CENTRO UNIVERSITÁRIO BRASILEIRO – UNIBRA

CURSO DE GRADUAÇÃO TECNÓLOGO EM

REDES DE COMPUTADORES

FERNANDO HENRIQUE DA SILVA CONSTANTINO

GALVANI DE SOUSA LOBO JUNIOR

PAULO NASCIMENTO DA SILVA FILHO

# A APLICAÇÃO E ADEQUAÇÃO DAS EMPRESAS AOS CRITÉRIOS DA LGPD

RECIFE/2021

FERNANDO HENRIQUE DA SILVA CONSTANTINO

GALVANI DE SOUSA LOBO JUNIOR

PAULO NASCIMENTO DA SILVA FILHO

# A APLICAÇÃO E ADEQUAÇÃO DAS EMPRESAS AOS CRITÉRIOS DA LGPD

Trabalho de conclusão de curso apresentado ao centro universitário brasileiro - UNIBRA, como requisito parcial para obtenção do título de tecnólogo em redes de computadores.

Professor Orientador: Msc Ameliara Freire Santos de Miranda

RECIFE/2021

S586a Silva, Fernando Henrique da
A aplicação e adequação das empresas aos critérios da LGPD / Fernando Henrique da Silva Constantino, Galvani de Souza Lobo Junior e Paulo Nascimento da Silva Filho. - Recife: O Autor, 2021.
37 p.

Orientador (A): Me. Ameliara Freire Santos Miranda

Trabalho de Conclusão de Curso (Graduação) Centro Universitário Brasileiro – UNIBRA Graduação Tecnológica em Redes de Computadores, 2021

1. LGPD. 2. GDPR. 3. Banco de dados. l. Centro Universitário Brasileiro. – Unibra.Il. Título.

CDU: 616-083

FERNANDO HENRIQUE DA SILVA CONSTANTINO

GALVANI DE SOUSA LOBO JUNIOR

PAULO NASCIMENTO DA SILVA FILHO

# A APLICAÇÃO E ADEQUAÇÃO DAS EMPRESAS AOS CRITÉRIOS DA LGPD

Artigo apresentado ao centro universitário brasileiro - UNIBRA, como requisito parcial para obtenção do título de tecnólogo em redes de computadores.

Professor Orientador: Msc Ameliara Freire Santos de Miranda.

_____

Prof.° Msc Ameliara Freire Santos de Miranda

Professor(a) orientadaor(a).

_____

Prof.° Msc Aline Ferreira Barbosa

Professor(a) examinador(a).

_____

Prof.° Msc Adilson da Silva

Professor(a) examinador(a).

Recife, __/__/____

NOTA:_____

*Dedicamos esse trabalho a nossos pais, amigos e mestres*.

## AGRADECIMENTOS

Agradecemos a Deus, pois sem ele, a elaboração desse trabalho não teria êxito; agradecemos aos nossos pais, pois sem os incentivos deles, esta formação não seria alcançada; agradecemos à nossa orientadora, pois sem a sua ajuda, não conseguiríamos chegar até aqui.

*“Nunca estou realmente satisfeita quanto a entender alguma coisa; porque, até onde entendo, a minha compreensão só pode ser uma fração infinitesimal de tudo o que eu quero compreender.”*

*(Ada Lovelace)*

**SUMÁRIO**

# A APLICAÇÃO E ADEQUAÇÃO DAS EMPRESAS AOS CRITÉRIOS DA LGPD.

FERNANDO HENRIQUE DA SILVA CONSTANTINO
GALVANI DE SOUSA LOBO JUNIOR
PAULO NASCIMENTO DA SILVA FILHO
AMELIARA FREIRE SANTOS DE MIRANDA

**Resumo:** O processo de desenvolvimento deste trabalho consiste na divulgação da informação técnica da LGPD (Lei Geral de Proteção de Dados), pesquisas que mostram o déficit de conhecimento da lei, para usuários e administradores, problemas identificados em empresas na implementação da lei, além de boas práticas do uso de dados.

A lei tem como objetivo proteger as informações sigilosas do cliente/usuário, trazendo uma segurança maior e transparência a respeito dos dados pessoais do cliente físico ou jurídico, prevendo punições para o descumprimento em casos de vazamentos, ou outras irregularidades, conforme normas baseadas na GDPR (Regulamento Geral sobre Proteção de Dados).

Na atualidade, a informação de dados é de suma importância, pois a maioria dos sistemas hoje são integrados a um determinado banco de dados, se tornando um recurso informacional, gerando valores fundamentais para gerar um mundo cada vez mais conectado. A implementação da LGPD em uma empresa consiste em um processo que envolve muitas etapas e um custo elevado de estrutura, equipamentos e capacitação dos profissionais.

**Palavras-chave:** LGPD. GDPR. Banco de dados.

## 1 INTRODUÇÃO

Com a criação da lei 13.709 (lei geral de proteção de dados), a agregação de sigilo e interação do usuário/cliente necessitou de uma adequação das empresas ao gerenciamento de dados, onde torna o uso ciente das informações que lhe foram

asseguradas, por meio de práticas transparentes e seguras. Esta criação, porém, demanda de certa estrutura para seu correto funcionamento, tornando necessário um investimento na preparação dos funcionários.

Pode-se dizer que:

> A LGPD tem como objetivo proteger dados pessoais de pessoas naturais, ou seja, pessoas físicas. Este é o primeiro ponto: a LGPD não tem como escopo os dados das empresas (pessoas jurídicas), mas sim os dados que as empresas têm das pessoas físicas, seja elas funcionárias, terceiras, clientes, acionistas etc. – ou seja, todo mundo. (GARCIA, 2020).

Segundo Lucca (2020, p. 23): “fica claro que as empresas que se adequarem à LGPD, o quanto antes sairão ganhando, podendo, inclusive, usar dessa premissa como uma forma de marketing para sua empresa, uma vez que a busca do usuário é a efetiva proteção de seus dados”.

O trabalho inclui uma situação que ocorreu no mundo, com a Cambridge Analytica e o Facebook, afetando vários usuários no vazamento de informações. Enfatizando o quão é importante uma estrutura LGPD deve ser adequada. A segurança de dados é o foco principal de uma empresa que pretende implementar a LGPD, tendo uma confiabilidade para com o cliente, através de um gerenciamento de dados especializados e transparente (ALTASNET, 2021)

## 1.1 Problemas

De acordo Lehfeld, Celiot, Siqueira, Barufi (2021):

> Vírus de computadores e programas com malware incluídos em pacotes de software ou arquivos aparentemente inofensivos são os meios mais comum através dos quais se praticam crimes ou violações digitais. A partir disso, por exemplo, se roubam perfis de redes sociais, acessam contas bancárias e fraudam cartões de créditos. Inobstante, quase nove em dez adultos reconhece a potencialidade da ocorrência de um crime cibernético, menos de um quarto espera ser vítima dele. No mesmo sentido, apenas metade se diz disposto a mudar sua forma de comportamento online para evitar tornar-se uma vítima.

Na LGPD, o consentimento do consumidor é um dos fatores principais e necessário pois a propriedade dos dados tratados foi e sempre será do seu titular, motivo pelo qual pode revogar a qualquer tempo o consentimento.

Quando uma empresa não cumpre a lei, pode ter empecilhos com parceiros e clientes próximos. Isso acontece porque o consumidor final dos produtos e/ou serviços está cada vez mais criterioso, desconfiado de corporações que não contam com boas práticas internas, o impacto com contatos internacionais será ainda mais severo, uma vez que muitos países já estão em dia com o plano de proteção de dados.

É preciso ter uma cultura direcionada para a proteção de dados, que mesmo arcando com a penalidade, pode trazer outros riscos financeiros, uma vez que pode impactar negativamente nos setores da empresa

### 1.2 Objetivos gerais

O presente trabalho tem como objetivo fornecer informações a respeito da LGPD para empresas e usuários que não possuem conhecimento da nova lei de proteção de dados.

### 1.3 Objetivos específicos

Realizar análise e estudo de implementação da LGPD em empresas que buscam zelar pela segurança e privacidade de informações pessoais, sugerir boas práticas no uso de dados, informar problemas das empresas para implementação da LGPD, citar normas e penalidades caso haja o descumprimento da lei, mostrar o tratamento de dados a ser feito pela as empresas e analisar a pesquisa feita com usuários e administradores a respeito da lei.

## 2 DELINEAMENTO METODOLÓGICO

Durante o desenvolvimento deste trabalho, foi aplicada a técnica de documentação indireta, com embasamento em artigos, publicações e depoimentos, e a técnica de documentação direta, onde foi efetuada a pesquisa de campo com meios

quantitativos e qualitativos. Foram escolhidos para fazerem parte desta pesquisa 20 empresários e 20 pessoas físicas, totalizando 40 pessoas.

A importância que esses empresários fundamentaram para a elaboração deste, evidencia o quão disseminada esta lei foi, e o quanto que ela é realmente aplicada na sociedade em geral. As pessoas físicas mostraram o quanto a informação sobre a lei é desconhecida, tornando-as refém de um sistema antiquado e impróprio à revolução tecnológica que se encontra eminente.

## 3 REFERENCIAL TEÓRICO

Ao longo destes capítulos, será abordado os aspectos que pesaram para o desenvolvimento da lei, sobre como deve ser feita a aplicação da LGPD, de como um usuário deve ser informado sobre o uso dos seus dados, e as implicações postas às empresas caso haja o descumprimento dos parâmetros. Com as descrições a seguir sendo baseadas em evidências coletadas com empresários locais, tornamos este trabalho autêntico e evidenciamos como os microempresários e os cidadãos locais estão sendo informados sobre a aplicação da lei estabelecida.

### 3.1 O que impulsionou a criação da LGPD?

Impulsionado pelo General Data Protection Regulation ou Regulamento Geral Sobre a Proteção de Dados (GDPR), com base em leis antigas, datadas desde 1995 da União Europeia (CAETANO, 2020), ela visa tornar o usuário ciente de como será gerenciada a informação concedida.

Com o avanço da tecnologia no mundo e a globalização da internet, tornou-se de extrema importância a manutenção da privacidade dos dados fornecidos pelos usuários. Após diversos vazamentos de dados da plataforma social, como por exemplo o Facebook e o escândalo da Cambridge Analytica em 2018, entrou em discussão como esses dados serão manipulados e qual será o destino dessas informações após o seu devido uso.

#### *3.1.1 A Cambridge Analytica e a falha do Facebook*

Fundada em 2013, a Cambridge Analytica utilizava de mineração e análise de dados para ajudar em divulgação política nos Estados Unidos (FORNASIER; BECK, 2020). Em 2016, começou a apoiar Donald Trump em suas campanhas e ao Brexit (saída do Reino Unido da União Europeia). Questionada sobre a sua metodologia de abordagem e o impacto que estava causando à sociedade, a empresa começou a ser investigada nos Estados Unidos e União Europeia. Em 17 de março de 2018, jornais americanos divulgaram informações de que a empresa havia se beneficiado de dados sensíveis e sem o consentimento de alguns usuários da plataforma Facebook. O CEO da rede social foi questionado sobre como a empresa se beneficiou da vulnerabilidade dos seu software (FORNASIER; BECK, 2020), em resposta, Mark Zuckerberg disse que não sabia dessa utilização dos dados. Mais tarde, foi confirmado que o Facebook sabia sim sobre essa falha há mais de dois anos, e que nada havia sido feito para que não houvesse tal manipulação. Ao total, cerca de 87 milhões de usuários foram atingidos pela fraude, e dentre esses, 4,5 milhões de Brasileiros foram vítimas também.

O real uso dessas informações, tais como: linha do tempo, locais visitados, tipos de filmes e culturas, foram usados clandestinamente para efetuar uma persuasão de suas escolhas políticas, tornando claro a real necessidade de um sistema de leis que protegessem seus usuários a qualquer momento e em qualquer lugar.

## 4 NORMAS DA LGPD

Os critérios da LGPD não se aplicam apenas aos meios digitais, mas também às empresas físicas e órgãos públicos que se beneficiam das informações consideradas sensíveis e de dados pessoais à pessoa física ou jurídica. Entrando em vigor a partir do dia 1° de agosto de 2021, a lei está tentando dar prazo às empresas para que se adequem as tais normas, como algumas citadas abaixo, de acordo com o art. 6° da lei n° 13.708, de 14 de agosto de 2018 (BRASIL, 2018):

1. Criação de um banco de dados específicos para armazenar essas informações com o consentimento do usuário.
2. Capacitação de funcionários sobre como tratar os dados cedidos.

3. Transparência e não uso excessivo de palavras técnicas para designar como será feito o tratamento dos dados.
4. Esclarecimento do destino dos dados após sua utilização.
5. Disponibilizar um canal de atendimento próprio para realizar a exclusão dos dados.

## 4.1 O que pode acontecer caso haja o descumprimento da lei?

Com multas definidas para quem descumprir tais regras, o governo federal visa estabelecer ciência e controle de como esses dados podem ser usados. Diversos adiamentos ocorreram para a sua devida aplicação, porém, como há uma grande demanda das empresas para aperfeiçoarem seus bancos de dados e funcionários, esses adiamentos se tornam benéfico para as empresas, mas, algumas se apropriam deste problema. Uma prática muito comum que será proibida é o compartilhamento das informações pessoas de um cidadão.

Exemplo: Um cliente deve à uma empresa A. Uma empresa B compra a dívida da empresa A e os dados do cliente é cedido sem o seu consentimento.

Conforme cita o art. 7°, do cap. 2 da lei 13.708:

> § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei (BRASIL, 2018).

Seguindo este artigo, torna-se claro que a necessidade por uma grande infraestrutura será necessária para atender a demanda que irá ocorrer por parte do cliente/usuário ao solicitar algum esclarecimento dos métodos utilizados.

### *4.1.1 A fiscalização para padronização e aplicação da lei*

A regulamentação será feita pela Autoridade Nacional de Proteção de dados Pessoais (ANPD). Criada por uma medida provisória de número 869/18, na data de 27 de dezembro de 2018, ela tem como objetivo a aplicação das normas estabelecidas pela LGPD e a preservação da integridade física e pela moralidade da vida digital. Com esta criação, o Brasil entrou na lista de países que estão de acordo com a GDPR, da União Europeia.

Com um órgão federal destinado à fiscalização, a não aplicação das obrigatoriedades citadas poderá acarretar em: multas de até R$ 50 milhões por infração cometida, suspensão do alvará de funcionamento por tempo indeterminado, suspensão parcial do direito de funcionamento.

Segundo o art. 9°, da lei 13.708, de 14 de agosto de 2018 (Brasil,2018), ainda é destacado pontos que devem ser seguidos estritamente como:

- Finalidade: deve ser informado ao cedente dos dados, de forma clara e explícita, para qual propósito servirá aquele dado;
- Adequação: os dados cedidos dever servir apenas para o que foi proposto mediante contrato ou acordo;
- Necessidade: deve-se utilizar do mínimo possível de tais dados para sua finalidade, evitando o excesso e limitando-se apenas ao necessário;
- Livre acesso: garantia de acesso integral e gratuito aos dados concedidos pelos fornecedores das informações;
- Qualidade dos dados: deverá ser informado ao titular dos dados, a importância e necessidade que tal informação cedida terá em seu uso;
- Transparência: definir com exatidão e clareza quem irá administrar e gerenciar; os dados fornecidos, consolidando o fácil acesso a essas informações;
- Segurança: evitar acesso indevido aos dados. com um bom gerenciamento e administração das informações, impedindo as chances de acontecer algum vazamento ou ataque cibernético;
- Prevenção: utilizar de ferramentas específicas para evitar algum tipo de dano no tocante ao tratamento dos dados;
- Não discriminatório: não se apropriar dos dados para fins antiéticos, para fins de exclusão social mediante etnia, crença, religião e orientação sexual;

- Responsabilidade e prestação de contas: comprovar que as medidas adotadas pela retentora das informações cedidas são, de fato, eficazes, e mostrar que todas as obrigatoriedades informadas conforme a LGPD determina sejam compridas.

## 5 O CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE (CNPD)

Com proposta de estabelecer o vínculo entre a ANPD e a população, essa não é sua principal função. O serviço contará com 23 representantes, sem serem remunerados, pois será considerado um serviço de prestação pública, de acordo com o decreto n°10.474/2020. Entre suas atribuições estão: fornecimento de subsídio sobre como a ANPD pode e deverá aplicar suas medidas baseadas na lei, propor o compartilhamento de conhecimento sobre como as normas devem ser cumpridas e como as empresas tratam esses dados, emitir relatórios anuais de como as abordagens vêm sendo cometidas pelo órgão federal, propor novas abordagens e estratégias para o aprimoramento da LGPD, segundo o Art.58-B da lei n°13.709, de 14 de agosto de 2018 (Brasil, 2018) . Com abrangência nacional, a CNPD deve facilitar o acesso de qualquer cidadão ao seu respectivo dado cedido, aumentado a transparência em suas abordagens.

## 6 O PROCESSO DE IMPLEMENTAÇÃO DA LGPD NAS EMPRESAS

As empresas devem ser capazes de mostrar competência e capacidade para gerenciar os dados de seus respectivos fornecedores. Com a criação da lei impactando diretamente o funcionamento das empresas, prazo é crucial para a devida aplicação de todas as exigências.

Relatórios simplificados, de fácil compreensão, de livre acesso e de disponibilidade gratuita devem ser acordados mediante aceitação explícita do cedente das informações. Também deverá ser criado uma plataforma para contato direto com os mediadores da empresa que gerenciam os dados, e do órgão federal responsável pela análise das condutas realizada pela empresa, afim de prestar total transparência em suas análises e métodos.

A lei ainda determina a criação de três cargos responsáveis por distintas atividades, conforme cita o art.5° da lei 13.708, de 14 de agosto de 2018 (Brasil, 2018). Ambas se correlacionam e têm algumas atribuições em comum, como por exemplo podendo ser alguma pessoa ou empresa, de poder público ou privado. São elas:

1. Controlador: lhe é assegurado a responsabilidade de definir qual tipo de tratamento e qual finalidade vai ter aquele dado. Também é responsável pelas multas previstas pela lei caso aja irregularidade em sua manipulação ou destinação.
2. Operador: será essa pessoa que vai manipular esse dado. Sendo subordinado ao controlador, o mandatário que receber essa atribuição terá a responsabilidade de trabalhar em cima do que foi combinado com o controlador, afim de estabelecer concordância e ordenamento com a lei.
3. Encarregado: intitulado para estabelecer vínculo e contato entre o controlador, a pessoa que cedeu os dados e a ANPD, afim de prestar transparência e concordância em sua abordagem, metodologia e objetivos na hora de tratar esses dados.

## 7 O IMPACTO DA INSTAURAÇÃO DA LEI NO BRASIL, E A TENDÊNCIA DE BAIXA NOS CASOS DE FRAUDE VIRTUAL

A fim de estabelecer total controle sobre como as empresas e os órgãos públicos devem utilizar os dados fornecidos, ela também visa proteger quem está cedendo as informações, pois, dados como o CPF, e-mails, número de telefone e entre outros são dados de pessoas identificadas; já os dados referentes a pessoa identificável se remete aquelas informações onde, através de mineração de dados, se obtêm informações precisas de suas movimentações diárias. Tais empresas devem, por meio desta lei, ser responsável pelo armazenamento seguro destas informações, pois, caso contrário, pode se tornar vítima de diversos ataques cibernéticos.

Com essa liberdade de transação que era feita sobre os dados, era possivel efetuar das mais variadas fraudes virtuais. A mais usada em 2020 foi a tentativa de phishing, onde se é feito a tentativa de roubar os dados da pessoa, forjando um site que requesita tais dados para cometer a ilicitude, e também pelo o envio de e-mails maliciosos, sms e dentre outros meios. Segundo levantamento, por causa da

pandemia, esse número aumentou ainda mais, chegando a 120% em comparação ao mês de fevereiro e março (AGENCIABRASIL, 2021). Fraudes como essas fizeram o Brasil chegar ao primeiro lugar no ranking mundial de tentativa de roubo de dados por phishing e spam (AGENCIABRASIL, 2021); com esses dados, torna-se claro a necessidade da implementação da LGPD e um sistema robusto capaz de manter a proteção destes dados.

Implementado a robustez da LGPD e a fiscalização que será feita pela ANDP junto ao CNPD, é promissor que a queda destes números ocorra desde a completa instauração da lei, até sua plena abrangência.

## 7.1 Roubo de dados no Brasil e como essa prática compromete a relação entre a empresa e órgão com seus usuários e clientes

Com o aumento de casos sobre roubos de dados em uma crescente frenética, o governo tem que implementar um sistema capaz de suportar a devida demanda das empresas, lhe instruindo e auxiliando em um desenvolvimento eficaz contra esses tipos de práticas. Por causa da pandemia, o DATAPREV necessitou de criar um banco de dados capaz de suportar cerca de 97 milhões de dados extremamente confidenciais para o auxílio emergencial (BARTHOLO *et al.*, 2020) e garantir que esses dados não fossem vazados ou hackeados. Diversos testes foram efetuados no site da caixa para assegurar que não houvesse falha, mas, foram encontradas algumas que permitiam o acesso indevido dessas informações confidenciais, segundo o pesquisador de segurança que havia feito a denúncia: Heitor Gouvêa. Ele relatou que o site da caixa tinha uma falha que permitia um ataque via open redirect, onde ele consiste em um redirecionamento do usuário dentro do próprio site da caixa, fazendo com que o usuário concedesse acesso aos seus dados para os criminosos, segundo (Payão, 2020). Com a vigência da LGPD, formas de implementar segurança aos bancos de dados das empresas e órgãos serão distribuídas, a fim de estabelecer a confiança nesses vínculos criados.

## 8 A FALTA DE IMPLEMENTAÇÃO DE SEGURANÇA E IMPRUDÊNCIA NA ADMINISTRAÇÃO NOS BANCOS DE DADOS DAS EMPRESAS NO MUNDO E MEDIDAS CABÍVEIS PARA ACABAR COM ESSA PRÁTICA.

Diversos vazamentos recorrentes marcaram a real necessidade de um sistema eficaz, capaz de tornar um sistema absoluto em termos de falhas, mas, para isso acontecer, é necessário um alto investimento em seus servidores e em seus profissionais de segurança. Um caso que ficou marcado como um dos maiores vazamentos de dados da história foi a do famoso site Yahoo, onde foi responsável pelo vazamento de dados de cerca de 194 milhões de pessoas e a divulgação de 896 milhões de contas de usuários da plataforma entre o período de 2013 até 2016 (ISTOEDINHEIRO, 2019). Com a negligência evidenciada, a empresa foi vendida por US$ 4,48 bilhões e teve um investimento de cerca de US$ 306 milhões em segurança da informação e um aumento considerável na quantidade de profissional da área responsável pela proteção dos dados.

Vítima também dos ataques criminosos, a Uber teve um vazamento de 57 milhões de dados no ano de 2016 (ASSISEMENDES, 2020), entre eles: carteira de habilitação, número de celular e e-mails. A empresa chegou a negociar um acordo com os criminosos para que eles apagassem os dados e implementou um sistema mais robusto para evitar tais vazamentos.

Seguindo essa mesma conduta inadequada de implementar segurança após a falha no sistema ser explorada, a Adobe, empresa de software americana também sofreu um ataque que comprometeu os dados bancários e pessoais de 154,5 milhões de pessoas, mas a empresa confirma que foram 38 milhões. O ataque consistiu em uma invasão ao servidor antigo da empresa, onde não havia mais o suporte adequado para manter a segurança de tais dados. (MENDES, Adriano. 2020).

Evidenciando tais problemas em que as empresas têm em seguir tais protocolos para manter a segurança de seus usuários, tornando seus sistemas eficazes somente após os crimes cometidos, torna-se de extrema urgência que algum órgão supervisione se tais medidas, de seus respectivos países e leis, averigue que todas as normas estabelecidas sejam seguidas e que seus protocolos sejam respeitados, afim de manter todos os usuários em segurança. A criação dessa lei também impacta na transação de dados internacionalmente, pois, assim como na

União Europeia, é obrigatório que qualquer empresa que trate os dados do povo Europeu, é necessário que esteja de acordo com as normas da GDPR, assegurando que o seu cidadão terá direito ao sigilo e proteção de seus dados assegurada pela empresa.

O Brasil também irá seguir esse modelo, pois com os aumentos expressivos de roubo de dados, certas medidas devem ser postas, tais como as multas previstas e outras penalidades nas quais já foram citadas anteriormente, firmando que o cumprimento deve ser adotado por todas as empresas, setores públicos e privados.

## 9 A APLICAÇÃO DA PENALIDADE

Apesar da LGPD já ter entrado em vigor desde setembro de 2020, as penalidades apenas serão aplicadas a partir do dia 1° de agosto de 2021. Sendo assim, as empresas tiveram prazo para iniciar sua adequação, porém, caso haja a detecção da má conduta na utilização dos dados, a empresa será notificada pela ANPD para realizar a correção de tais falhas, se ainda houver o descumprimento da lei, será decretada a multa de 2% em cima do faturamento da empresa, limitado até R$50 milhões, e ainda estará sujeita a outras penalidades. A empresa também pode e deve ser observada pelos seus usuários, funcionários e clientes para confirmar que os dados estão sendo usados de forma combinada e que sua integridade está sendo mantida, preservando sua etnia, raça e escolha sexual.

## 10 OS PROBLEMAS ENCONTRADOS PELAS EMPRESAS PARA IMPLEMENTAR A LEI.

Os problemas que as empresas vêm encontrado consistem no aperfeiçoamento de sua equipe técnica até a preparação do servidor que irá armazenar tais informações. Em parte, por se tratar também de aperfeiçoamento pessoal, haverá demanda para os funcionários, pois a responsabilidade do tratamento cairá sobre ele. Complementando a lista, os servidores da empresa devem ser testados para estabelecer a segurança do mainframe.

É aconselhado a contratação de um Security Pentesting, pois ele irá fazer o teste de vulnerabilidade do sistema, proporcionando segurança e confiança aos seus clientes. Para evitar que maiores problemas ocorram durante a implementação, a empresa é aconselhada a contratar uma assessoria jurídica capaz de orientar aos critérios determinados e evitar que a empresa seja multada.

Por mais que a lei tente ajudar as empresas, sua agregação irá gerar custos e uma maior disponibilidade de acesso ao banco de dados poderá causar quedas e travamentos constantes no site caso haja uma simultaneidade de acesso por parte de seus clientes, mas, mesmo com esse alto investimento, a empresa tende a ter rapidamente o capital investido, pois com segurança e confiança agregada aos seus princípios, isso irá destacar a empresa rente a concorrência.

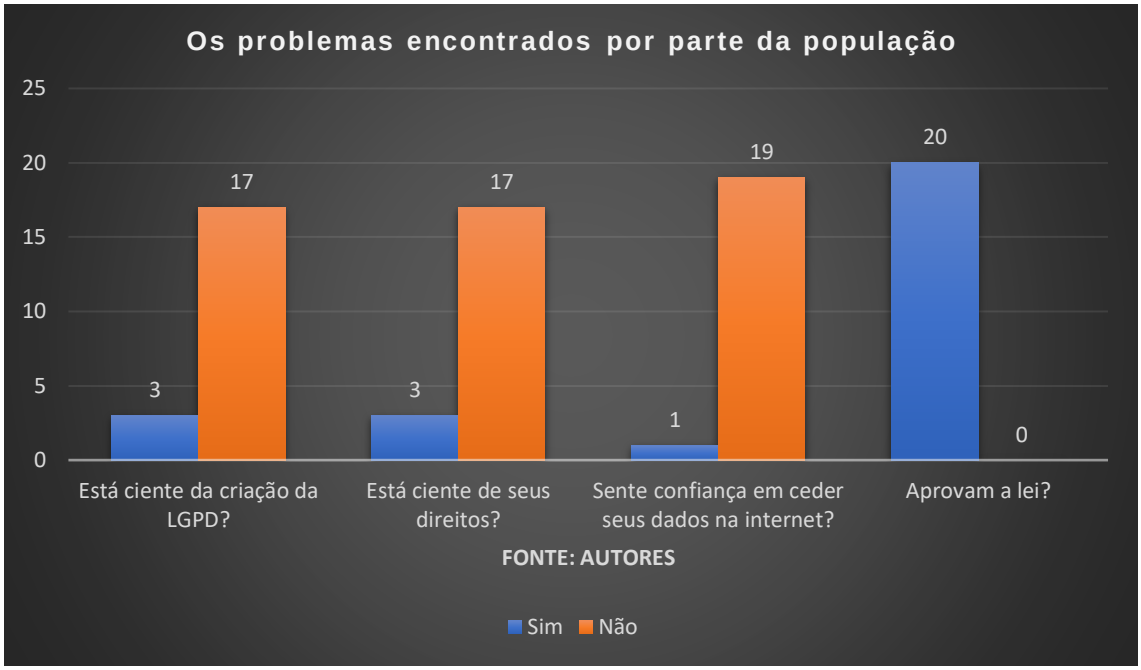
Quando se trata de empresas que utilizam os dados de seus clientes de forma não virtual, armazenando seus dados em espaços físicos, caberá a empresa responder aos mesmos critérios que se elegem ao tratamento de dados virtualmente, informando ao cedente qual a utilidade do dado concedido e fornecendo seu devido acesso. A lei abrange todas as empresas e órgãos governamentais que tratam de informações sensíveis e de dados pessoais, de forma virtual ou não; isso marca a postura de estabelecer a abrangência nacional dos critérios da lei.

### 10.1 Os problemas encontrados por parte da população

A pesquisa reuniu 40 voluntários, entre eles, estão: 20 pessoas físicas, de uma faixa-etária entre os 15 até os 70 anos. E um grupo de 20 empreendedores locais, formais e informais, entre os 30 e 60 anos.

Baseado em pesquisa feita com a população e a equipe, foi apurado os seguintes resultados:

Figura 1




Conforme mostra as evidencias e estatísticas coletadas, foi deduzida à conclusão de que há um déficit sobre a informação referente a todos os aspectos da lei sobre a população.

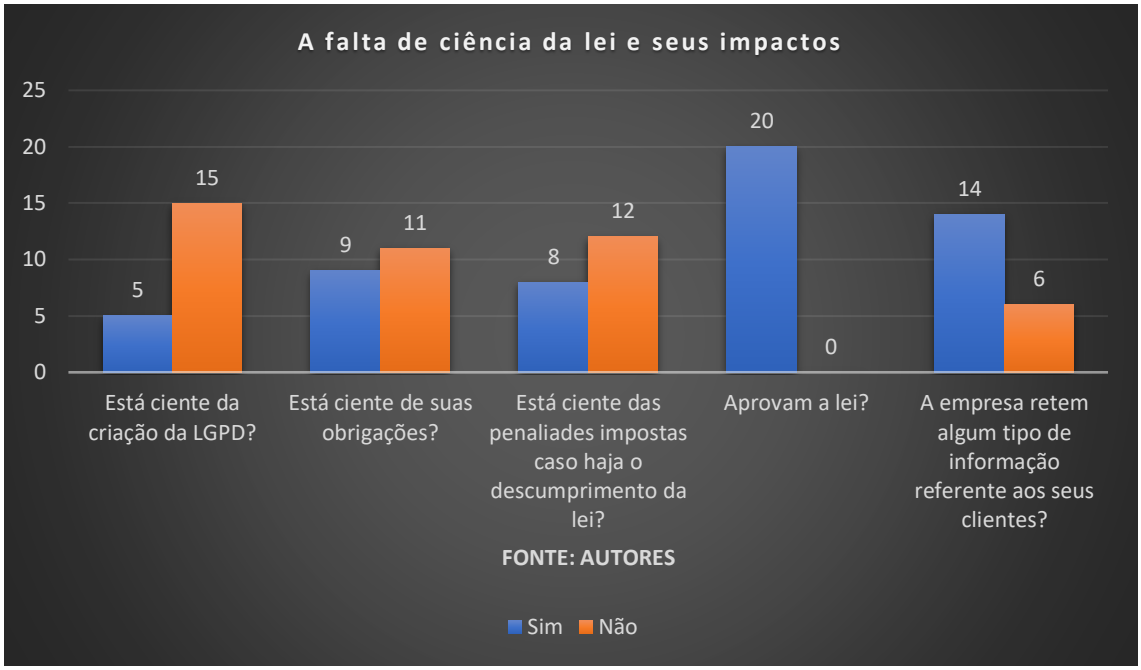
O não conhecimento destas práticas torna o público mais suscetível a várias práticas ilegais com os seus dados até a golpes mais complexos.

É evidenciado também que 99% dos entrevistados não sentem confiança na internet, pois se sentem vulneráveis a quaisquer ilicitudes encontrada no mundo virtual. Tendo isso em vista, o que contribui para tal valor elevado sobre a confiança na internet, é a falta de divulgação dos sistemas de proteção oferecidos, tanto pelas próprias plataformas digitais, como por parte da mídia.

A falta de oportunidade ao acesso das informações facilitada torna a população obsoleta em sua maioria, a tornando refém de sistemas antigos e antiquados à nossa geração. Muitas pessoas também não sabiam sequer da existência dessa lei, onde foi informado todos os parâmetros que a LGPD padronizará a todas as empresas; o resultado não poderia ser mais expressivo: 100% dos entrevistados aprovaram a criação da lei.

### *10.1.1 Os resultados obtidos mediante análise de pessoas administradoras entrevistadas*

Figura 2




Conforme as estatísticas, é evidente que a desinformação circunda também os administradores. Essa convivência com a desinformação pode causar diversos transtornos aos gestores de seus comércios, pois cerca de 70% dos administradores entrevistados usam de dados pessoais para fazer seu comércio.

É mostrado também que 60% dos entrevistados não estão cientes das penalidades previstas caso haja a constatação do não cumprimento da lei. A movimentação desses dados pode desempenhar um grande papel na hora de administrar o comércio, pois com o seu uso correto, é possível desenvolver grandes estratégias para alavancar o fluxo de caixa, agindo diretamente sobre os desejos de seus clientes.

## 11 TRATAMENTO DE DADOS PESSOAIS

(seção I: Requisitos para o tratamento de dados pessoais)

Tratamento de dados inclui toda operação realizada com dados pessoais, como: a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Na Lei geral de proteção de dados foi determinado que:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (BRASIL, 2018, p. 59)

- Mediante o fornecimento de consentimento pelo titular;
- Para o cumprimento de obrigação legal ou regulatória pelo controlador;
- Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
- Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
- Para a proteção da vida ou da incolumidade física do titular ou de terceiros; (BRASIL, 2018, p. 59)

> **Art. 9º** O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: (BRASIL, 2018, p. 59)

- Finalidade específica do tratamento;
- Forma e duração do tratamento, observados os segredos comercial e industrial;
- Identificação do controlador;
- Informações de contato do controlador;
- Informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

- Responsabilidades dos agentes que realizarão o tratamento; e
- Direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei (BRASIL, 2018, p. 59).

(Seção II: Tratamento de dados pessoais sensíveis)

O tratamento de dados pessoais sensíveis é aquele cujo procedimento deve ser mais cauteloso, priorizando a atenção aos princípios e aos direitos dos titulares. Caso haja um eventual incidente de segurança envolvendo esses tipos de dados, as consequências podem ser mais graves aos direitos e liberdades dos titulares.

> O artigo 11 do tratamento de dados pessoais sensíveis da lei 13.709 de 2018 somente poderá ocorrer em algumas das hipóteses abaixo: (BRASIL, 2018, p. 59)

- Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
- Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) Cumprimento de obrigação legal ou regulatória pelo controlador;
b) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
c) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
d) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
e) Proteção da vida ou da incolumidade física do titular ou de terceiros; (BRASIL, 2018, p. 59)

(seção III: Tratamento de dados pessoais de crianças e adolescentes)

O número de crianças e adolescentes que utilizam a internet é cada vez maior e mais precoce. Eles utilizam a internet, dispositivos, aplicativos e mídias sociais com

naturalidade e destreza; todavia, não podemos esquecer que estão em condição peculiar como pessoas em desenvolvimento e merecem atenção especial em razão de sua vulnerabilidade. Portanto, toda essa habilidade precisa ser exercida com cautela. Nesse sentido, o ordenamento jurídico impõe como dever da família, da sociedade e do próprio Estado garantir com absoluta prioridade direitos e segurança das crianças e adolescentes, como diz o artigo 227, da Constituição Federal.

### 11.1 Quem são as crianças e adolescentes?

Parece uma pergunta óbvia, mas é de fundamental importância esclarecer esse ponto para compreender melhor o artigo 14 da LGPD.

Diferente de muitos países, que consideram crianças as que não possuem até 13, 14, 15 ou mesmo 16 anos completos, o ECA estabelece distinção entre criança - a pessoa até 12 anos de idade incompletos - e adolescente - entre 12 e 18 anos.

A preocupação da LGPD com o tratamento dos dados pessoais, conforme o artigo 1º da Lei Geral de Proteção de Dados.

> (Art. 1º 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.), tem por finalidade proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
>
> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente (BRASIL, 2018, p. 59).

1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o 1º deste artigo.
4º Os controladores não deverão condicionar a participação dos titulares de que trata o 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança (BRASIL, 2018, p. 59).

### *11.1.1 O que mudará com essa nova forma de tratamento de dados pessoais?*

A LGPD empodera os titulares de dados pessoais, fornecendo-lhes direitos a serem exercidos durante toda a existência do tratamento dos dados pessoais do titular pela instituição detentora da informação. A Lei prevê um conjunto de ferramentas, que, no âmbito público, traduzem-se em mecanismos que aprofundam obrigações de transparência ativa e passiva.

## 12 TRANSFERÊNCIA INTERNACIONAL DE DADOS

A transferência internacional de dados na LGPD é um importante fator que deve mudar a maneira como diferentes países se relacionam na era da informação.
A nova lei informa o seguinte sobre esse assunto:

- A LGPD estabelece apenas diretrizes genéricas a serem observadas pelas autoridades nacionais.

- Permite a transferência de dados pessoais para países ou órgãos internacionais que proporcionem grau de proteção de dados pessoais adequados ao previsto. A lei é breve quanto a este procedimento e elementos a serem considerados como adequados.
- Alega que a transferência internacional dos dados pode ser realizada independente de autorização específica caso a comissão europeia reconheça que o país terceiro assegure um nível de proteção adequado. Caso não, a transferência internacional estará condicionada a garantias adequadas, que devem ser asseguradas pelo Agente.
- Todos os procedimentos e elementos que são levados em consideração pela Comissão para a autorização da transferência estão descritos na GDPR.

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: (BRASIL, 2018, p. 59)

- Para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
- Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;
b) cláusulas-padrão contratuais;
c) normas corporativas globais;
d) selos, certificados e códigos de conduta regularmente emitidos;

- Quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
- Quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros;
- Quando a autoridade nacional autorizar a transferência;
- Quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

- Quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
- Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades (BRASIL, 2018, p. 59).

## 13 SEGURANÇA E BOAS PRÁTICAS

Os dados são considerados a principal matéria prima das empresas, sem eles não tem como falar de inteligência empresarial, inovação e crescimento. Os dados são um combustível, ou seja, são coletadas informações que são transformadas em conhecimento para a empresa. Entendendo essa valorosidade, é preciso respeitar a legislação e oferecer um ambiente seguro para que as pessoas entreguem suas informações.

Segurança e Sigilo de Dados, que tem um capítulo exclusivo na LGPD, é uma das discussões mais populares quando se trata da proteção de dados pessoais. De forma resumida, o objetivo da discussão é entender: “Como reduzir os riscos de ter dados vazados ou roubados?” (É importante ressaltar que a lei impacta todas as empresas, do baixo ao alto escalão).

Os artigos 46, 47, 48 e 49 da lei geral de proteção de dados esclarece a pergunta feita acima:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018, p. 59).

1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia,

especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (BRASIL, 2018, p. 59).

> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.
> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (BRASIL, 2018, p. 59).

1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

- A descrição da natureza dos dados pessoais afetados;
- As informações sobre os titulares envolvidos;
- a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata; e
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

- Ampla divulgação do fato em meios de comunicação; e
- Medidas para reverter ou mitigar os efeitos do incidente.

3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los (BRASIL, 2018, p. 59).

> Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares (BRASIL, 2018, p. 59).

## 14 BOAS PRÁTICAS E GOVERNANÇA

Os agentes de tratamento de dados pessoais - controladores e operadores -, no âmbito de suas competências, com relação ao tratamento de dados, podem elaborar individualmente ou por intermédio de associações regras de boas práticas e de governança, que determinem as condições de organização, os padrões técnicos, as normas de segurança, entre outros, nos termos do artigo 50, caput, da LGPD.

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018, p. 59).

1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

a) Implementar programa de governança em privacidade que, no mínimo:

demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
g) conte com planos de resposta a incidentes e remediação; e
h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
i) Demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei (BRASIL, 2018, p. 59).

3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

> Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais (BRASIL, 2018, p. 59).

Ao estabelecer as referidas regras, os controladores e os operadores devem levar em consideração, no que se refere ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade, bem como, a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados do titular. De mesma maneira, as regras de boas práticas e de governança devem ser atualizadas e publicadas de maneira periódica e podem ser reconhecidas e divulgadas pela Autoridade Nacional.

A Autoridade Nacional de Proteção de Dados (ANPD) é responsável por zelar pela proteção dos dados pessoais, com base na legislação; por elaborar as diretrizes

para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; por fiscalizar e aplicar sanções nos casos de tratamento de dados que descumprirem a legislação, por meio de processo administrativo, que assegure o contraditório, a ampla defesa e o recurso, entre outros (BRASIL, 2018, p. 59).

## 15 RESULTADO

O incentivo deste trabalho partiu-se do pressuposto de que as empresas encontram dificuldades em atualizar o seu banco de dados, pois o alto custo e a falta de profissional na área responsável pela vistoria de seus servidores, torna o processo de adequação mais lento, facilitando o uso indevido dos dados e os grandes vazamentos conforme vem acontecendo. O resultado que se obteve foi a qual objetivou a conclusão desta obra: a criação de uma lei que supervisione o tratamento de dados no Brasil; a LGPD.

Com tais problemas evidenciados, concluímos que as medidas para controlar e guiar a integração das empresas à lei estabelecida, a aplicação e adequação das empresas aos critérios da LGPD tornará o Brasil mais inclusivo, social e seguro para seus cidadãos.

A adoção de um perfil nas redes sociais voltado à dispersão da LGPD para com a população acarretará em um maior conhecimento aos mesmos sobre seus novos direitos, o que proporcionará uma melhor imagem da LGPD diante da sociedade.

## 16 CONSIDERAÇÕES FINAIS

No decorrer deste estudo, observou-se que a Lei Geral de Proteção de Dados (LGPD) é capaz de trazer ao sujeito uma proteção de dados extremamente eficiente, não só de forma ativa, mas de forma passiva também, garantindo uma maior privacidade, intimidade, honra, direito de imagem e a dignidade, além de garantir segurança jurídica.

Contudo, na operacionalização desse trabalho de final de curso, foi observado que grande parte dos cidadãos ainda, infelizmente, não está ciente dos seus direitos e da criação da lei. Essa falta de conhecimento pode gerar em uma série de

problemas, visto que o alicerce para o tratamento de dados é o consentimento dos cidadãos, exceto em casos que sejam indispensáveis, como, por exemplo, para o cumprimento de uma obrigação legal, execução de contratos, preservação da vida e integridade física de uma pessoa, dentre outras normas.

Essa dissertação procurou apenas fazer uma discussão prévia da importância e da atuação da Lei Geral de Proteção de Dados como ferramenta de proteção ao usuário, bem como do nível de conhecimento da mesma para com os cidadãos brasileiros. 62% das pessoas entrevistadas alegam nunca terem tido problemas com vazamento de dados. 75% dos brasileiros ainda não conhecem a LGPD (Serasa Experian, 2019).

Para projetos futuros visasse trabalhar na dispersão da Lei Geral de Proteção de Dados com as pessoas que estiverem ao alcance na nossa equipe, e também alertá-los sobre o risco de vazamento de dados, mesmo que os seus nunca tenham sido vazados, visto que o descuido é o gatilho para uma série de problemas sobre privacidade de dados na internet.

## REFERÊNCIAS


AGENCIABRASIL: **Brasil é o país com maior número de vítimas de phishing na internet**. 2021. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-03/brasil-e-o-pais-com-maior-numero-de-vitimas-de-phishing-na-internet#:~:text=Em%202020%2C%20o%20Brasil%20foi,se%20fazendo%20passar%20por%20ela.. Acesso em: 24 abr. 2021.

ALTASNET: **Proteção de dados na empresa: o guia completo com boas práticas baseadas na LGPD.** 2021. Disponível em: https://www.altasnet.com.br/protecao-de-dados-o-guia-completo-com-boas-praticas-baseadas-na-lgpd/.

BARTHOLO, Letícia *et al* (org.). **As Transferências monetárias federais de caráter assistencial em resposta à Covid-19 : mudanças e desafios de implementação**. {S.L}: Ipea, 2020. 24 p. Disponível em: http://repositorio.ipea.gov.br/handle/11058/10042. Acesso em: 16 jun. 2021.

BATISTELLA, Carla. **Quais as penalidades LGPD e quando elas começam a valer?** 2021. Disponível em: https://www.certifiquei.com.br/penalidades-lgpd/#:~:text=Penalidades%20LGPD%20s%C3%A3o%20uma%20s%C3%A9rie,dados%20pessoais%20realizadas%20pela%20empresa.&text=Mas%20as%20san%C3%A7%C3%B5es%20da%20Lei%20podem%20ir%20al%C3%A9m%20disso.. Acesso em: 30 abr. 2021.

BRASIL**. Constituição (2018). Lei nº 13.709**, de 14 de agosto de 2018. **Do Tratamento dos Dados Pessoais:** Dos requisitos para o tratamento dos dados pessoais. 2018. ed. Brasília, DF, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 21 abr. 2021.

BRASIL. Constituição (2018). **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Brasília, Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337. Acesso em: 28 abr. 2021.

BRASIL. Constituição (2018). **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Brasília, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 28 abr. 2021. CAETANO, João Victor Lima. O regulamento geral de proteção de

dados (GDPR): uma análise do extraterritorial scope à luz da jurisdição internacional. **Cadernos Eletrônicos: Direito Internacional sem Fronteiras.** Ceará, p. 5-5. 30 jun. 2020. Disponível em: https://cedisf.emnuvens.com.br/cedisf/article/view/76. Acesso em: 20 jun. 2021.

DIREITOPARATECNOLOGIA: **Quais São as Maiores Dificuldades Que as Empresas Enfrentarão para Implementar a LGPD?.** 2019. Disponível em: https://direitoparatecnologia.com.br/implementar-a-lgpd/. Acesso em: 20 jun. 2021

EXPERIAN, Serasa. **75% dos consumidores desconhecem ou conhecem pouco sobre a Lei de Proteção de Dados, revela pesquisa inédita da Serasa Experian**. 2019. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/estudos-e-pesquisas/75-dos-consumidores-desconhecem-ou-conhecem-pouco-sobre-a-lei-de-protecao-de-dados-revela-pesquisa-inedita-da-serasa-experian/. Acesso em: 14 jun. 2021.

FORNASIER, Mateus de Oliveira; BECK, Cesar. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. **Revista Direito em Debate**, Rio Grande do Sul, v. 29, p. 03-03, 26 maio 2020. Disponível em: https://revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033. Acesso em: 20 jun. 2021.

GARCIA, Lara Rocha *et al*. **Lei Geral de Proteção de Dados Pessoais (LGPD**: guia de implantação. São Paulo: Edgard Blücher Ltda, 2020. 125 p. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=lS3sDwAAQBAJ&oi=fnd&pg=PA3&dq=objetivo+da+LGPD+tem+como+foco+&ots=WkRpjHOIXw&sig=nRkH_wCYR8SUvgNl-XaCIA7Kfs8#v=onepage&q=objetivo%20da%20LGPD%20tem%20como%20foco&f=false. Acesso em: 20 jun. 2021.

ISTOEDINHEIRO: **YAHOO oferece US$ 117,5 mi para encerrar processo de vazamento de dados**. 2019. Disponível em: https://www.istoedinheiro.com.br/yahoo-oferece-us-1175-mi-para-encerrar-processo-de-vazamento-de-dados/. Acesso em: 29 abr. 2021.

LEHFELD, Lucas de Souza *et al*. **A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD**. **Pesquiseduca**, Santos, v. 13, n. 29, p. 236-255, 21 mar. 2021. Disponível em: https://periodicos.unisantos.br/pesquiseduca/article/view/1029/902. Acesso em: 18 jun. 2021.

LUCCA, Victor Spera de. **Análise da Lei Geral de Proteção de Dados Acerca das Relações trabalhistas**. **Intertem@S**, Presidente Prudente, v. 40, n. 40, p. 1-51, 24 nov. 2020. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/Direito/article/view/8892. Acesso em: 20 jun. 2021.

MENDES, Adriano. **5 casos de vazamento de dados nas grandes empresas**. 2020. Elaborado por: Assis e mendes: direito digital, empresarial e proteção de dados.. Disponível em: https://assisemendes.com.br/vazamento-de-dados-nas-empresas/. Acesso em: 29 abr. 2021.

PAYÃO, Felipe. **Vazamento de dados no site da CAIXA permitia golpe hacker**. 2020. Disponível em: https://www.tecmundo.com.br/seguranca/149166-site-banco-caixa-permitia-golpe-hacker-vazamento-dados.htm. Acesso em: 20 jun. 2021.