa sanção é paralisar o tratamento de dados pessoais que não esteja sendo realizado de maneira adequada ou legal, até que a empresa ajuste suas operações e volte a seguir a legislação.

A transferência de dados pessoais para outros países só pode ocorrer em conformidade com a LGPD, garantindo a proteção dos dados mesmo fora do território brasileiro.

A LGPD é crucial para proteger a privacidade dos cidadãos e promover a responsabilidade no tratamento de dados pessoais. Ela se alinha com movimentos globais em prol da privacidade e segurança de dados, como o GDPR na União Europeia, estabelecendo um ambiente jurídico mais robusto para a gestão de informações pessoais no Brasil.

A implementação da Lei Geral de Proteção de Dados (LGPD) nas empresas implica custos associados a diversos aspectos, incluindo adaptação de processos, treinamento de pessoal, investimento em tecnologia, e revisão de políticas internas. Além disso, a necessidade legislativa é motivada pela obrigatoriedade de as empresas se adequarem às normas estabelecidas pela LGPD, evitando possíveis penalidades e garantindo o cumprimento das diretrizes relacionadas à privacidade e segurança dos dados pessoais.

As empresas precisam conduzir auditorias internas para identificar os dados pessoais que estão sendo processados e avaliar como esses dados são coletados, armazenados, processados e compartilhados.

Ajustes nos processos internos para garantir a conformidade com as disposições da LGPD, incluindo a revisão de políticas de privacidade, termos de uso e contratos com fornecedores.

Treinamento dos funcionários sobre as práticas adequadas de tratamento de dados pessoais, conscientizando-os sobre a importância da proteção da privacidade.

Investimento em tecnologias que auxiliem na proteção de dados, como sistemas de criptografia, firewalls, e soluções de gerenciamento de acesso. Isso pode envolver a contratação de serviços especializados em segurança da informação.

Algumas empresas podem precisar nomear um Encarregado de Proteção de Dados, responsável por garantir o cumprimento da LGPD e servir

como ponto de contato entre a empresa, os titulares de dados e a Autoridade Nacional de Proteção de Dados.

Empresas que tratam dados pessoais (coletam, armazenam, processam ou compartilham) são obrigadas a nomear um encarregado, independentemente do seu porte ou setor. O objetivo é garantir que todas as atividades relacionadas aos dados pessoais estejam em conformidade com a LGPD. Empresas que tratam dados sensíveis (como dados de saúde, biométricos, raciais, religiosos, etc.) ou que realizam tratamento em larga escala (grande volume de dados de muitas pessoas) têm a obrigatoriedade de nomear um encarregado, independentemente de seu porte. Nestes casos, a função do encarregado é ainda mais crítica, pois os riscos à privacidade e à proteção de dados são maiores.

A ANPD pode dispensar a obrigatoriedade do encarregado para microempresas, empresas de pequeno porte, startups e empresas de inovação, dependendo do risco e do volume de tratamento de dados. Essas organizações podem adotar procedimentos simplificados para adequação à LGPD, desde que não envolvam tratamento de alto risco ou grande volume de dados sensíveis. Ela emite regulamentações específicas para esses casos, e cabe à empresa verificar se se enquadra em tais exceções.

Revisão e adaptação de contratos com parceiros de negócios e fornecedores para garantir que eles também estejam em conformidade com a LGPD.

A LGPD exige conformidade legal, e o não cumprimento pode resultar em multas e outras sanções, aplicável pela ANPD. É fundamental que as empresas estejam cientes das responsabilidades legais impostas pela legislação para evitar consequências financeiras e danos à reputação.

A implementação da LGPD não é um evento único; é um processo contínuo que requer monitoramento constante das práticas de proteção de dados para garantir a conformidade ao longo do tempo.

É importante destacar sobre o assunto o que relata MALDONATO et al. (2019) em sua obra:

> Outra definição muito relevante constante da LGPD é a atinente ao próprio tratamento, assim entendido como toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Note-se que a conceituação é extremamente abrangente e inclui todas as operações relativas aos dados pessoais, desde sua coleta até o termino propriamente dito. No mais, é importante destacar que o mero armazenamento está inserido, por definição legal, como atividade de tratamento, de sorte que a simples posse de dados determina, por si só, a observância dos dispositivos legais. (MALDONADO et al., 2019, p16).

A LGPD caracteriza tratamento como qualquer operação realizada com dados pessoais, abrangendo uma ampla gama de atividades associadas ao manuseio dessas informações. É enfatizado que essa definição é abrangente e inclui todas as etapas relacionadas ao tratamento de dados pessoais, desde a coleta até a conclusão do processo. Além disso, destaca a relevância de observar que, de acordo com a definição legal, o simples armazenamento de dados já é considerado uma atividade de tratamento. Portanto, a mera posse ou guarda de dados implica automaticamente a necessidade de cumprir as disposições legais estabelecidas pela LGPD. Além disso essa abordagem reflete a crescente importância da privacidade e segurança dos dados pessoais na era digital, na qual as informações pessoais são frequentemente coletadas, processadas e utilizadas em diversos setores da sociedade.

A adaptação à LGPD envolve um investimento significativo, tanto em recursos financeiros quanto em esforços operacionais, mas é essencial para garantir a proteção da privacidade dos dados pessoais e evitar riscos legais associados à não conformidade.

A falta de profissionais especializados em LGPD pode ocasionar uma série de problemas nas empresas, neles se inclui:

Se uma empresa não estiver em conformidade com a LGPD, ela pode ser sujeita a diversas multas e penalidades. A LGPD estabelece um conjunto de sanções que podem ser aplicadas pela Autoridade Nacional de Proteção de

Dados (ANPD), nestes casos a falta de especialistas pode resultar em não conformidade, expondo a empresa a penalidades severas.

Os riscos à reputação, acontecem quando a violação de dados causa danos à reputação da empresa, levando à perda de confiança por parte de clientes e parceiros. Portanto profissionais especializados em LGPD são essenciais para garantir que as práticas de proteção de dados sejam adequadas, assim evitando que ocorra vazamentos destes na empresa.

A ineficiência na Implementação de políticas, quando a ausência de especialistas pode resultar em uma implementação inadequada das políticas de proteção de dados, o que pode comprometer a segurança das informações e dificultar a resposta a incidentes de violação de dados, ocasionando vários problemas a empresa.

A perda de Vantagem Competitiva, podem gerar danos a imagem pública, a perda de confiança dos consumidores, a redução de valor de marca, desconfiança de parceiros e investidores, dificuldade me atrair grandes talentos, o aumento da exposição a concorrentes, a negativação em rankings e avaliações públicas, a crescente pressão de órgãos reguladores e ONGs, dentre outras vantagens. As empresas que não aderem às melhores práticas de proteção de dados podem perder oportunidades de grandes negócios, especialmente em setores onde a conformidade com a LGPD é um requisito essencial para fazer negócios.

Os desafios na Gestão de Incidente, esses desafios podem impactar a eficácia na resposta a incidentes de segurança e na proteção dos dados pessoais caso houver uma violação de dados. A falta de profissionais qualificados pode dificultar a resposta rápida e eficaz, agravando as consequências do incidente e trazendo vários problemas. Isso mostra a importância de ter um plano robusto de gestão de incidentes, com processos bem definidos, equipes treinadas, e uma comunicação clara e eficaz, tanto interna quanto externamente.

Os problemas Jurídicos gerados pela falta de LGPD nas empresas são vários, vai além de gerar somente uma multa. Dentre eles ações civis por danos

morais e materiais, ações coletivas, processos administrativos, responsabilidade solidaria, injunções judiciais e a perda de credibilidade jurídica. Além disso a falta de conformidade gera processos judiciais tanto por parte de consumidores quanto de parceiros comerciais, resultando em custos legais bastante elevados. Esses problemas não tratam somente de custos financeiros, mas também podem causar danos irreparáveis a reputação da empresa podendo comprometer sua sustentabilidade a longo prazo.

Esses problemas mostram a importância de contar com profissionais qualificados em LGPD para garantir que a empresa esteja protegida e em conformidade com a legislação.

Investir no treinamento da equipe oferece diversos benefícios para a empresa, sendo o principal a redução dos riscos de incidentes relacionados a dados. Além disso, o treinamento contribui para garantir maior segurança e proteção dos dados pessoais, minimizando ameaças à segurança da informação. Com uma capacitação adequada, os colaboradores aprendem a utilizar o e-mail corporativo de forma correta, evitam acessar sites maliciosos e compreendem quais informações podem ou não ser compartilhadas.

Em BARBIERI (2019, p.58) mostra duas formas diferentes de abordar processos de análise e tomada de decisões em uma empresa:

> Uma empresa poderá iniciar a sua abordagem pela aplicação do modelo mais estruturado de entrevistas e reuniões e, depois, sugerir uma dinâmica para certos assuntos que mereçam uma discussão mais profunda. Também, poderá fazer o caminho inverso, iniciando com uma abordagem dinâmica motivadora que poderá ser detalhada, adiante, por um conjunto de entrevistas e pesquisas mais estruturadas. (BARBIERI, 2019, p58)

Ambas as abordagens visam adaptar a metodologia ao tipo de discussão e ao nível de profundidade necessário para resolver questões da empresa. Dada a relevância do treinamento sobre a LGPD, podemos citar alguns passos para conscientizar os colaboradores sobre a proteção de dados.

As empresas devem fornecer aos colaboradores uma definição clara e comum de privacidade no tratamento de informações pessoais. Essa definição deve ser parte integrante do treinamento e da conscientização sobre a LGPD,

garantindo que a coleta, processamento e proteção de dados sejam realizados de maneira uniforme e consistente por todos os funcionários da organização.

A implementação de um programa de conformidade com a LGPD é um processo complexo, exigindo a participação de diversos setores da empresa. Durante esse processo, é comum surgirem dúvidas e desafios internos. O treinamento da equipe é essencial para que todos compreendam os processos envolvidos na adequação à LGPD. Dessa forma, a empresa garante que os colaboradores estejam alinhados e comprometidos com o programa de conformidade.

O fator humano é uma das principais vulnerabilidades na proteção de dados, sendo as falhas humanas uma das maiores causas de ataques e incidentes. Muitas vezes, erros ocorrem porque os colaboradores não conhecem as políticas da empresa para o tratamento de dados pessoais. Por isso, o treinamento sobre a LGPD deve reforçar as políticas e procedimentos adotados, capacitando os funcionários a lidar corretamente com os dados e incentivando uma cultura de responsabilidade.

A organização de uma empresa para a implementação da LGPD deve ser munida com informações essenciais sobre proteção de dados e privacidade. A comunicação deve ser estratégica, com o propósito de gerar engajamento, e não apenas informar por informar. De acordo com Kyriazoglou, uma estratégia para um plano de comunicação, conscientização e treinamento podem incluir objetivos de privacidade que devem ser revisados constantemente e alinhados à estratégia da organização, dentre eles, identificar o público-alvo, tanto interno quanto externo, definir mensagens que levem em conta o público e os pontos a serem comunicados, escolher as ferramentas e atividades mais adequadas para o reporte (como relatórios mensais e anuais), elaborar um plano de ação voltado à conscientização, comunicação e treinamento, tornar o treinamento em privacidade obrigatório, vinculando-o à avaliação de desempenho, e implementar revisões periódicas através de auditorias internas e externas, visando a melhoria contínua.

A empresa deve garantir a atualização constante dos profissionais que integram a equipe de privacidade. Essa iniciativa abrange desde a assinatura de publicações especializadas até a participação em eventos do setor. O objetivo é manter a equipe de proteção de dados e privacidade sempre atualizada sobre as melhores práticas e tendências do mercado. Todo o conhecimento adquirido pelos membros da equipe de segurança será revertido em benefício da organização.

Conforme o autor MALDONATO et al. (2019) assevera em sua obra:

> Outro aspecto que deve ser considerado é a periodicidade com que os colaboradores devem ser expostos ao treinamento básico de proteção de dados e privacidade. Além do período arbitrado pela própria organização, existem alguns drivers de mudança que podem demandar uma nova rodada de treinamento básico junto aos colaboradores, tais como: mudanças na estratégia, e consequentemente na política, indicadores, calendário de certificação da organização etc. (MALDONADO et al., 2019, p126).

A proteção de dados deve ser um tema presente em toda a empresa, desde a alta administração até as operações diárias. É necessário estabelecer um processo de aprendizado contínuo, criando uma cultura organizacional em que os colaboradores compreendam a importância de proteger os dados. A empresa deve guiar as ações diárias da organização, promovendo alinhamento e engajamento da equipe com esse propósito.

Cada colaborador deve entender claramente o propósito do trabalho que realiza diariamente. Embora as tarefas possam parecer simples, elas fazem parte de um conjunto maior que contribui para o objetivo da organização. Isso também se aplica às questões de privacidade, que não são responsabilidade exclusiva do DPO e sua equipe, mas de todos os membros da organização. A proteção de dados e privacidade deve ser uma responsabilidade coletiva.

Portanto, a implementação de novos modelos de gestão e negócios precisa envolver todos os funcionários, baseando-se em uma cultura sólida de proteção de dados. Embora possa ser desafiador garantir que todos compreendam os impactos de uma má administração de dados pessoais, treinamentos específicos podem conscientizar a equipe sobre a importância de

tratar os dados com responsabilidade, ética e transparência. O investimento em educação e treinamento transforma a organização em todas as suas esferas.

3 BARREIRAS QUE AS EMPRESAS COLOCAM PARA A IMPLEMENTAÇÃO DA LGPD

A implementação da LGPD (Lei Geral de Proteção de Dados) nas empresas pode encontrar diversas barreiras. Algumas das mais comuns incluem a falta de comunicação e conscientização onde muitas empresas têm dificuldade em compreender completamente as exigências da LGPD. Isso inclui tanto a alta administração quanto os colaboradores em geral, que podem não estar cientes da importância de proteger dados pessoais ou de como a lei impacta suas funções diárias.

A resistência à mudança é outro aspecto em que as empresas apresentam ao implementar a LGPD, pois ela exige mudanças culturais e operacionais. A resistência interna a essas mudanças, principalmente de setores que veem a adequação como uma burocracia extra ou um obstáculo à eficiência, pode retardar o processo.

A conformidade com a LGPD pode gerar custos elevados, como a necessidade de contratar consultorias especializadas, investir em infraestrutura tecnológica e realizar treinamentos. Pequenas e médias empresas, em particular, podem ver essas despesas como um fardo financeiro.

Esses custos dependem de vários fatores, dependendo da empresa, pode variar por causa da quantidade de cadastros envolvidos, podem ser pelo porte que são Microempresa, empresa de pequeno, médio ou grande porte, sendo a classificação definida, quer pela quantidade de empregados ou pelo faturamento, dependendo do órgão, como a ANVISA, IBGE ou outros. Ou pelo ramo que são operadoras de planos de saúde, instituição financeira, indústria, comércio, escritórios de advocacia entre outros. Contudo, implantar a LGPD

em uma empresa depende de inúmeros fatores, pois se trata de um serviço personalizado. (LEITE, 2021).

Para que seja dado cumprimento ao disposto na legislação, é necessário que se designe um representante para adequação da empresa aos moldes da lei, e criação de processos para que seja assegurado tal direito.

Um exemplo pertinente, é a nomeação de um encarregado para a proteção de dados chamado de DPO (Data Protection Officer) que não precisa ser uma dor de cabeça para a sua empresa. Com o serviço de DPO as a Service, você contrata um especialista em privacidade de dados para ocupar a função, garantindo conformidade com um ponto fundamental da LGPD. O DPO é um escritório jurídico que trata de assuntos de privacidade e atende sobre os assuntos que trata a lei. Esse serviço pode custar entre R$10.000 a R$20.000. A função do DPO é um ponto de comunicação e entrega sendo controlador e autoridade ou controlador e titular. (BOHRER, 2023)

De acordo a art. 38 da Lei Geral de Proteção de Dados Pessoais:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O DPO pode ser contratado em dois momentos. Contrata-se para fazer um programa de adequação seguindo os laços de mapeamento, políticas, adequação de documentos existentes, identificação de risco, plano de ação. Depois de implementado, o trabalho do DPO é manter o programa atualizado. O valor médio para implementação de um programa vai de R$80.000 a

R$100.000. Para empresas de pequeno e médio porte. A remuneração do DPO pode variar entre R$16.000 até R$35.000. (BOHRER, 2023)

Empresas com processos complexos de coleta e tratamento de dados podem encontrar dificuldades para mapear esses fluxos de dados e identificar onde estão as vulnerabilidades ou os pontos de adequação à LGPD.

Sistemas de TI desatualizados ou mal integrados podem dificultar a implementação de medidas de segurança, controle de acesso e anonimização de dados exigidos pela LGPD. Além disso, pode ser necessário um grande investimento em novas tecnologias para estar em conformidade.

A ausência de profissionais com conhecimento técnico e jurídico sobre a LGPD, como Data Protection Officers (DPOs), pode ser uma barreira significativa. Empresas sem equipes qualificadas enfrentam maiores dificuldades para interpretar e implementar corretamente a lei.

Quando dados são armazenados de forma descentralizada ou por diferentes setores da empresa, pode ser desafiador garantir uma governança de dados eficiente. Isso cria barreiras para mapear, controlar e proteger adequadamente as informações.

A implementação da LGPD pode ser vista como algo que atrapalha as operações diárias, principalmente em ambientes empresariais focados em prazos apertados e produtividade, onde dedicar tempo para a adequação à lei é visto como um obstáculo.

Algumas empresas subestimam as consequências legais e reputacionais de não estarem em conformidade com a LGPD. Isso pode resultar na priorização inadequada da implementação, ou na percepção de que os riscos de sanções ou multas são baixos.

Se a liderança da empresa não está comprometida com a implementação da LGPD, as iniciativas podem falhar por falta de apoio necessário em termos de recursos, orçamento e prioridade estratégica.

Essas barreiras podem ser superadas com planejamento adequado, engajamento dos colaboradores e um compromisso estratégico da liderança para implementar a conformidade de forma eficaz.

CONCLUSÃO

A partir do que foi desenvolvido ao longo deste artigo a LGPD é um marco regulatório crucial para a proteção de dados pessoais no Brasil. Ela estabelece diretrizes claras para o tratamento de informações, impondo responsabilidades e obrigações às empresas, independentemente do seu porte ou setor de atuação. A aplicabilidade da LGPD nas empresas brasileiras visa garantir que os direitos dos titulares de dados sejam respeitados, promovendo a privacidade, a segurança e a transparência no uso de informações pessoais. A proposta deste trabalho foi um estudo sobre os impactos da implementação da LGPD em ambientes corporativos. Além do mais analisa as possíveis estratégias que uma empresa pode adotar em relação aos dados coletados de seus clientes, além de identificar formas de protegê-los. Destaca-se a importância da legislação para as empresas e para a sociedade, proporcionando maior clareza sobre as novas regulamentações de proteção de dados.

A LGPD exige que as empresas adotem boas práticas e implementem medidas de segurança adequadas para proteger os dados que coletam e processam. Isso inclui a nomeação de um Encarregado de Proteção de Dados (DPO), a criação de políticas de privacidade, e a realização de auditorias e avaliações de impacto. Para as organizações que não cumprem essas normas, a Autoridade Nacional de Proteção de Dados (ANPD) é responsável por fiscalizar, monitorar e aplicar sanções, que podem variar de advertências a multas significativas e até mesmo à suspensão das atividades de tratamento de dados.

Portanto, a LGPD não apenas assegura os direitos dos cidadãos em um ambiente cada vez mais digitalizado, mas também impulsiona as empresas a se adaptarem a um cenário de conformidade e responsabilidade. Aquelas que se adequarem às exigências da LGPD não só evitam penalidades, mas também ganham credibilidade e confiança dos consumidores, consolidando sua posição no mercado e fortalecendo a cultura de privacidade e segurança de dados no país.

THE GENERAL DATA PROTECTION LAW AND ITS APPLICABILITY TO BRAZILIAN COMPANIES

ABSTRACT

Law No. 13,709/2018, known as the General Data Protection Law (LGPD), is a legal framework in Brazil that aims to protect the privacy and security of citizens' personal data. Inspired by the General Data Protection Regulation (GDPR) of the European Union, the LGPD establishes rules for the processing of data by public and private organizations in Brazil, applying to activities carried out in the country or related to services and goods offered to people in the country. Brazil. The law requires companies to adopt transparent and responsible data management practices, giving individuals greater control over their information, to strengthen trust in business relationships and protect individual rights. As well as the importance of an LGPD specialist working in a company. The study highlights the challenges faced by companies in adapting to the LGPD, which, despite the difficulties, is mandatory. The article also addresses the transition of the business sector in the face of the requirements imposed by law. In this research, study methodology and in-depth research were used on companies' difficulties with the implementation of LGPD in companies, with doctrinal and legislative analyzes on the right to privacy of personal data.

Keywords: Companies. Difficulties. Implementation. Protection. Privacy.

REFERÊNCIAS

BARBIERE, Carlos. Governança de Dados: Práticas, Conceitos e Novos Caminhos, Rio de Janeiro: Alta Books, 2019.

BERTOLAZI A. DPO as a service: o que é? Como funciona e quanto custa? Disponível em: https://rasteksolucoes.com.br/2022/05/dpo-as-a-service-o-que-e-como-funciona-e-quanto-custa/#:~:text=Plano%20LGPD%20Gerenciada:%20adequa%C3%A7%C3%A3o%20LGPD,RS%20(Assesspro%2DRS). Acesso em: 06 de Out. 2024

BOHRER J. Quanto custa uma acessoria de LGPD, Disponível em: https://www.implementandoalgpd.com.br/ blog/quanto-custa-uma-consultoria-delgpd/#:~:text=Para%20esse%20formato%2C%20o%20valor,relacionados%20%C3%A0%20LGPD%20clicando%20AQUI! Acesso em: 06 de Out. 2024.

BORELLI, Alessandra; GUTIERREZ, Andriei; LIMA CARVALHO CÉSAR, Caio; ARANTES RIOJA, Camila; JIMENES VALE, Camilla; ALVES MOTA, Fabricio; CHAVES PRADO FERNANDO, Luis; BLUM OPICE, Renato; VAINZOF, Rony; MALDONADO NÓBREGA, Viviane. Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia. 2. Ed. São PAULO, 2019.

BRASIL, Constituição (1988). *Constituição da República federativa do Brasil*. Brasília DF: senado,1988.

BRASIL, Lei Nº 13.709, 14 de agosto de 2018. *Lei Geral de Proteção de Dados*.

BRASIL, Resolução CD/ANPD Nº 4, de fevereiro de 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf Acesso em 22 de Set. de 2024.

FERREIRA, V. R., Falcão, B. N., & Bizzocchi, L. J. J. (2022). Sociedade digital, privacidade e proteção de dados: uma análise dos impactos da LGPD no Direito do Trabalho.Conjecturas,22(2), 219-241. DOI: https://doi.org/10.53660/CONJ-645-614. Acesso em: 15 de Set. 2024.

FREITAS, F; ARAUJO, M. Politicas De Segurança Da Informação: Guia prático para elaboração e implementação. 2ed. Rio de Janeiro: Ciência Moderna LTDA, 2008.

GOMES, Bruna. Treinamento sobre LGPD: como conscientizar os colaboradores. Disponível em: https://www.contacta.com.br/blog/treinamento-sobre-lgpd-como-conscientizar-os-colaboradores. Acesso em: 22 de Set. 2024.

INTUIX. As penalidades para as empresas que não se adequarem. Disponível em: https://intuix.com.br/dpo-o-profissional-necessario-para-adequacao-a-lgpd/. Acesso em: 06 de Out de 2024.

LIMA CARLOS, Adriano; PRATA, Alexandre; VIEIRA, Claudinei; MONTANARO, Domingo; VIEIRA CARVALHO LÚCIA, Elba; PALHARES, Felipe; JUNIOR GIOVANNINI LENINE, Josmar; SILVA OLIVEIRA APARECIDO, Sergio; MALDONARO NÓBREGA, Viviane; CAPANEMA ARANHA, Walter; JUNIOR ALMEIDA UMPIERRES, Washington. LGPD Lei Geral de Proteção de Dados: Manual de Implementação. São Paulo, 2019.

MACIEL, Rafael Fernandes. Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18). 1. ed. Goiânia: RM Digital Education, 2019.

MARTINS, Romulo. Treinamento LGPD: entenda a importância de capacitar os colaboradores. Disponível em: https://www.gupy.io/blog/treinamento-lgpd. Acesso em 22 de Set. 2024.

MOREIRA, Carolina Vasques; GARCÉS, Lina. Diretrizes propostas para exibição de termos de uso e políticas de privacidade com base nos requisitos da LGPD e em boas práticas de design de experiência do usuário. Revista dos Trabalhos de Iniciação Científica, 2022. Disponível em: https://periodicos.unifei.edu.br/index.php/rtic/article/view/200. DOI: https://doi.org/10.29327/1307153.1-151. Acesso em: 15 de Set. 2024.

NOVAKOSKI, A. L. M., & Naspolini, S. H. D. F. (2020). Responsabilidade civil na LGPD: problemas e soluções. Conpedi Law Review, Florianópolis, 6(1), 158-174. Disponível em: 382457955.pdf (core.ac.uk). Acesso em: 16 de Set. 2024.

PAULA NETO, Juliomar de et al. A tutela dos dados pessoais sensíveis pelo ordenamento jurídico: uma análise do dever de segurança institucional no setor público sob a óptica da LGPD. 2021. Disponível em: https://repositorio.ufu.br/handle/123456789/33169 DOI: http://orcid.org/0000-0002-6491-9345. Acesso em: 18 de Set. 2024.

REIS, Rafael. Os desafios da implementação em empresas brasileiras. Disponível em: https://www.direitoempresarial.com.br/os-desafios-da-implementacao-da-lgpd-em-empresas-brasileiras#:~:text=Falta%20de%20investimento%20em%20ciberseguran%C3%A7a,privacidade%20e%20vazamentos%20de%20informa%C3%A7%C3%B5es. Acesso em 22 de Set. de 2024.

STACCHINI, I. S. (2022). Proteção de dados pessoais no campo do direito penal à luz da lei geral de proteção de dados (lei Nº 13.709/2018). DOI: Proteçhttps://dspace.mackenzie.br/items/ae4b1f88-f3b2-4430-9f68-b61668d4a260/fullão de dados pessoais no campo do direito penal à luz da lei geral de proteção de dados (lei Nº 13.709/2018) (mackenzie.br) Disponível em: https://dspace.mackenzie.br/handle/10899/32639 . Acesso em: 15 de Set. 2024.