UNIVERSIDADE SÃO JUDAS
CURSO DE DIREITO
TRABALHO DE CONCLUSÃO DE CURSO II

NOME: MARCOS HENRIQUE BANDEIRA DOS SANTOS TINOCO
RA: 819161261

LGPD - IMPORTÂNCIA DOS DADOS PESSOAIS E O CENÁRIO DE SEGURANÇA JURÍDICA.

SÃO PAULO

2O23

NOME: MARCOS HENRIQUE BANDEIRA DOS SANTOS TINOCO

RA: 819161261

LGPD - IMPORTÂNCIA DOS DADOS PESSOAIS E O CENÁRIO DE SEGURANÇA JURÍDICA.

Trabalho de Conclusão de Curso apresentado à coordenação do Curso de Direito da Universidade São Judas, como requisito final para obtenção do diploma de Bacharel em Direito.

PROFESSOR ORIENTADOR: Carlos Henrique Raguza

Aprovado em: __/__/____.

Prof. Orientador. Dr. Carlos Henrique Raguza
UNIVERSIDADE SÃO JUDAS

Prof Me.
UNIVERSIDADE SÃO JUDAS

Prof Me.
UNIVERSIDADE SÃO JUDAS

RESUMO:

A pesquisa abordou a eficácia da Lei Geral de Proteção de Dados (LGPD) na garantia da segurança jurídica no contexto do tratamento de dados pessoais no Brasil. Explorando princípios, direitos dos titulares e desafios de implementação, a análise destaca a importância da legislação na promoção da privacidade. Comparando com outras leis internacionais, examinando o papel da ANPD e considerando desafios emergentes. A conclusão aponta para a necessidade contínua de adaptação e conscientização. Sugere-se investigar o impacto econômico, aprimorar a eficácia da ANPD e explorar setores específicos para orientar futuras pesquisas e melhorias legislativas.

Palavras-Chave: LGPD, Proteção de Dados, Segurança Jurídica, Privacidade, Autoridade Nacional de Proteção de Dados (ANPD), Desafios na Implementação, Conformidade Legal, Direitos dos Titulares de Dados, Comparação Internacional, Impacto Econômico, Cultura Organizacional, Tecnologias Emergentes, Conscientização Pública, Ética em Dados, Relações Internacionais, Privacidade por Design, Saúde Digital, Inovação Tecnológica, Práticas de Privacidade.

ABSTRACT

The research addressed the effectiveness of the General Data Protection Law (LGPD) in ensuring legal security in the context of personal data processing in Brazil. Exploring principles, rights of data subjects, and implementation challenges, the analysis highlights the significance of the legislation in promoting privacy. By comparing it with other international laws, examining the role of the National Data Protection Authority (ANPD), and considering emerging challenges. The conclusion points to the ongoing need for adaptation and awareness. The suggestion includes investigating economic impact, enhancing the effectiveness of the ANPD, and exploring specific sectors to guide future research and legislative improvements.

Keywords: LGPD, Data Protection, Legal Security, Privacy, National Data Protection Authority (ANPD), Implementation Challenges, Legal Compliance, Data Subject Rights, International Comparison, Economic Impact, Organizational Culture, Emerging Technologies, Public Awareness, Ethics in Data, International Relations, Privacy by Design, Digital Health, Technological Innovation, Privacy Practices.

LISTA DE SIGLAS E ABREVIATURAS

ANPD	Autoridade Nacional de Proteção de Dados
Art.	Artigo
CCPA	California Consumer Privacy Act
C/C.	Combinado com
CEO	Chief Executive Officer
CETIC	Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
CF.	Constituição Federal
CPC	Código de Processo Civil
DPIA	Avaliação de Impacto à Proteção de Dados
DPO	Data Protection Officer
EC.	Emenda Constitucional
GDPR	Regulamento Geral de Proteção de Dados da União Europeia
IPEA	Instituto de Pesquisa Econômica Aplicada
LGPD	Lei Geral de Proteção de Dados Pessoais
PIPEDA	Lei de Privacidade do Consumidor do Canadá
PL	Projeto de Lei
PLS	Projeto de Lei do Senado
TI	Tecnologia da Informação
USP	Universidade de São Paulo

SUMÁRIO

Introdução ……..……..……..……08

a. Contextualização da LGPD no cenário brasileiro……..08

b. Declaração do problema: a necessidade de garantir segurança jurídica na implementação da LGPD……09

1. **Princípios Norteadores**……15

1.1. Fundamentos da LGPD: princípios, direitos dos titulares, obrigações das organizações
……15

1.2. Comparação com outras leis de proteção de dados em nível internacional……16

1.3. Importância da segurança jurídica na proteção de dados pessoais……...17

2**. Desenvolvimento da LGPD no Brasil**……..19

2.1. Histórico da criação da LGPD……19

2.2. Papel e atribuições da Autoridade Nacional de Proteção de Dados (ANPD).....20

3. **Desafios na Implementação da LGPD**……22

3.1. Barreiras organizacionais: custos, treinamento de pessoal, adaptação de processo.....……22

3.2. Desafios tecnológicos: conformidade de sistemas, segurança cibernética……...24

3.3. Aspectos culturais: conscientização e mudança de cultura organizacional……..25

4. **Segurança Jurídica na Prática**……..26

4.1. Como funciona na prática……..27

4.2. Números da proteção de dados vêm crescendo no país…….28

5. **Perspectivas Futuras**……...31

5.1. Tendências na regulamentação de proteção de dados……..31

5.2. Desafios emergentes na segurança jurídica……...32

5.3. Possíveis aprimoramentos na LGPD……34

Conclusão……35

Recapitulação dos principais pontos discutidos…….35

Conclusões sobre a eficácia da LGPD na garantia da segurança jurídica……37

Sugestões para futuras pesquisas e aprimoramentos na legislação…….....38

Referências Bibliográficas …….....…….....…….39

- **INTRODUÇÃO À PROBLEMÁTICA**

“Com o advento da Lei nº 13.709/2018, isto é, a Lei Geral de Proteção de Dados Pessoais, ficou estabelecido as regras para a coleta, uso, armazenamento e compartilhamento de dados pessoais de indivíduos. A lei entrou em vigor em setembro de 2020 e tem como objetivo proteger a privacidade e os direitos dos titulares de dados pessoais. Trouxe consigo alguns desafios para as empresas que precisaram se adaptar para garantir a conformidade com a nova lei.

A LGPD é uma lei moderna e alinhada com as principais leis internacionais de proteção de dados, traz no seu escopo muitas tendências internacionais. Sua implementação é fundamental para garantir a privacidade dos dados pessoais dos cidadãos brasileiros, visando promover a segurança jurídica nas relações interpessoais.

A de se compreender se tal estrutura pode trazer diversos benefícios. E se trazem quais seriam.

De acordo com Miriam Wimmer, Chefe da Divisão de Estudos e Pesquisas do Instituto de Pesquisa Econômica Aplicada (Ipea):

> "A LGPD representa um marco na proteção da privacidade e dos dados pessoais no Brasil. Ela estabelece regras claras para a coleta, uso e compartilhamento de dados, garantindo maior transparência e controle para os titulares desses dados.(1)"

Porém, a simples implementação da lei não garante sua aplicação e precisa de algumas especificações para começo de conversa

Para listar os rumos da LGPD pode-se dizer que o consentimento explícito do titular dos dados para o seu uso, o direito do titular de acessar, corrigir e excluir seus dados, a exigência de medidas de segurança adequadas para proteger os dados e a responsabilização das empresas e organizações que violarem a lei. Vemos que a aplicação vai garantir a privacidade e a proteção dos dados pessoais da sociedade brasileira, alavancando impactos significativos na forma como as empresas e organizações lidam com os dados pessoais de sua base de clientes e colaboradores.

A questão toda aqui é o fato das empresas ainda não estarem preparadas para cumprir as exigências da lei, o que pode resultar em multas e perda de confiança dos clientes.

Neste diapasão, podemos apontar a seguinte questão a respondida por esta pesquisa: Quais os principais desafios que as empresas brasileiras enfrentam para se adequar à LGPD e quais impactos que essas mudanças vão gerar na relação com seus clientes?

Segundo Dayana Caroline Costa, que é especialista em Direito Digital, e também membro da Comissão de Direito Digital:

> (2)"Os dados pessoais são hoje um dos maiores ativos da sociedade mundial, impactando diretamente na definição de modelos de negócio e criação de oportunidades. O mundo todo assiste a um fenômeno progressivo de enormes quantidades de dados pessoais de cidadãos serem coletados, processados e tratados deliberadamente por empresas e instituições públicas e privadas (...).(2)"

Se mesmo após implementação de uma lei, as mudanças na prática não passam a ser notadas, nem minimamente, por que então há essa ineficácia de normas?

Existem diversas razões pelas quais as normas brasileiras podem ser consideradas ineficazes em alguns casos. Algumas das principais razões incluem:

1.1 - Muitas vezes, as normas são ignoradas ou descumpridas; 1.2 Complexidade excessiva: Algumas normas podem ser complexas e/ou difíceis de entender que acabam sendo ignoradas ou mal interpretadas; 1.3 Falta de recursos: normas que aparentam ser boas em teoria, podem carecer de recursos para implementá-las adequadamente, desde recursos financeiros, humanos ou até tecnológicos; 1.4 Interesses conflitantes: como por exemplo uma empresa pode estar mais interessada em maximizar seus lucros do que em cumprir as normas ambientais ou de segurança no trabalho; 1.5 Falta de atualização: As normas podem se tornar obsoletas ao longo do tempo, tornando-se ineficazes ou até mesmo contraproducentes.

Para ficar mais claro, a eficácia das normas no Brasil depende de uma série de fatores, desde a sua aplicação prática, sua clareza e simplicidade, a disponibilidade de recursos para implementá-las e a capacidade de utilizá-las regularmente.

Sob as palavras da Ana Frazão, ao JOTA, ressalta-se que:

> (3) A razão da preocupação especial com os dados sensíveis diz respeito a assegurar não apenas a privacidade, mas também que tais dados não possam ser utilizados contra os titulares, trazendo-lhes restrições ao acesso a bens, serviços e mesmo ao exercício de direitos. Basta imaginarmos o potencial dos dados biométricos, como imagens faciais ou impressões digitais, para se ter conhecimento de características físicas, psicológicas e comportamentais de um indivíduo. (3)

E assim será pesquisado a melhor aplicação da norma, descobrindo quais são os mecanismos e artifícios que são utilizados. Se possuem legalidade em seus atos, ou não.

> A principal problemática abordada terá como objetivo analisar os impactos da LGPD no cenário jurídico e a falta de importância que tem sido adotada para o tratamento de dados pessoais, quais medidas foram implementadas e o que falta fazer e quais os métodos e caminhos que é comum ante ocorrido. Para que assim seja elucidado e compreendido tal situação.

Qual o perigo de acontecer um vazamento de dados pessoais por parte de empresas e organizações? A presente pesquisa tem como objetivo buscando identificar os principais fatores que levam à ocorrência de vazamentos e as medidas que podem ser adotadas para prevenir e combater esse tipo de prática ilegal.

Outra teoria que será discutida é: como está sendo aplicado a lei de proteção de dados e como isso se dá no âmbito judicial, isto é, pelos juízes e tribunais?

No tocante ao direito à proteção de dados pessoais, afirma-se que:

> (4) Embora não se trate de direito absoluto, o direito à proteção dos dados, especialmente na medida de sua conexão com a dignidade humana, revela-se como um direito bastante sensível, tanto mais sensível quanto mais a sua restrição afeta a intimidade e pode implicar violação da dignidade da pessoa humana. (4)

Uma discussão que ocorre é se há relação de vazamento de dados de uma empresa com golpes de ladrões e ligações indesejadas? O que será um tema abordado, já que abre espaço para entender qual real importância da norma e ocorrer um ideal funcionamento da mesma.

Quais dados pessoais a maioria das empresas utilizam e para qual finalidade? Nesse sentido, será importante compreender os riscos associados à autorização da coleta de dados.

Atrelado ao conceito de dados pessoais, o tratamento de dados é o procedimento que envolve a utilização destes dados, tais como a coleta, classificação, utilização, processamento, armazenamento, compartilhamento, transferência, eliminação e outras funções relativas a esse tratamento. Patrícia Peck Pinheiro (2018, p. 45) defende que a opção do legislador em pontuar todos os principais termos no contexto dos dados pessoais é extremamente importante, pois diminui quaisquer problemas de conceituação ou categorização que as informações coletadas sofriam, dessa maneira(5) "a partir da LGPD, passa a ficar claro é apontável o que é ou não dado pessoal, assim como todos os processos, as técnicas ou os procedimentos relativos ao tratamento de dados". “Destarte, pode-se afirmar que o Brasil adotou um conceito expansionista do dado pessoal "pelo qual não somente a informação relativa a pessoa diretamente identificada estará protegida pela Lei, mas também qualquer informação que possa - têm o potencial de - tornar a pessoa identificável"(5) .

Como uma empresa pode se proteger de ter seus dados vazados por hackers? Investigar a relação entre a estrutura empresarial, e se pode haver medidas para bloquear/interromper e ao mesmo manter a segurança dos dados.

Quais as diferenças e semelhanças da LGPD com a GDPR? Analisar essa relação é crucial para entender se tem sido eficaz sua aplicação.

A presente pesquisa científica tem por sua finalidade preencher as lacunas que contém em face dos mecanismos eficazes no combate a ataques hacker e cibernéticos que vazam dados pessoais de grandes bases de dados das empresas bancárias.

O vazamento de dados pessoais de empresas pode ter consequências graves para a privacidade e segurança dos indivíduos envolvidos. Algumas das consequências que posso elencar são:

Roubo de identidade: Com maior grau de periculosidade quando há vazamento de dados pessoais. Com informações como nome completo, endereço, data de nascimento, CPF e etc. Os criminosos podem se passar pela vítima para obter acesso a contas bancárias, cartões de crédito e outros bens pessoais, e efetivar compras.

Fraude financeira: Com informações pessoais, os criminosos podem realizar fraudes financeiras em nome da vítima, fazendo compras e empréstimos, abrindo contas e aplicando para crédito, gerando um prejuízo financeiro significativo.

Extorsão e chantagem: Quando as informações vazadas incluem fotos, vídeos, conversas ou outras informações pessoais sensíveis, os criminosos podem usá-las para extorsão ou chantagem.

Spam e phishing: Algo recorrente, vindo de pessoas má intencionadas que mandam spam e phishing para o e-mail ou mensagem de texto de um destinatário, tentando convencê-lo a clicar em links ou fornecer mais informações pessoais.

Prejuízo à reputação: Incluindo danos à sua reputação e imagem pública, o que pode afetar suas operações e a confiança de seus clientes.

Enfim, para deixar mais claro, o vazamento de dados pessoais de empresas é uma ameaça real. Pode acarretar consequências graves para a privacidade e segurança das pessoas envolvidas. Medidas devem ser tomadas e aplicadas por empresas com a intenção de proteger os dados de pessoas que eles tenham em seu banco de dados. No caso de acontecer o vazamento, elas devem notificar imediatamente as pessoas afetadas. É preciso estar atento aos possíveis golpes/fraudes e spam.

Seguindo esse raciocínio, veremos se as empresas (públicas ou privadas) devem tomar medidas para se protegerem de hackers que tentam roubar dados. Então vamos ver algumas dicas importantes:

1.1 Fortalecer a segurança da rede: Ao garantir que sua rede esteja protegida por senhas fortes e até verificação de dois fatores, firewalls, sistemas de detecção de intrusos e criptografia de dados. Também é importante manter os softwares e sistemas atualizados para corrigir vulnerabilidades conhecidas; 1.2 Educar os funcionários: Os funcionários são a primeira linha de defesa contra hackers. Eles devem ser treinados sobre como reconhecer e evitar ameaças de segurança, como phishing e ataques de engenharia social; 1.3 Restringir o acesso aos dados: As empresas devem limitar o acesso aos dados somente a funcionários que precisam deles para realizar suas funções, e estes devem ter uma autenticação de dois fatores para acessá-los; 1.4 Fazer backups regulares: É importante fazer backup regular dos dados para garantir que a informação crítica esteja disponível no caso de um ataque de ransomware ou outro evento de segurança; 1.5 Realizar testes de segurança: As empresas devem testar regularmente suas defesas de segurança por meio de testes de penetração e outras avaliações de segurança para identificar vulnerabilidades e corrigi-las antes que um hacker às aproveite; 1.6 Estabeleça um plano de resposta a incidentes: As empresas devem ter um plano de resposta a incidentes em vigor para reagir rapidamente a um ataque e minimizar os danos; 1.7 Contrate especialistas em segurança: É importante que as empresas contratem especialistas em segurança de TI para avaliar continuamente sua segurança e implementar medidas adequadas de proteção de dados.

Em resumo, as empresas devem implementar uma série de medidas de segurança para proteger seus dados e minimizar o risco de vazamento de dados por hackers. Isso inclui fortalecer a segurança da rede, educar os funcionários, restringir o acesso aos dados, fazer backups regulares, testar a segurança regularmente, ter um plano de resposta a incidentes e contratar especialistas em segurança.

Ao pesquisar o assunto e conversar com pessoas que o conhecem, concluímos que existe uma correlação direta entre violações de dados corporativos e um aumento de golpes de ladrões e chamadas de spam. Quando os dados são

vazados, como de uma agência governamental, os criminosos podem usar os dados para realizar atividades fraudulentas, como phishing, roubo de identidade e extorsão.

Por exemplo, se um hacker acessar informações pessoais de clientes de uma empresa, tipo de um banco ou algo do tipo, seja o nome completo, endereço, número de telefone e endereço de e-mail, ele pode usar esses dados para fazer ligações tentando convencer o público a fornecer informações adicionais, das quais podem ser senhas, números de cartão de crédito e outras informações financeiras.

Além disso, eles podem estar mais dispostos a usar esse tempo para fazer ligações que nunca gostaríamos de receber, na tentativa de cometer um golpe, para que os criminosos se façam passar por representantes de empresas respeitáveis, solicitem informações pessoais ou financeiras ou ameacem penalidades se as informações forem reveladas. não fornecido.

Portanto, providências adequadas na proteção dos dados pessoais podem reduzir e conter estes criminosos. Caso eles consigam, é preciso notificar imediatamente as pessoas afetadas.

A presente pesquisa explorará a legislação vigente no Brasil, inclusive, mas não se limitando à Lei Geral de Proteção de Dados Pessoais (“LGPD” -LEI Nº 13.709, DE 14 DE AGOSTO DE 2018); o Marco Civil da Internet (Lei n° 12.965/2014); a Convenção sobre o Crime Cibernético firmada pela República Federativa do Brasil, em Budapeste (Decreto nº 11.491/2023);

Além disso, o presente trabalho buscará discutir o papel das empresas, organizações, magistrados e do Estado na promoção da segurança e proteção dos dados das pessoas coletadas e armazenadas em seus bancos de dados.

Ante ao exposto, conclui-se que o presente trabalho visa uma análise crítica através de pesquisas e doutrinas quanto ao tema a fim de resguardar a proteção dos dados pessoais no ambiente digital. Vejamos os pilares da LGPD adiante”.

• Princípios Norteadores

1.1. Fundamentos da LGPD:

Finalidade: Os dados pessoais devem ser coletados para propósitos específicos e legítimos, sendo vedado o tratamento posterior de maneira incompatível com essas finalidades. **Adequação**: O tratamento de dados deve ser adequado ao propósito para o qual foram coletados, evitando excessos. **Necessidade**: A coleta de dados deve ser limitada ao mínimo necessário para alcançar os propósitos para os quais são processados. **Transparência**: As organizações devem fornecer informações claras e acessíveis sobre o tratamento de dados, garantindo a transparência aos titulares.

Direitos dos Titulares que seriam o **Direito de Acesso**: Os titulares têm o direito de obter informações claras sobre se seus dados estão sendo processados e, em caso afirmativo, acesso a esses dados. **Direito de Retificação**: Titulares podem corrigir dados imprecisos ou incompletos que as organizações possuam sobre eles. **Direito à Exclusão** (ou "Direito ao Esquecimento"): Os titulares podem solicitar a exclusão de seus dados pessoais, sob certas condições. **Direito à Portabilidade**: Em alguns casos, os titulares têm o direito de receber os dados pessoais que forneceram a uma organização em um formato estruturado. Dentre outros.

Obrigações das Organizações são criar uma certa **Segurança dos Dados**: As organizações são responsáveis por implementar medidas técnicas e organizacionais para garantir a segurança dos dados pessoais. **Notificação de Incidentes**: Em caso de violações de segurança que possam resultar em riscos para os titulares, as organizações devem notificar prontamente a Autoridade Nacional de Proteção de Dados (ANPD) e, em alguns casos, os próprios titulares. **Consentimento**: Em muitos casos, o tratamento de dados requer o consentimento do titular. As organizações devem obter esse consentimento de maneira clara e específica para cada finalidade. Esses fundamentos da LGPD são essenciais para garantir que o tratamento de dados seja ético, transparente e em conformidade com os direitos dos titulares, estabelecendo uma base sólida para a proteção da privacidade no ambiente digital.

Embora a legislação tenha descrito diversas atividades relacionadas ao tratamento de dados e até bem abrangente, pode-se afirmar que o rol é exemplificativo, conforme explica Viviane Nóbrega Maldonado e Renato Ópice Blum:

> (6)“Referida constatação de abrangência do conceito é de fundamental importância, pois o agente de tratamento, em absolutamente todas essas hipóteses, deverá manter registros das suas operações, bem como, no caso do controlador, avaliar o cumprimento de uma das bases legais previstas na Lei, o que implica dizer que um simples dado pessoal arquivado, mesmo que não seja processado, precisará ter um fundamento previsto na Lei para estar sob a responsabilidade do agente. Se o controlador não encontrar um embasamento jurídico para manter o dado pessoal consigo (ou com o operador), deverá eliminá- lo”(6).

1.2. Comparação com outras leis de proteção de dados em nível internacional.

A proteção de dados pessoais é uma preocupação global, refletida na implementação de leis e regulamentos em diversos países. Em comparação com outras leis de proteção de dados em nível internacional, destaco algumas diferenças e semelhanças significativas.

- **GDPR (Regulamento Geral de Proteção de Dados da União Europeia):**

Semelhanças: A LGPD compartilha muitos princípios fundamentais com o GDPR, como a ênfase na transparência, finalidade específica, necessidade e segurança dos dados. Diferenças: Algumas distinções notáveis incluem a abordagem mais detalhada do GDPR em relação ao consentimento e o direito ao esquecimento, que não é expressamente mencionado na LGPD.

- **California Consumer Privacy Act (CCPA):**

Semelhanças: A CCPA, nos Estados Unidos, e a LGPD compartilham a ideia de conferir aos consumidores o direito de acessar, corrigir e excluir suas informações pessoais. Diferenças: A CCPA possui disposições específicas relacionadas à venda de dados

pessoais e fornece aos consumidores o direito de optar por não participar dessa prática, o que não é diretamente equivalente na LGPD.

- **A Lei de Privacidade do Consumidor do Canadá (PIPEDA):**

Semelhanças: Ambas as legislações destacam a importância da transparência, consentimento e segurança dos dados. Diferenças: A PIPEDA tem um foco específico na coleta, uso e divulgação de informações pessoais por organizações privadas no Canadá, enquanto a LGPD é mais abrangente e se aplica a uma gama mais ampla de entidades.

1.3. Importância da segurança jurídica na proteção de dados pessoais.

Fornecendo um arcabouço normativo que estabelece diretrizes claras para o tratamento ético e responsável das informações pessoais, com certo grau de importância no qual irei destacar a seguir através de vários pontos:

Confiabilidade e Previsibilidade: A existência de leis claras e objetivas, que geram confiança tanto para os titulares dos dados quanto para as organizações que os processam. A previsibilidade jurídica é essencial para a construção de relações transparentes e éticas. **Responsabilidade das Organizações**: com a imposição de obrigações claras às organizações, promovendo a responsabilidade no tratar dos dados pessoais. Isso incentiva práticas de segurança robustas e a implementação de medidas adequadas para proteger as informações confidenciais. **Direitos e Proteção dos Titulares** e **Fomento à Inovação Responsável:** Um ambiente jurídico seguro proporciona espaço para a inovação, incentivando o desenvolvimento de tecnologias e práticas que respeitem a privacidade. Isso cria um equilíbrio entre o progresso tecnológico e a proteção dos direitos individuais.

Ainda, o consentimento deverá ser informado, isto significa que o titular dos dados deverá compreender e permitir para quais fins os seus dados serão coletados antes decidir, e mais, a informação deverá ser passada de forma integral e dinâmica, seja transparente e simples para ele(a). Nesse sentido, em razão desse grau de transparência exigido pela legislação, o que traz mais segurança jurídica ao controlador, é que o mesmo terá o ônus

da prova para demonstrar que o consentimento foi obtido na forma da Lei. Patrícia Peck Pinheiro, ao analisar o art. 8º sobre o consentimento, afirma que:

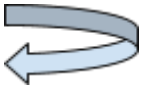
> (7)“Ao longo dos anos, a necessidade do consentimento na coleta dos dados, principalmente no ambiente virtual, foi ganhando importância em razão da sensibilidade e vulnerabilidade que as informações pessoais foram adquirindo com o desenvolvimento da tecnologia. Nesse sentido, garantir que as pessoas/usuários tenham ciência de que devem consentir o uso dos dados, assim como tenham direito de saber a finalidade da coleta e acesso ao seu conte do em qualquer momento, é primordial para a assegurar a liberdade e a privacidade. Ao mesmo tempo, as empresas devem ter a liberdade de utilizar os dados de maneira transparente e ética em troca de um serviço ou acesso, tendo em vista que o desenvolvimento econômico também deve ser garantido a esses sujeitos. Importante destacar que cabe à instituição que realiza o tratamento a capacidade de demonstrar que estava legítima (detinha o registro do consentimento ou se enquadrava nas hipóteses de exceção)”(7).

Ou seja, a segurança jurídica é um alicerce essencial para a eficácia das leis de proteção de dados pessoais, assegurando que o tratamento dessas informações seja conduzido de maneira ética, transparente e em conformidade com os princípios fundamentais estabelecidos. Passo a demonstrar como foi o desenvolver da norma no Brasil.

• Desenvolvimento da LGPD no Brasil

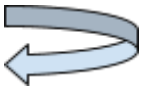
2.1. Histórico da criação da LGPD.

O histórico da criação da Lei Geral de Proteção de Dados (LGPD) no Brasil é marcado por um processo que culminou na necessidade de regulamentar a proteção da privacidade e dos dados pessoais no contexto digital. Aqui estão os principais marcos do histórico da LGPD: 🔻



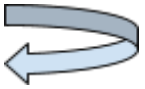
Projeto de Lei do Senado (PLS) 330/2013:

Em 2013, o Senado Federal brasileiro apresentou o Projeto de Lei do Senado (PLS) 330/2013, que buscava regular o tratamento de dados pessoais no Brasil. No entanto, o projeto não obteve avanço significativo na época. 🔻



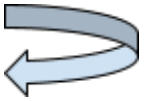
Influência do Regulamento Geral de Proteção de Dados (GDPR):

A aprovação e implementação bem-sucedida do Regulamento Geral de Proteção de Dados (GDPR) na União Europeia em 2018 influenciou positivamente a discussão sobre a necessidade de uma legislação semelhante no Brasil. O GDPR estabeleceu padrões rigorosos para a proteção de dados pessoais e inspirou outros países a seguirem o exemplo. 🔻



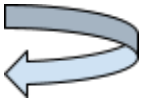
Aprovação do Projeto de Lei na Câmara dos Deputados:

Em maio de 2018, a Câmara dos Deputados aprovou o Projeto de Lei de Proteção de Dados Pessoais (PL 4060/2012), que posteriormente foi convertido na Lei Geral de Proteção de Dados (Lei nº 13.709/2018), conhecida como LGPD. O texto foi aprovado pelo Senado Federal e sancionado pelo então presidente Michel Temer em agosto de 2018. 🔻



Prazo para Entrada em Vigor:

Originalmente, a LGPD previa um prazo de 18 meses após sua publicação para que suas disposições entrassem em vigor. No entanto, devido a pressões e discussões, esse prazo foi prorrogado, e a lei entrou em vigor em setembro de 2020. 🔻



Criação da Autoridade Nacional de Proteção de Dados (ANPD):

Em dezembro de 2018, o presidente Jair Bolsonaro sancionou a lei que cria a Autoridade Nacional de Proteção de Dados (ANPD), um órgão responsável por fiscalizar e aplicar a LGPD. A ANPD começou a operar efetivamente em novembro de 2020.

Esse histórico reflete a crescente conscientização sobre a importância da proteção de dados pessoais no ambiente digital, assim como a influência de eventos globais e regulamentações estrangeiras. A legislação visa garantir a privacidade e a segurança dos dados dos cidadãos brasileiros, alinhando o Brasil às práticas internacionais nesse campo.

2.2. Papel e atribuições da Autoridade Nacional de Proteção de Dados (ANPD).

A Autoridade que carrega o papel de desempenhar o poder legislador, fiscalizador e executivo é crucial na efetivação da LGPD no Brasil. Suas atribuições e responsabilidades são delineadas na legislação vigente e garante que a proteção de dados pessoais seja efetivamente regulamentada. E quais seriam as principais atribuições da ANPD:

Fiscalização e Aplicação da LGPD: Sendo responsável por fiscalizar o cumprimento da LGPD por parte das organizações que realizam o tratamento de dados pessoais. Isso inclui a aplicação de sanções e penalidades em casos de descumprimento das disposições da lei.

Elaboração de Normas e Diretrizes: Detém o poder de criar normas e diretrizes que complementam a LGPD, fornecendo orientações detalhadas sobre como as organizações devem cumprir as disposições legais junto a cultura e boas práticas. Essas normas podem abordar questões específicas relacionadas ao tratamento de dados e segurança da informação.

Estímulo à Adoção de Boas Práticas: Sustenta o papel de incentivar as organizações a adotarem boas práticas no tratamento de dados pessoais, incluindo a promoção de medidas que vão além do simples cumprimento legal, visando à excelência na proteção da privacidade.

Registro de Atividades de Tratamento:

A ANPD pode estabelecer diretrizes para o registro das atividades de tratamento de dados pelas organizações. Esse registro é um requisito fundamental da LGPD, permitindo maior transparência e prestação de contas no processo de tratamento de dados.

Recepção de Reclamações e Demandas: A autoridade é responsável por receber e avaliar reclamações e demandas apresentadas por titulares de dados, fornecendo um canal para que os cidadãos possam buscar proteção de seus direitos em relação ao tratamento de suas informações pessoais.

Cooperação Internacional: A ANPD pode cooperar com autoridades de proteção de dados de outros países para promover a consistência e a colaboração internacional na proteção de dados transfronteiriços.

Educação e Conscientização: A ANPD tem o papel de educar a sociedade e as organizações sobre a importância da proteção de dados pessoais e as disposições da LGPD. Isso inclui a realização de campanhas de conscientização e a disseminação de informações sobre práticas recomendadas.

Poder Sancionatório: A ANPD tem a autoridade para aplicar sanções e penalidades em caso de descumprimento da LGPD. As penalidades podem incluir advertências, multas, suspensão do tratamento de dados e até mesmo a proibição do tratamento de dados em situações específicas.

A pessoa que será indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Conforme esclarece Viviane Nóbrega Maldonado e Renato Ópice Blum:

> (8) “Seu papel vai muito além de atuar como canal de comunicação entre controlador ou o operador, os titulares dos dados e a ANPD, como previsto no conceito em estudo, pois ele será o responsável por aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da ANPD e adotar providências; orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à

> proteção de dados pessoais; e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares". (8)

O papel da ANPD é essencial para garantir a efetiva aplicação da LGPD e promover uma cultura de respeito à privacidade e proteção de dados no Brasil. A autoridade desempenha um papel ativo na criação de um ambiente regulatório que equilibra os interesses dos titulares de dados, das organizações e da sociedade como um todo. Vejamos quais desafios a norma enfrenta ao ser implementada.

- Desafios na Implementação da LGPD

3.1. Barreiras organizacionais: custos, treinamento, adaptação de processos.

Certamente, a implementação da LGPD pode acarretar diversos desafios para as organizações. Entre esses desafios, destacam-se barreiras organizacionais, ou seja, questões relacionadas a custos, treinamento de pessoal capacitado e adaptação de processos. Aqui exponho alguns detalhes a respeito desses desafios:

Custos Associados à Conformidade:

A adequação às normas da LGPD muitas vezes requer investimentos significativos em tecnologia, segurança da informação e recursos humanos. Implementar sistemas de proteção de dados, realizar auditorias de segurança e manter uma estrutura que garanta a conformidade têm custos associados, e muitas organizações podem enfrentar desafios financeiros ao buscar atender a esses requisitos.

Treinamento de Pessoal:

A conscientização e o treinamento dos funcionários são cruciais para o sucesso na implementação da LGPD. Muitas organizações enfrentam desafios ao tentar educar sua equipe sobre as novas práticas e procedimentos necessários para garantir a proteção

adequada dos dados pessoais. Isso inclui desde os profissionais de tecnologia da informação até os departamentos jurídico e de recursos humanos.

Adaptação de Processos Internos:

A LGPD exige mudanças significativas nos processos internos das organizações, desde a coleta e armazenamento de dados até a maneira como respondem a solicitações dos titulares de dados. A adaptação de processos existentes para estar em conformidade com a lei pode ser um desafio operacional, especialmente para organizações com sistemas estabelecidos.

Complexidade na Identificação e Categorização de Dados:

Identificar e categorizar os dados pessoais que uma organização possui pode ser uma tarefa complexa, especialmente em empresas com grandes volumes de informações. A LGPD requer uma compreensão detalhada de quais tipos de dados estão sendo processados, e essa análise pode ser desafiadora. **Gestão de Incidentes de Segurança:**

A LGPD estabelece a obrigação de notificar incidentes de segurança que possam comprometer a segurança dos dados. Desenvolver planos eficientes para a gestão desses incidentes, bem como a comunicação adequada com a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares, pode ser um desafio significativo.

Passa-se a analisar alguns conceitos mais importantes para entendimento do tema, previstos no resto do art. 5º. Veja-se que a LGPD define o significado de bloqueio de dados pessoais, ao estabelecer que se trata da suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados. Isso implica em dizer que

> (9) “Quando o controlador avaliar, de ofício ou mediante requisição do titular, eventuais dados pessoais ou banco de dados que possam ser excessivos ou tenha dúvida sobre a conformidade do tratamento perante qualquer ordenamento jurídico de proteção de dados, é recomendável que, temporariamente, segregue completamente tais dados de toda

a operação até que chegue a uma conclusão efetiva e fundamentada sobre a sua necessidade e licitude". (9)

Conscientização Cultural e Organizacional:

Mudar a cultura organizacional para incorporar a proteção de dados como um valor fundamental pode ser um desafio. É crucial estabelecer uma mentalidade de respeito à privacidade em todos os níveis da organização, o que pode exigir esforços significativos de conscientização e mudança de mentalidade.

Superar esses desafios requer uma abordagem estratégica, envolvimento de todas as partes interessadas e a adoção de boas práticas de governança de dados. As organizações que conseguem superar esses obstáculos estarão em melhor posição para garantir a conformidade com a LGPD e proteger efetivamente os dados pessoais.

3.2. Desafios tecnológicos: conformidade de sistemas, segurança cibernética.

Os desafios tecnológicos na implementação da LGPD incluem a conformidade de sistemas e a garantia de segurança cibernética. Esses aspectos são cruciais para garantir que as organizações possam tratar dados pessoais de maneira ética e segura. Aqui estão mais detalhes sobre esses desafios:

Conformidade de Sistemas:

Integração de Sistemas: Muitas organizações têm uma variedade de sistemas e aplicativos que processam dados. Garantir que esses sistemas estejam integrados e operando em conformidade com os requisitos da LGPD pode ser desafiador, especialmente em organizações com infraestruturas complexas. **Atualização de Sistemas Legados:** Empresas que dependem de sistemas mais antigos podem enfrentar desafios ao tentar adaptar esses sistemas para atender aos padrões modernos de proteção de dados. A atualização e a adaptação de sistemas legados podem demandar tempo e recursos significativos. **Avaliação de Fornecedores:** Empresas que terceirizam serviços ou usam fornecedores externos para processar dados devem garantir que esses

parceiros também estejam em conformidade com a LGPD. Isso envolve avaliar e garantir que os sistemas dos fornecedores atendam aos requisitos de proteção de dados.

Segurança Cibernética:

Proteção contra Ameaças Cibernéticas: A LGPD exige que as organizações tomem medidas eficazes para proteger os dados pessoais contra ameaças cibernéticas. Isso inclui a implementação de medidas de segurança, como firewalls, antivírus, detecção de intrusões e outras tecnologias para proteger contra-ataques. **Criptografia e Anonimização**: A LGPD incentiva o uso de técnicas de criptografia e anonimização para proteger os dados pessoais. Implementar essas técnicas de maneira eficaz pode ser desafiador, especialmente ao equilibrar a segurança com a usabilidade e a acessibilidade dos dados. **Monitoramento Contínuo**: A segurança cibernética não é uma preocupação estática. As organizações precisam implementar sistemas de monitoramento contínuo para detectar atividades suspeitas e responder prontamente a incidentes de segurança.

Treinamento e Conscientização: A falha humana é uma causa comum de brechas de segurança. Garantir que os funcionários estejam devidamente treinados e conscientes dos riscos de segurança cibernética é essencial para manter um ambiente seguro.

Resposta a Incidentes: Desenvolver planos de resposta a incidentes é crucial para lidar com violações de dados de maneira eficaz. Isso envolve a identificação, contenção, investigação e notificação adequada de incidentes de segurança.

Superar esses desafios tecnológicos requer investimentos contínuos em tecnologia, treinamento de pessoal e a implementação de práticas de segurança cibernética sólidas. Além disso, as organizações devem manter-se atualizadas sobre as melhores práticas e regulamentações para garantir uma proteção de dados eficaz e contínua.

3.3. Aspectos culturais: conscientização e mudança de cultura organizacional

Os aspectos culturais são fundamentais na implementação bem-sucedida da Lei Geral de Proteção de Dados (LGPD) e na promoção de uma cultura organizacional que valoriza a

privacidade e a segurança dos dados. No Brasil existe muito forte uma cultura de ‘não vai dar em nada’ que é perigosa quando abordamos o tema da proteção de dados, e há dois aspectos principais nesse contexto que são a conscientização e a mudança na cultura organizacional. Aqui estão mais detalhes sobre esses aspectos:

Conscientização:

Educação e Treinamento: A conscientização começa com a educação e o treinamento dos membros da organização. É crucial que todos os funcionários compreendam os princípios da LGPD, os riscos associados ao tratamento inadequado de dados pessoais e suas responsabilidades individuais na proteção da privacidade. **Campanhas de Conscientização:** A realização de campanhas de conscientização é uma estratégia eficaz para comunicar a importância da proteção de dados. Isso pode incluir a distribuição de materiais educativos, workshops, seminários e comunicações regulares para manter a atenção e o entendimento contínuos. **Engajamento dos Funcionários:** Incentivar a participação ativa dos funcionários na proteção de dados e fornecer canais para esclarecimento de dúvidas e preocupações contribui para uma cultura organizacional mais consciente e comprometida.

Mudança de Cultura Organizacional:

Integração nos Valores Organizacionais: A proteção de dados deve ser integrada aos valores fundamentais da organização. Isso envolve a incorporação da privacidade e da segurança dos dados nos objetivos, missão e valores da empresa. **Liderança e Comprometimento:** A liderança desempenha um papel crucial na mudança cultural. Os líderes devem demonstrar um comprometimento claro com a conformidade com a LGPD, incentivando ações que promovam uma cultura de respeito à privacidade. **Revisão de Políticas e Processos:** Uma mudança cultural efetiva requer a revisão e adaptação de políticas e processos internos para refletir os requisitos da LGPD. Isso inclui a criação de políticas claras de privacidade, a implementação de procedimentos para responder a solicitações de titulares de dados e a revisão de práticas de coleta e processamento de dados. **Incentivos e Reconhecimento:** Incentivar comportamentos positivos relacionados à proteção de dados e reconhecer o esforço individual e coletivo para atingir os objetivos de conformidade pode fortalecer a cultura organizacional. **Avaliação Contínua:** A mudança cultural não ocorre da noite para o dia. É necessário um esforço contínuo para

avaliar a eficácia das iniciativas, ajustar abordagens conforme necessário e garantir que a cultura organizacional evolua para refletir as demandas da LGPD.

A integração bem-sucedida desses aspectos culturais contribui para uma organização mais resiliente em relação à conformidade com a LGPD, promovendo uma abordagem proativa para a proteção de dados e construindo a confiança dos titulares de dados e do público em geral. A seguir uma amostra de como tudo isso funciona pra valer.

- **Segurança Jurídica na Prática**

4.1. Como funciona na prática

Para compreendermos ainda mais sobre o assunto, é importante ressaltar que envolve a adoção de boas práticas de governança de dados, a realização de avaliações de impacto à privacidade mitigando riscos legais, a capacitação dos colaboradores e o monitoramento constante do cumprimento das obrigações previstas com referenciais quanto à capacidade de operar de acordo com as disposições legais. Aqui estão alguns aspectos de como a segurança jurídica é praticada no mundo real:

Políticas e Procedimentos Claros: Isto é, definir como os dados pessoais são coletados, processados, armazenados e compartilhados. Desta forma elas expõem para o público qual dado elas coletam e para qual finalidade vai ser utilizado. Não obstante, é necessário que haja procedimentos operacionais detalhados que ajudem a garantir a conformidade com a LGPD e outras regulamentações aplicáveis.

Consentimento Adequado: A segurança jurídica exige que as organizações obtenham consentimento adequado dos titulares de dados antes de processar suas informações. Isso implica em fornecer informações claras sobre as finalidades do processamento, garantindo que o consentimento seja voluntário, específico, informado e inequívoco.

Registro de Atividades de Tratamento: Manter registros detalhados das atividades de tratamento de dados é uma prática essencial para garantir a segurança jurídica. Isso inclui documentar o propósito do processamento, categorias de dados envolvidas, medidas de segurança implementadas e a base legal para o tratamento.

Adequação nas Transferências Internacionais: Caso haja transferências internacionais de dados, a segurança jurídica exige que as organizações adotem medidas adequadas, como cláusulas contratuais padrão ou garantias específicas, para garantir que os dados estejam protegidos de acordo com os padrões da LGPD.

Resposta a Solicitações de Titulares: Organizações que valorizam um ambiente de segurança na jurisdição têm procedimentos claros para lidar com solicitações de titulares de dados, como acesso, retificação, exclusão ou portabilidade. Responder a essas solicitações de maneira oportuna e eficaz é crucial para cumprir as obrigações legais.

Treinamento e Conscientização: A segurança jurídica é reforçada por meio do treinamento contínuo e da conscientização dos funcionários. Garantir que todos na organização estejam cientes das implicações legais da LGPD e compreendam suas responsabilidades contribui para uma cultura de conformidade.

Avaliação de Impacto à Proteção de Dados (DPIA): Quando necessário, a realização de Avaliações de Impacto à Proteção de Dados (DPIA) que reforça o nível de segurança jurídica, envolvendo avaliar os riscos e impactos potenciais sobre a privacidade antes de realizar determinados tipos de processamento de dados.

Comunicação Transparente:

A comunicação transparente com os titulares de dados, autoridades de proteção de dados e outros stakeholders é fundamental. Isso inclui notificar prontamente sobre violações de dados e fornecer informações claras sobre as práticas de proteção de dados.

Para se alcançar a segurança jurídica de forma prática, portanto, exigirá uma abordagem holística, integrando aspectos legais, operacionais e culturais para garantir que as

organizações estejam em conformidade com a LGPD e outras normas de proteção de dados, reduzindo assim os riscos legais associados ao tratamento de dados pessoais.

4.2. Números da proteção de dados vêm crescendo no país.

Um evento realizado em agosto lançou a publicação “Privacidade e proteção de dados pessoais 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil”, da Cetic (Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação). O documento mostrou as informações coletadas de 2.556 usuários de Internet e 1.473 empresas relacionadas à proteção de dados pessoais. A pesquisa apontou que 77% dos entrevistados relataram já ter desinstalado algum aplicativo do seu smartphone, enquanto 69% afirmaram já ter deixado de entrar em algum site por preocupação.

Existe uma diferença no nível de preocupação sobre o uso de dados de acordo com a cor. Afinal, 52% dos pretos e 49% dos pardos afirmaram ter muita preocupação sobre seus dados, enquanto, entre as pessoas que se declararam brancas, 43% afirmaram o mesmo.

Outro dado interessante também se refere à preocupação das empresas, visto que, apenas 32% das empresas entrevistadas alegaram possuir uma política de privacidade que informa aos usuários como seus dados são tratados.

Entre as empresas entrevistadas, 30% afirmaram realizar testes de segurança como prevenção ao vazamento de dados, enquanto 24% afirmaram ter elaborado um plano de conformidade com a lei.

Levantamento realizado pelo Grupo Daryus, consultoria especializada no tema, indica que 80% das empresas no Brasil ainda não estão completamente adequadas à LGPD; 35% dizem estar parcialmente adequadas e 24% em fase inicial de adequação.

Realizado em setembro do ano passado, o levantamento contempla 200 profissionais de organizações em 16 áreas de atuação, além de órgãos governamentais, em 27 estados brasileiros; 34% são companhias de grande porte com mais de mil funcionários.

Jeferson D'Addario, CEO do Grupo Daryus, comenta que a empresa que se adequa à LGPD, além de cumprir uma regra, contribui com o ecossistema corporativo. (10) "É um trabalho importante para as organizações e deve ser contínuo, já que a informação é um bem valioso para as empresas diante de possíveis ameaças no ambiente digital"(10), destaca.

A preocupação em relação à conformidade e adequação à LGPD é iminente, visto que a ANPD, autarquia especial responsável por fiscalizar a lei, projeta, para 2023, a publicação do Regulamento de Dosimetria e Aplicação de Sanções Administrativas contra as empresas que não cumprirem a legislação. “Ou seja, muito em breve, teremos notícias das primeiras sanções aplicadas pela agência com base na LGPD”, projeta Alexander Coelho, advogado especializado em direito digital e proteção de dados.

A pesquisa também revela que apesar de um cenário preocupante, o assunto já é tratado como prioridade nas companhias. **Mais da metade dos entrevistados (58%) afirmam que, neste momento**, as organizações em que trabalham tratam o tema de proteção de dados pessoais com alta relevância. Já 33% tratam o assunto com média ou baixa relevância e apenas 4% não consideram a pauta relevante.

"Esse tema precisa ser tratado dentro das organizações com mais frequência, pois influencia na saúde dos negócios. As empresas que ainda não perceberam a relevância da proteção de dados podem ter sanções administrativas, conforme aponta a LGPD, ou se tornar alvos de cibercriminosos", alerta D'Addario.

Outra descoberta do estudo é que a preocupação com os dados pessoais vem crescendo entre os usuários da internet: a maioria dos internautas já deixou de fazer alguma atividade por preocupações com dados pessoais (87%), como deixar de instalar aplicativos para celulares, navegar em alguma página da internet por preocupação com

ataques de phishing [tipo de golpe digital em que os criminosos enviam ou publicam links falsos para “pescar” informações dos usuários] ou deixar de realizar alguma compra online por receio de fraudes e golpes.

De acordo com o levantamento, em 45% das empresas a área responsável por privacidade e proteção de dados responde diretamente à presidência ou alta direção da empresa, 10% ao setor de Tecnologia da Informação (TI), 7% à área jurídica e 6% à Segurança da Informação. Há que se ressaltar que o legislador não determinou quais circunstâncias uma organização deverá indicar um encarregado, no entanto, o Guia Orientativo (2021, p. 22) da ANPD determina que se deve assumir como regra geral, que toda organização deverá indicar alguém para exercer este papel, como uma boa prática. Além disso:

> A LGPD também não distingue se o encarregado deve ser pessoa física ou jurídica, e se deve ser um funcionário da organização ou um agente externo. Considerando as boas práticas internacionais, o encarregado poderá ser tanto um funcionário da instituição quanto um agente externo, de natureza física ou jurídica. Recomenda-se que o encarregado seja indicado por um ato formal, como um contrato de prestação de serviços ou um ato administrativo.

(12) Pela definição do artigo 5º, inciso VII, conforme alteração trazida pela lei 13.853/19, o Encarregado é a pessoa indicada pelo controlador e pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. E da forma como ficou a redação da lei é possível ser pessoa física ou jurídica, interna ou externa à organização. (12)

> (13) Muitos acreditam que o DPO atuaria como uma espécie de ombudsman, que seria um indivíduo encarregado do estabelecimento de um canal de comunicação entre consumidores, empregados e diretores, mas muitas

organizações, na prática, ultrapassam as definições previstas na LGPD e atribuem mais atividades ao DPO (Lima & Alves, 2021) (12).

Por fim, é importante ressaltar que ainda não enxergamos o tema proteção de dados pessoais com a seriedade que deveríamos. Porém, claramente temos mostrado que estamos avançando no tema. Agora vou introduzir alguns cenários futuros a respeito.

- **Perspectivas Futuras**

5.1. Tendências na regulamentação de proteção de dados.

algumas tendências e perspectivas futuras que geralmente são consideradas relevantes na regulamentação de proteção de dados:

Globalização das Normas de Proteção de Dados: Espera-se que mais países adotem legislações de proteção de dados inspiradas em regulamentações como a GDPR da União Europeia. Isso reflete uma tendência global em direção a padrões mais rigorosos de privacidade e segurança de dados. Aprimoramento da Governança de Dados: A governança de dados continuará sendo uma área de foco, com as organizações sendo desafiadas a implementar estruturas eficazes de governança para gerenciar dados de maneira ética, transparente e conforme as regulamentações. Ênfase em Direitos dos Titulares de Dados: As regulamentações de proteção de dados devem colocar uma ênfase contínua nos direitos dos titulares de dados, incentivando organizações a facilitarem o exercício desses direitos, como o direito de acesso, retificação, exclusão e portabilidade.

Segurança Cibernética e Notificações de Violações: A ênfase na segurança cibernética deve crescer, com regulamentações exigindo medidas proativas para prevenir violações de dados. Além disso, notificações de violações podem se tornar mais padronizadas e estritas. Regulações Setoriais Específicas: Algumas indústrias podem ver o surgimento de regulamentações específicas de proteção de dados, adaptadas às particularidades de

setores como saúde, finanças e tecnologia. Maior Fiscalização e Penalidades: A fiscalização por parte das autoridades de proteção de dados pode se intensificar, com a aplicação mais rigorosa de penalidades em caso de não conformidade. Isso pode motivar as organizações a investirem mais em conformidade. Proteção de Dados em Contexto Internacional: A colaboração internacional em questões de proteção de dados pode se intensificar, com regulamentações e padrões comuns sendo desenvolvidos para lidar com desafios transfronteiriços. Responsabilidade de Agentes de Tratamento: As regulamentações podem evoluir para abordar a responsabilidade de agentes de tratamento, como processadores de dados, em garantir a conformidade com as normas de proteção de dados.

Inovação e Privacidade: Regulamentações podem ser projetadas para equilibrar a inovação tecnológica com a proteção da privacidade, incentivando a implementação de práticas éticas no desenvolvimento e uso de novas tecnologias.

Essas perspectivas refletem as tendências gerais observadas na área de proteção de dados, mas é fundamental acompanhar as mudanças específicas em cada jurisdição para compreender completamente o cenário regulatório atualizado.

5.2. Desafios emergentes na segurança jurídica.

À medida que o cenário de proteção de dados continua a evoluir, surgem desafios emergentes na segurança jurídica que requerem atenção, como por exemplo Tecnologias Emergentes e Proteção de Dados: O avanço de tecnologias como Inteligência Artificial, aprendizado de máquina e internet das coisas levanta novos desafios para a privacidade, há questões éticas e de privacidade associadas ao uso dessas tecnologias que precisam ser abordadas de maneira eficaz pelas regulamentações. Outros desafios que podemos mencionar incluem:

Regulamentações em Evolução: A constante evolução das leis de proteção de dados pode representar um desafio para as organizações que precisam se adaptar a novos

requisitos e interpretações legais. Acompanhar as mudanças nas regulamentações pode exigir recursos significativos.

Proteção de Dados em Ambientes Cloud: Com a crescente adoção de serviços em nuvem, garantir a segurança jurídica em ambientes de armazenamento e processamento de dados em nuvem é um desafio. Isso inclui questões relacionadas à localização dos dados, responsabilidades de conformidade e segurança dos provedores de serviços em nuvem. Privacidade por Design e por Padrão: Integrar princípios de privacidade desde a concepção (privacy by design) e garantir que esses princípios sejam padrão nas práticas organizacionais (privacy by default) pode ser desafiador. Isso envolve incorporar considerações de privacidade desde a fase inicial de desenvolvimento de produtos e serviços.

Transparência e Aplicabilidade em Algoritmos: A conformidade com regulamentações pode ser desafiadora quando se trata da transparência e aplicabilidade em algoritmos de tomada de decisão automatizada. Garantir que os titulares de dados compreendam o impacto das decisões automatizadas em seus direitos pode ser um ponto crítico.

Transferência Internacional de Dados: As restrições sobre a transferência internacional de dados, especialmente em jurisdições com requisitos rigorosos de proteção de dados, podem criar desafios para empresas globais. Garantir que as transferências de dados respeitem as regulamentações locais e internacionais é um ponto crítico.

Direitos dos Titulares de Dados: A implementação efetiva dos direitos dos titulares de dados, como o direito de acesso, retificação, exclusão e portabilidade, pode ser um desafio. Organizações precisam estabelecer processos claros para atender a essas solicitações de maneira oportuna. Segurança Cibernética e Incidentes de Dados: O aumento da sofisticação de ataques cibernéticos e o risco de violações de dados podem criar desafios na manutenção da segurança jurídica. Desenvolver planos de resposta a incidentes e cumprir os requisitos de notificação são áreas críticas nesse contexto.

Responsabilidade de Agentes de Tratamento: Identificar e estabelecer claramente a responsabilidade de agentes de tratamento, como processadores de dados, em conformidade com as leis de proteção de dados é um desafio. Isso inclui a definição de papéis e responsabilidades contratuais. Cultura Organizacional e Conscientização: A criação de uma cultura organizacional que valorize a privacidade e a segurança de dados, bem como a conscientização contínua dos funcionários sobre as implicações legais, representam desafios persistentes.

Superar tais desafios requer uma abordagem proativa e adaptativa, com organizações dedicando recursos significativos à conformidade contínua e à proteção de forma eficaz dos dados pessoais.

5.3. Possíveis aprimoramentos na LGPD.

Alguns possíveis aprimoramentos que poderiam ser aplicados segundo o meu entendimento:

Refinamento de Definições e Escopo: Clarificação e refinamento das definições e do escopo da LGPD para abordar ambiguidades e garantir uma interpretação mais consistente. **Adaptação a Tecnologias Emergentes**: Inclusão de disposições específicas para lidar com desafios trazidos por tecnologias emergentes, como inteligência artificial, aprendizado de máquina e internet das coisas.

Regras Claras sobre Transferências Internacionais de Dados: Estabelecimento de regras mais claras e procedimentos para a transferência internacional de dados, especialmente à luz de decisões judiciais recentes sobre esse tema. **Aprimoramento dos Direitos dos Titulares de Dados**: Consideração de aprimoramentos nos direitos dos titulares de dados, incluindo maior clareza sobre como exercer esses direitos e garantir respostas mais rápidas por parte das organizações. **Abordagem a Incidentes de Segurança**: Reforço das obrigações relacionadas à notificação de incidentes de segurança, incluindo diretrizes mais detalhadas sobre o tempo de notificação e o conteúdo necessário.

Regulamentação Setorial Específica: Exploração de regulamentações específicas para setores particulares, reconhecendo as nuances e características específicas de diferentes indústrias. **Flexibilidade para Micro e Pequenas Empresas**: Consideração de disposições que reconheçam as limitações e recursos limitados de micro e pequenas empresas, proporcionando maior flexibilidade, especialmente em termos de conformidade.

Fomento à Conscientização e Educação: Incentivo à conscientização e educação contínua sobre a LGPD, tanto para organizações quanto para o público em geral, visando promover uma cultura de respeito à privacidade. **Mecanismos de Supervisão e Fiscalização Aprimorados**: Aprimoramento dos mecanismos de supervisão e fiscalização pela Autoridade Nacional de Proteção de Dados (ANPD), garantindo sua eficácia na aplicação da lei. **Avaliação Periódica e Atualização**: Instituição de uma prática regular de avaliação e atualização da LGPD para garantir sua relevância contínua em um ambiente dinâmico de proteção de dados.

• CONCLUSÃO

Recapitulação dos principais pontos discutidos:

A presente pesquisa explorou os fundamentos e desafios inerentes à Lei Geral de Proteção de Dados (LGPD) no contexto da segurança jurídica, abordei princípios como a finalidade, adequação, necessidade, livre acesso, transparência, segurança, prevenção, não discriminação e responsabilização apresentando uma análise abrangente sobre direitos dos titulares como acesso, retificação, exclusão, portabilidade, oposição, entre outros ademais as obrigações impostas às organizações das quais a coleta e tratamento de dados apenas para fins específicos, consentimento adequado, segurança da informação, notificação de violações, entre outros, sempre destacando a importância da LGPD na proteção da privacidade dos indivíduos numa sociedade onde se vive um ambiente global cada vez mais conectado.

Para entender melhor o panorama do histórico da Criação da LGPD, busquei colocar de forma cronológica e contextualizada, valendo-se de suas origens, debates e processo de criação da LGPD. Ao comparar a LGPD com a GDPR e outras legislações internacionais de proteção de dados e analisar desafios emergentes, percebemos a necessidade de conformidade global, considerando práticas de outras jurisdições, e precisa ser um processo contínuo de adaptação e aprimoramento para enfrentar questões tecnológicas, culturais e legais numa constante evolução. O papel central da Autoridade Nacional de Proteção de Dados (ANPD) como fiscalizadora e orientadora foi enfatizado, ressaltando sua importância na promoção da conformidade e na construção de uma cultura organizacional de respeito à privacidade.

As perspectivas futuras indicam uma crescente ênfase nos direitos dos titulares de dados, regulamentação de tecnologias emergentes e colaboração internacional. No entanto, o sucesso contínuo da LGPD dependerá não apenas de avanços legislativos, mas também da capacidade de organizações e autoridades se adaptarem a um cenário dinâmico, enfrentando barreiras de custos, treinamento de pessoas capacitadas e adaptação de processos.

Por fim, esta pesquisa sugere que o caminho para a eficácia duradoura da LGPD reside na educação contínua, conscientização pública e revisões periódicas para manter a legislação alinhada aos desenvolvimentos tecnológicos e expectativas da sociedade. Ao adotar uma abordagem proativa, podemos garantir não apenas a conformidade legal, mas também a proteção eficaz dos dados pessoais e a preservação da segurança jurídica no cenário da era digital.

Conclusões sobre a eficácia da LGPD na garantia da segurança jurídica.

A Lei nº 13.709/2018 emerge como um marco significativo na busca pela segurança jurídica no tratamento de dados pessoais no Brasil. Ao longo desta análise, fica claro que a legislação desempenha um papel crucial na promoção de princípios éticos e transparentes no cenário cada vez mais complexo da era digital.

A LGPD, ao estabelecer direitos dos titulares de dados representa um avanço significativo para tal proteção e fornece uma estrutura legal robusta ao impor obrigações claras às organizações, sinalizando um avanço na salvaguarda da privacidade individual. Contudo, a eficácia real da LGPD dependerá da efetiva implementação que desafia a adoção de uma postura proativa sobre esses princípios e da fiscalização diligente por parte da ANPD.

A comparação internacional destaca a importância de alinhar as práticas nacionais com as tendências globais em proteção de dados. Enquanto a LGPD se inspira em regulamentações como a GDPR, a necessidade de adaptação contínua e aprimoramento fica evidente, especialmente diante de desafios tecnológicos e culturais emergentes.

A segurança jurídica, portanto, se torna uma busca dinâmica. A legislação, por si só, fornece uma base robusta, mas a eficácia total requer a colaboração ativa de empresas e companhias, a conscientização do público e a prontidão para revisões periódicas para acompanhar o ritmo acelerado das mudanças, colocando o Brasil em posição de consonância com as tendências internacionais de proteção de dados, alinhando-se a regulamentações como a GDPR.

Num panorama futuro, a LGPD pode não apenas moldar a forma como as organizações lidam com dados pessoais, mas também impulsionar uma cultura de responsabilidade e respeito à privacidade. A eficácia continuada dependerá da adaptação constante, refletindo não apenas a evolução da tecnologia, mas também a evolução das expectativas sociais e legais em relação à proteção de dados.

Sugestões para futuras pesquisas e aprimoramentos na legislação.

Como esse tema ainda é muito recente, com a Lei datada de 2018 e sua aplicação continua pendente, que acarreta a falta de dados e estatísticas específicos e necessários para maior compreensão, aqui vão algumas sugestões para quem se interessar sobre o tema.

Impacto Econômico da LGPD; Avaliação da Eficácia da ANPD; Adaptação da LGPD a Tecnologias Emergentes; Comparação Internacional a Longo Prazo; Privacidade e Saúde Digital; Mecanismos de Resolução de Disputas; Educação e Conscientização Pública; Proteção de Dados na Pesquisa Científica; Revisão Periódica da LGPD e etc.

Essas sugestões podem servir como pontos de partida para futuras pesquisas acadêmicas e o aprimoramento contínuo da legislação de proteção de dados no Brasil. Destaco que a intenção é fazer crescer o interesse das pessoas, alcançado a real importância e relevância no qual eu considero que deveria ser tratado. Uma maior contribuição depende de ter acesso a estatísticas e dados que possam vir a ser divulgados, desde empresas a agências do governo, e alcance todos os níveis da sociedade.

• Referências Bibliográficas

https://civilistica.emnuvens.com.br/redc/article/view/510/384.

https://revistas.cesmac.edu.br/administracao/article/view/1035.

https://books.google.com.br/books?hl=pt-BR&lr=&id=oXPWDwAAQBAJ&oi=fnd&pg=PT13&dq=lgpd&ots=k84mHoMQ3L&sig=SZmXTfAbDq7GuAoHcCEBbrCVpKA&redir_esc=y#v=onepage&q=lgpd&f=false.

BRASIL. Lei nº 13.709/2018, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), Brasília, DF, 14 de agosto de 2018.

BRASIL. Lei nº 13.853/2019, de 08 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018 para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências, Brasília, DF, 08 de julho de 2019.

(1) WIMMER, Miriam. A Lei Geral de Proteção de Dados (LGPD) e o setor produtivo. In: Revista do BNDES, Rio de Janeiro, v. 25, n. 49, p. 55-80, dez. 2018. (1)

(2)Dayana Caroline Costa, 2018. https://www.migalhas.com.br/depeso/277799/tres-grandes-motivos-para-o-brasil-se-preocupar-com-o-regulamento-geral-de-protecao-de-dados-da-uniao-europeia.

(3) FRAZÃO, Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis. https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018.(3)

(4) MALDONADO, Viviane Nóbrega. BLUM, Opice Renato. LGPD: Lei Geral de Proteção de Dados Comentada. 2ª ed., São Paulo: Thomson Reuters Brasil, 2020. pg. 82. (4)

(5) PINHEIRO, Patrícia Peck. Proteção de Dados Pessoais. Comentários à Lei nº 13.709/2018. São Paulo: Saraiva, 2018. pg. 48. (5)

(6) MALDONADO, Viviane Nóbrega. BLUM, Ópice Renato. LGPD: Lei Geral de Proteção de Dados Comentada. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. pg. 108. (5)

(7) PINHEIRO, Patrícia Peck. Direito Digital. 6ª ed. São Paulo: Saraiva, 2016. (7)

(8) MALDONADO, Viviane Nóbrega. BLUM, Ópice Renato. LGPD: Lei Geral de Proteção de Dados Comentada. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. pg. 103. (8)

(9) MALDONADO, Viviane Nóbrega. BLUM, Opice Renato. LGPD: Lei Geral de Proteção de Dados Comentada. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. pg. 113. (9)

(10) https://febrabantech.febraban.org.br/blog/lgpd-esta-fora-da-realidade-de-80-das-empresas-no-brasil-diz-estudo**. (10)**

(11) ANPD. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Brasília, Maio/2021. https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf **(11)**

(12) ALCASSA, Flávia. CORREIA, Umberto. CRISOSTOMO, Juliana Neves. LIMA, Adrianne. PINHEIRO, Patrícia Peck. TUFAILE, Cinthia. "Advogados - encarregados (DPO interno e DPO as a service)" Nos programas de governança em privacidade (LGPD). Migalhas. Disponível em: <https://www.migalhas.com.br/depeso/345714/advogados--encarregados-dpo-interno-e-dpo-as-a-service**> (12)**

(13) LIMA, Adrianne. Migalhas. Disponível em: <https://www.migalhas.com.br/depeso/345714/advogados--encarregados-dpo-interno-e-dpo-as-a-service**> (13)**

BAPTISTA LUZ ADVOGADOS. Lei Geral de Proteção de Dados e GDPR: Histórico, análise e impactos. Disponível em: <https://baptistaluz.com.br/institucional/manual-normativo-lei-geral-de-protecao-de-dados-e-gdpr**/ >.**

SARLET, Ingo Wolfgang. MARINONI, Luiz Guilherme. MITIDIERO, Daniel. Curso de Direito Constitucional. São Paulo: Saraiva, 2018. 497.

MALDONADO, Viviane Nóbrega. BLUM, Opice Renato. LGPD: Lei Geral de Proteção de Dados Comentada. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. pg. 109.

SARLET, Ingo Wolfgang. MARINONI, Luiz Guilherme. MITIDIERO, Daniel. Curso de Direito Constitucional. São Paulo: Saraiva, 2018.

MALDONADO, Viviane Nóbrega. BLUM, Opice Renato. LGPD: Lei Geral de Proteção de Dados Comentada. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020.

PINHEIRO, Patrícia Peck. Proteção de Dados Pessoais. Comentários à Lei nº 13.709/2018. São Paulo: Saraiva, 2018

São Paulo, 15 de dezembro de 2023.

_____

Assinatura do Aluno orientando

(Marcos Henrique Bandeira – R.A. 819161261)