UNIVERSIDADE REGIONAL INTEGRADA DO ALTO URUGUAI E DAS MISSÕES
PRÓ-REITORIA DE ENSINO, PESQUISA E PÓS GRADUAÇÃO
CAMPUS DE ERECHIM
DEPARTAMENTO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE DIREITO

PATRÍCIA PRECZEVSKI DE JESUS

# EFEITOS DA LEI GERAL DE PROTEÇÃO DE DADOS NO MERCADO DE CONSUMO

ERECHIM

2021

PATRÍCIA PRECZEVSKI DE JESUS

# EFEITOS DA LEI GERAL DE PROTEÇÃO DE DADOS NO MERCADO DE CONSUMO

Trabalho de conclusão de curso apresentado como requisito parcial à obtenção do grau de Bacharel em Direito, Departamento de Ciências Jurídicas e Sociais da Universidade Regional Integrada do Alto Uruguai e das Missões – Câmpus de Erechim.

Orientador (a): Esp. Alessandra Regina Biasus.

ERECHIM
2021

PATRÍCIA PRECZEVSKI DE JESUS

# EFEITOS DA LEI GERAL DE PROTEÇÃO DE DADOS NO MERCADO DE CONSUMO

Trabalho de conclusão de curso apresentado como requisito parcial para obtenção do título de Bacharel em Direito, pelo Curso de Direito do Departamento de Ciências Sociais Aplicadas da Universidade Regional Integrada do Alto Uruguai e das Missões – Câmpus de Erechim.

Erechim/RS, 08 de junho de 2021.

**BANCA EXAMINADORA**

_____

Prof.ª Esp. Alessandra Regina Biasus.

Universidade Regional Integrada do Alto Uruguai e das Missões

_____

Prof.ª Me. Simone Gasperim de Albuquerque.

Universidade Regional Integrada do Alto Uruguai e das Missões

_____

Prof.ª Me. Vera Maria Calegari Detoni.

Universidade Regional Integrada do Alto Uruguai e das Missões

**Dedico** este trabalho a toda minha família, em especial a minha mãe Bernardete, por todo apoio e incentivo, e meu pai afetivo Iris, que sempre me deu muita força mesmo não estando mais presente. Ao meu noivo Cristian, que esteve ao meu lado em todos os momentos e nunca me deixou desistir. Sem vocês, nada disso seria possível.

## AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus por ter me acompanhado durante estes 05 anos de estudos, permitindo que eu tivesse saúde e determinação em especial para a conclusão deste trabalho, por me permitir ultrapassar todos os obstáculos encontrados ao longo do caminho.

Agradeço a minha mãe, Bernardete, que nunca desistiu de mim, que sempre me apoiou independente do caminho que eu escolhesse seguir, que sempre me incentivou a seguir meus sonhos. Obrigada pelo seu incentivo diário, por comemorar comigo cada pequena vitória, por estar sempre ao meu lado e principalmente obrigada por ser minha mãe.

Ao meu pai afetivo, Iris, que me escolheu como filha. Me tornei a pessoa que sou hoje graças a ti, obrigada por compartilhar comigo tantos ensinamentos e me mostrar como a vida é linda até nos pequenos detalhes, por me indicar o caminho certo a seguir, e principalmente, obrigada por ter me escolhido como sua filha. Infelizmente você não pode acompanhar esse momento ao meu lado, mas esteve e estará sempre em meu coração, e independente de onde estiver sei que sempre estaremos juntos!

Ao Cristian, obrigada por ser essa pessoa tão especial em minha vida, sem você eu não chegaria até aqui. Obrigada por todo apoio, amor e paciência que teve comigo, por me mostrar que tudo é possível. Você foi minha fortaleza durante todo esse período, mas acima de tudo, obrigada por ser o meu companheiro de vida e estar comigo do começo ao fim.

Ao meu irmão, Renan, agradeço pelo companheirismo, espero que eu possa ser a tua inspiração em algum momento.

Agradeço ao meu pai Adilson, que chegou a pouco em minha vida, mas que mesmo assim não deixou de me apoiar e incentivar, assim como sua esposa Sonia e toda a família.

A minha sogra Marli, que é como uma segunda mãe, que me ouviu e aconselhou por diversas vezes, isso foi muito importante para que eu seguisse em frente.

Gratidão a toda minha família, meus avós Ladislau e Melânia, meus afilhados Adrieli, Guilherme e Henrique, aos meus tios Ari, Claudete e Milton, minha cunhada Mahyara, e todos os demais, vocês são a base de tudo, sou eternamente grata por tê-los em minha vida.

Agradeço imensamente a minha orientadora, Prof.ª Esp.ª Alessandra, que me acolheu tão bem como orientanda, que dedicou parte do seu tempo a mim, obrigada por compartilhar conhecimentos, ideias e entusiasmo. Suas contribuições foram essenciais ao desenvolvimento dessa pesquisa, tenho um carinho e respeito enorme por você, obrigada por tudo.

A Universidade Regional Integrada do Alto Uruguai e das Missões – Campus de Erechim, obrigada a toda equipe de colaboradores, em especial aos professores, que compartilham seus conhecimentos com muito amor e profissionalismo

Agradeço a todos os meus colegas da Sicredi UniEstados, principalmente da área GJCIC, em especial a Simone e Silvana, que tiveram muita compreensão nesse período, compartilharam seus conhecimentos comigo, me incentivaram a seguir em frente me dando muito apoio, vocês são meus maiores exemplos. Agradeço também a Andressa, pelo companheirismo do dia a dia, vocês três são muito importantes pra mim.

Não posso deixar de agradecer aos amigos que a faculdade me deu, em especial ao Fabiano, Laura, Mariana e Priscila, vocês são as pessoas que eu tive o prazer de ter ao meu lado durante estes 05 anos, obrigada por todas as ideias trocadas, por toda ajuda, por todas palavras de incentivo que tivemos uns com os outros, por compartilhar as angustias e as alegrias. Nós conseguimos, chegamos até aqui juntos, obrigada por isso.

A todos aqueles que não citei nomes, mas que estiveram ao meu lado nessa jornada e torceram por mim, meu muito obrigada.

Enfim, a todos aqui citados, minha família, amigos e colegas, só tenho a agradecer por me auxiliarem a chegar até aqui. Este é apenas o início da minha trajetória, espero que ainda tenhamos muitas conquistas para comemorarmos juntos, e que eu possa dar muito orgulho a todos vocês!

*“Que todos os nossos esforços estejam sempre focados no desafio à impossibilidade. Todas as grandes conquistas humanas vieram daquilo que parecia impossível.”*

Charles Chaplin

## RESUMO

A informação é um dos bens mais preciosos que existe, e a forma de lidar com ela tem causado grandes transformações em âmbito global. Cada vez mais as empresas buscam informações e dados pessoais para prospectar negócios e atingir os clientes da melhor maneira, estes, por sua vez, buscam cada vez mais entender e compreender o que será feito com o dado fornecido, o que levou o Brasil a criar uma legislação específica para o tratamento de dados pessoais. Nesse sentido, foi proposto e estudou-se qual a real aplicabilidade da Lei Geral de Proteção de Dados e quais os efeitos que serão por ela causados no mercado de consumo na atualidade. Parte-se da hipótese de que é uma legislação nova que impactará diretamente os indivíduos e empresas que coletam e tratam dados, afetando os mais diversos setores e serviços, todavia, é necessário verificar qual a sua aplicabilidade e quais os efeitos que causará. Alinhado ao problema da pesquisa e hipótese, o objetivo geral consiste em analisar a aplicabilidade e efeitos da Lei Geral de proteção de Dados no mercado de consumo na atualidade. Em seguida, os objetivos específicos propões a: compreender a evolução da proteção de dados pessoais no âmbito global; estudar a Lei Geral de Proteção de Dados Brasileira e verificar sua aplicabilidade; analisar os efeitos que serão causados pela LGPD. Desse modo, na perspectiva de cumprir o que foi proposto nesta pesquisa, o método utilizado foi o indutivo, com pesquisa bibliográfica, monográfica, doutrinária e legislativa. O resultado da pesquisa indica que o dado pessoal é sim o nosso novo petróleo, e será cada vez mais requisitado, a criação desta legislação era necessária e será aplicada nas mais diversas situações em que ocorra o uso, tratamento ou compartilhamento de dado. Além disso, o maior impacto está nas empresas, que deverão passar por longo processo de adaptação, aderindo as boas práticas de governança, e mudando alguns comportamentos para que possam estar em conformidade com a legislação.



Palavras chave: LGPD; proteção de dados; Empresas

## ABSTRACT

The information is one of the most precious assets there is, and the way of dealing with it has caused major transformations globally. Companies are increasingly seeking information and personal data to prospect new business and reach customers in the best way, and customers, in the other hand, are increasingly seeking to understand what will be done with the data they provide, which led Brazil to create specific legislation for the handling of personal data. In this way, it was proposed and studied what is the actual applicability of the General Law of Data Protection and what effects it will have on the consumer market nowadays. It was assumed that it is a new legislation that will directly impact individuals and companies that collect and process data, affecting the most diversified sectors and services; however, it is needed to verify its applicability and the effects it will cause. In alignment with the research problem and hypothesis, the general goal is to analyze the applicability and effects of the General Law of Data Protection in the consumer market in modern times. Then, the specific goals propose to: comprehend the evolution of personal data protection in the global context; study the Brazilian General Law of Data Protection and verify its applicability; analyze the effects that will be caused by the LGPD. Therefore, in order to fulfill what was proposed in this research, the method used was inductive, with bibliographic, monographic, doctrinal and legislative research. The result of the research indicates that personal data is indeed our new oil, and will be increasingly demanded, the establishment of this legislation was necessary and will be applied in the most various situations in which the use, treatment, or sharing of data occurs. In addition, the biggest impact is on the companies, which will have to go through a long adaptation process, adopting good governance practices and changing some behaviors in order to comply with the legislation.



Keywords: LGPD; data protection; Companies

## LISTA DE SIGLAS

| | |
|---|---|
| ANPD | Autoridade Nacional de Proteção de Dados |
| GDPR | *General Data Protection Regulation* |
| IBGC | Instituto Brasileiro de Governança Corporativa |
| LGPD | Lei Geral de Proteção de Dados |
| OECD | *Organization for Economic Cooperation and Development* |
| PL | Projeto de Lei |
| UE | União Europeia |

**SUMÁRIO**

# 1 INTRODUÇÃO

A Lei 13.709/2018 representa um novo marco histórico na legislação brasileira, foi promulgada em 14 de agosto de 2018, conta com 65 artigos e está vigente desde 18/09/2020. A partir de então, muito vem se falando da Lei Geral de Proteção de Dados, que ficou popularmente conhecida como LGPD, pois promete causar grande impacto tanto em instituições privadas quanto públicas. É uma regulamentação extremamente técnica, reúne uma série de princípios, direitos e deveres relacionados ao que é considerado o ativo mais precioso na era em que vivemos, o dado pessoal, que por ora se funda na proteção dos direitos humanos.

Como vivemos em um mundo com tecnologia avançada, cada vez mais nossas vidas são controladas por algoritmos e conclusões são tomadas através deles, muitas vezes sem o nosso conhecimento. Dessa forma, a LGPD veio para regulamentar o uso e o tratamento de dados pessoais, ou seja, de pessoas físicas, em qualquer relação que estes dados estejam envolvidos.

No primeiro capítulo será tratado da evolução da proteção de dados em âmbito global, pois por mais que a Proteção de Dados Pessoais pareça ser um tema presumivelmente novo, ela teve início durante a “Quarta Revolução Industrial”, iniciada em 1970 com o fenômeno da “informacionalização da sociedade”, mas foi ao longo dos últimos anos que sua relevância foi vista pelas autoridades competentes a fim de criarem leis específicas sobre o assunto. O Brasil, inspirado no Regulamento Geral de Proteção de Dados da União Europeia, foi o último país da América Latina a adotar uma lei específica para tratamento de dados pessoais, devido a este motivo, grande parte da população brasileira considera o tema como novo.

No segundo capítulo da Monografia, será feito um estudo sobre a Lei Geral de Proteção de Dados para compreender qual será sua aplicabilidade no mercado de consumo brasileiro, tendo em vista que esta possui como principal objetivo, regular o tratamento de dados pessoais, protegendo a privacidade e também outros direitos fundamentais e liberdades individuais.

No terceiro capítulo será estudado quais os maiores desafios e consequências que as empresas enfrentarão com a entrada da LGPD em vigor. Seus impactos serão

expressivos para os titulares dos dados, mas principalmente para a atividade empresarial, pois a LGPD determina uma série de princípios e diretrizes a serem seguidos pelas empresas para que possam tratar os dados de forma licita.

Todo esse estudo foi desenvolvido através de pesquisa bibliográfica e documental, com um método de abordagem indutivo e analítico-descritivo de procedimento.

Por fim, cabe destacar que esta pesquisa tem uma relevância social e é de extrema importância para que possamos compreender qual a aplicabilidade da LGPD, quais nossos direitos e deveres frente a ela, e quais os impactos que serão causados no mercado de consumo diante de sua vigência. Para isso, os principais objetivos são compreender a evolução da proteção de dados, estudar a Lei 13.209/2018 e verificar qual a sua aplicabilidade, e por fim analisar os efeitos que ela produzirá.

# 2 EVOLUÇÃO HISTÓRICA DA LEGISLAÇÃO DE PROTEÇÃO DE DADOS

O presente capítulo será dedicado a tratar da evolução histórica no que tange a legislação de proteção de dados, para tanto irá apontar como é feito o tratamento dos dados pessoais, passando pela diretiva 95/46/CE e a GDPR (*General Data Protection Regulation)* para LGPD (lei geral de proteção de dados).

Os dados pessoais sempre estiveram circulando livremente, mas com o passar do tempo foram ficando mais atrativos para empresas, que com base neles poderiam montar estratégias de negócios mais atraentes e assertivas, hoje o dado pessoal é o novo petróleo. Com esse avanço foi necessária a criação de normativos que atendessem à proteção dos dados, para que pessoas não ficassem desamparadas quanto ao tema.

As legislações começaram a surgir por todo o mundo, porém a mais importante foi a *General Data Protection Regulation* – GDPR, que surgiu na Europa em 2016, pode-se considerar que esta foi a que melhor tratou do assunto. O Brasil foi um dos últimos países do América Latina a implementar uma legislação que protegesse os dados pessoais, mas baseando-se na GDPR fora criada a Lei nº 13.709 em agosto de 2018. Ao longo deste capítulo, será exposta toda a evolução quanto ao tratamento e proteção de dados pessoais, e o quanto isso nos importa hoje.

## 2.1 DADOS PESSOAIS E SEU TRATAMENTO

Para o mercado, os dados pessoais de consumidores sempre foram chamativos, através deles é possível criar um planejamento estratégico de vendas com produtos selecionados, uma campanha de publicidade voltada as necessidades de cada consumidor, dentre outras possibilidades. Há pouco tempo atrás a maneira de obter estes dados era mais restrita, hoje vivemos em um ambiente onde muitas de nossas ações são passíveis de registro e utilização.

O Brasil possui diversos diplomas legais que tratam a respeito do assunto, mas nenhum que trate de forma efetiva a proteção de dados pessoais, com regras claras

que promovam a segurança jurídica. Faustino (2016) expõe que muitas empresas se utilizam dos dados para consolidarem-se no mercado, usando deste meio pra aproveitarem-se, haja vista que até então não existia uma política efetiva de proteção e tutela destes dados.

A LGPD surge então para dirimir este problema, com objetivo de trazer maior proteção às informações pessoais de cada indivíduo, regulamentando o tratamento dos dados, prevenindo eventuais abusos por parte dos controladores e operadores e aplicando sanções para tais ocorrências. Ela aplica-se a qualquer dado de pessoa física, coletado ou tratado em território nacional por pessoa natural ou jurídica, tanto de direito público quanto privado.

Tratar sobre a Proteção de Dados Pessoais é algo presumidamente novo no Brasil, e implica numa alteração do padrão até então experimentado, impactando significativamente na atividade econômico-empresarial, dado que o Estado passa a disciplinar o tratamento de dados pessoais, a fiscalização e as penalizações. (OLIVEIRA, 2019).

Em primeiro lugar, temos que observar a sobreposição dos termos “dado” e “informação”, que por muitas vezes se confunde.

> Assim, o “dado” apresenta conotação mais primitiva e fragmentada, semelhante a uma informação em estado potencial, antes de ser transmitida ou associado a uma espécie de “pré-informação”, que antecederia a sua interpretação e elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Sem aludir ao seu significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação é um termo que carrega também um sentido instrumental, no sentido da redução de um estado de incerteza. (DONEDA, 2010, p. 19)

O dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável, conforme menciona o art. 5º, § I da Lei nº 13.709/18, portanto, a proteção sobre estes dados que a lei prevê, incide somente sobre os dados de pessoas físicas. Estes dados não se limitam apenas a nome e sobrenome, podendo serem dados de localização, número de *Internet Protocol* (IP), histórico de compras, dentre outros. (Brasil, 2018)

Dentro destes dados, existem os chamados dados pessoais sensíveis, conforme disposto no art. 5º, § II da Lei nº 13.709/18, estes dados estão relacionados com características ou personalidades do indivíduo, que deixam a pessoa em um grau de exposição maior por ser possível alguma discriminação, para estes, a lei prevê requisitos mais rígidos para o tratamento. E existem ainda os dados anonimizados, que são os dados relativos a um titular que não são identificáveis, conforme art. 5º, § III da Lei nº 13.709/18. (Brasil, 2018)

Conforme Pinheiro, (2018, p. 60), “A partir da LGPD, passa a ficar claro e apontável o que é ou não dado pessoal, assim como todos os processos, as técnicas ou os procedimentos relativos ao tratamento de dados”.

Dessa forma, as empresas que desejarem passar uma boa imagem junto ao seu público deverão agir com credibilidade tendo como seus principais pilares a transparência e a garantia de privacidade, o que passará ser cada vez mais significativo com os brasileiros, será um compromisso indubitável com a segurança e o respeito da população.

A nova lei estabelece que todos os dados coletados deverão ser tratados, e para isso trouxe consigo 10 princípios que deverão ser obedecidos pelas empresas ao realizarem o tratamento, sendo:

> Finalidade: Propósitos legítimos, específicos, explícitos e informados.
> Adequação: Compatível com as finalidades.
> Necessidade: Utilização (apenas) de dados estritamente necessários.
> Livre Acesso: Acesso ao tratamento e integralidade dos dados.
> Qualidade dos Dados: Dados exatos, claros, relevantes e atualizados.
> Transparência: Informações claras e precisas aos titulares.
> Segurança: Medidas técnicas e administrativas aptas a proteger os dados pessoais.
> Prevenção: Adoção de medidas para evitar danos aos titulares.
> Não Discriminação: Não utilização para fins discriminatórios, ilícitos ou abusivos.
> Responsabilização e Prestação de Contas: Demonstração de adoção de medidas eficazes ao cumprimento das normas. (NUNES, 2019, p. 04).

Além disso, a lei determina que o tratamento de dados só poderá ser realizado com o consentimento do titular, e em alguns casos específicos como o cumprimento de obrigação legal. O consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a vontade do titular em fornecer os dados, autorizando que estes sejam registrados. E por fim, no consentimento deve constar as finalidades

determinadas as quais os dados serão utilizados, se uma autorização for genérica, ou seja, não estiver especificado a utilidade dos dados, esta será nula.

Havendo qualquer mudança na finalidade para o tratamento de dados pessoais do indivíduo que não sejam compatíveis com o consentimento original, a empresa deverá informar previamente o cliente sobre as mudanças de finalidade. Além disso, o cliente poderá revogar o consentimento a qualquer momento e sem custos, e também poderá solicitar à empresa quais os dados que a mesma possui de sua pessoa, sendo dever da empresa de informar com transparência e agilidade.

### 2.1.1 Diretiva 95/46/CE (Diretiva Européria de Proteção de Dados Pessoais)

O “direito à privacidade” começou a ser tratado em jurisprudências e doutrinas norte americanas, mas foi na Europa que surgiram os primeiros conjuntos de leis que regulassem o tema. Em suma, essas leis foram desenvolvidas individualmente para cada país, o que acabou se tornando um fenômeno atingindo uma condição multinacional.

Em 1980, fora publicado as “Diretrizes sobre Proteção da Privacidade e o Fluxo Transnacional de Informações Pessoais” pelo Comitê de Ministros da OECD (*Organization for Economic Cooperation and Development*), um documento que de forma muito sucinta tratava sobre a proteção de dados.

> Essas “guidelines”, no entanto, não têm força coercitiva e permitem uma variação muito ampla na sua implementação no direito interno dos países. Um ano mais tarde, em 1981, o Conselho da Europa promulgou a Convenção “Para a proteção dos indivíduos com respeito ao processamento automático de dados pessoais”, que entrou em vigor em 1985. Dita Convenção é bem similar às “Guidelines” da OECD, embora com foco na proteção de dados para resguardar a privacidade individual. (FILHO, 2013, p. 02)

Esta nova Convenção passou a tratar a proteção de dados de forma mais rígida, desde a obtenção dos dados, seu processamento, tratamento e armazenamento. Ela institui também que todos os países signatários devem dispor de

leis nacionais que estejam de encontro com seus princípios, sob pena de sofrerem as sanções estabelecidas.

Ambos os textos multinacionais foram de grande importância para a criação de um normativo que estabelecesse quanto a proteção de dados de diversos países. Ainda assim, o objetivo final da Convenção não foi alcançado, isso pois ela deixava muitas lacunas que davam autonomia aos países para implementarem-na de diversas maneiras, inclusive, adotando conceitos e definições diversas entre um país e outro.

Em razão desta variância, a união Europeia editou a Diretiva 95/46/EC, para assegurar e harmonizar o fluxo de informações de dados entre países. A Diretiva não só criou um novo conjunto de regras a serem aplicadas no processamento de dados, mas também estabeleceu preceitos que reforçassem os direitos previstos nos normativo nacionais já existentes.

Aprovada em 24 de outubro de 1995 para entrar em vigor em 24 de outubro de 1998, este prazo se deu para que os países membros da União Europeia pudessem ter tempo hábil para se adaptarem as novas medidas legislativas e regulamentares. Dentre as adaptações necessárias, estão que cada país deverá criar e editar leis que tratem sobre o processamento de dados pessoais, e que cada um terá de dispor de uma agência ou comissário de proteção de dados, para que este supervisione a aplicação dos princípios da Diretiva.

De acordo com Filho (2013) ressalta que uma das falhas da Convenção foi não incluir definições de cunho importante quanto ao processamento de dados, o que foi sanado com a Diretiva que logo em seu art. 2º trouxe diversos conceitos sobre. Ela define o que são dados pessoais, qual a extensão de sua proteção, o que é o processamento de dados, dentre outros que são de suma importância para uma correta definição, compreensão e aplicação de seus preceitos.

Em seu art. 3º ela define o âmbito de aplicação, que se dará tanto em tratamento de dados automatizados ou não, e logo em seguida expõe os princípios e direitos básicos em relação a este processamento. Prevê ainda, regras relativas ao tratamento de dados específicos, como por exemplo o dado considerado sensível, que é tratado de maneira diversa dos demais, deixando aberto a cada Estado-membro estabelecer exceções à regra quanto ao processamento destes dados.

Outro aspecto relevante que a Diretiva apresenta é a liberdade do indivíduo de não se submeter a processos de decisões automatizadas. De acordo com Silva (2013), estes sistemas automatizados trabalham com a criação de perfis onde são incluídas características da pessoa a partir da coleta de dados, para tratar a pessoa de acordo com estas características. Eles fornecem uma série de indicações comportamentais do perfil, baseado em probabilidades. A partir deste perfil, torna-se mais fácil influenciar o indivíduo a determinado ato, e esta norma da Diretiva busca minimizar essa predisposição.

O texto da Diretiva resultou de diversas discussões e experiências nacionais sobre a proteção de dados, que levaram a suas principais disposições. Ela foi o principal instrumento a tratar sobre proteção de dados, servindo de base para os normativos que foram elaborados posteriormente, inclusive para a GDPR (SILVA; SILVA, 2013). Por estes motivos, ao falarmos de proteção de dados não podemos deixar de mencionar esta Diretiva que foi o início de tudo.

### 2.1.2 A GDPR (General Data Protection Regulation) como base para LGPD (Lei Geral de Proteção de Dados)

A Diretiva 95/46/CE acabou reproduzindo diversas leis nacionais, através das quais muitas empresas norte americanas aproveitavam-se das brechas para não adotarem as medidas corretas de *compliance*. Em decorrência disso, a União Europeia estava com uma visão fragilizada e desorientados quanto a privacidade de dados, o que os induziu a criar uma nova legislação com o intuito desta ter maior efetividade.

Após 4 anos de estudos e discussões, em abril de 2016 o Parlamento Europeu aprovou o texto base que daria origem a GDPR, que passou por 2 anos de vacância para que empresas, companhias e organizações pudessem tomar medidas para adequarem-se aos padrões da lei. E então, em 25 de maio de 2018 a GDPR entrou em vigor, tornando-se um marco legal mundial, pois representou a maior inovação legislativa em matéria de proteção de dados pessoais (CAETANO, 2020).

A GDPR foi incorporada ao ordenamento jurídico europeu contando com 173 considerados, 11 capítulos e 99 artigos, causando um grande impacto inovador com seu entendimento de que como no ambiente virtual não existem fronteiras, assim também deve ser com a lei, para que esta possa ultrapassar os limites nacionais. Além de conseguir atingir seu objetivo de harmonizar as leis de proteção de dados existentes em cada país europeu (CAETANO, 2020).

> Pois, ao contrário da sua predecessora (DPD), que tinha caráter de diretriz, que consistia em um mero conjunto de normas que previam um resultado a ser alcançado, GDPR tem uma estrutura jurídica de regulamento. Isto significa que o Regulamento Europeu é uma ordem que deve ser executada de modo homogêneo por cada estado membro, vindo a tornar-se lei nacional em cada um deles e, com exceção de alguns casos específicos de segurança nacional, não há nenhuma oportunidade de mudanças ao passar pelo processo legislativo doméstico (DIBLLE, 2020, apud CAETANO, 2020, p. 08).

Hoje, a GDPR é diretamente aplicável a toda União Europeia, mas sua entrada em vigor não causou tamanho impacto como a LGPD deverá causar ao Brasil. Isso pois, suas maiores disposições já se encontravam dispersas em leis nacionais e seu intuito foi apenas harmonizar alguns pontos destoantes entre estas, enquanto que para o Brasil a proteção de dados é algo totalmente novo, onde muitas empresas, organizações e companhias sequer já ouviram falar do assunto.

A GDPR trata-se de um regulamento recente, mas que vem servindo de exemplo para os demais países. Para Pinheiro:

> Este, por sua vez, ocasionou um “efeito dominó”, visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação do mesmo nível que a GDPR. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE. (PINHEIRO, 2018, p. 18)

Nesse período, o Brasil já dispunha do Marco Civil da Internet e da Lei do Cadastro Positivo, mas estes não eram suficientes para efetivar negócios com a UE, pois não previam critérios objetivos para determinar de que forma se daria a guarda, manuseio e descarte dos dados transacionados na relação. Este foi um dos motivos que levou o Brasil a criar a Lei nº 13.709/18, para que esta padronize a proteção de

dados pessoais e regule penalidades para quem agir em inconformidade com os atributos qualitativos.

A LGPD foi sancionada em 14 de agosto de 2018, dividida em 10 capítulos, com 65 artigos, menor que sua referência europeia (GDPR). Sendo a versão brasileira mais enxuta, deixando margens para hesitações em alguns pontos em que deveria ser mais assertiva. “Um exemplo disso ocorre em relação à determinação de prazos: enquanto o GDPR prevê prazos exatos, como de 72 horas, a LGPD prevê ‘prazo razoável”. (PINHEIRO, 2018, p. 22)

O tratamento de dados pode ser entendido como qualquer procedimento que envolva a utilização dos dados pessoais coletados, e para que as empresas possam tratar estes dados, a LGPD trouxe consigo dez princípios que garantem a proteção do direito dos dados, devendo sempre respeitar-se os limites dos direitos fundamentais. Conforme art. 6º, da Lei nº 13.709/18, são estes os princípios: Finalidade; Adequação; Necessidade; Livre Acesso; Qualidade dos Dados; Transparência; Segurança; Prevenção; Não Discriminação e Responsabilização e Prestação de Contas. (Brasil, 2018)

Além disso, a lei determina que o tratamento de dados só poderá ser realizado com o consentimento do titular, e em alguns casos específicos como o cumprimento de obrigação legal. O consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a vontade do titular em fornecer os dados, autorizando que estes sejam registrados. E por fim, no consentimento deve constar as finalidades determinadas as quais os dados serão utilizados, se uma autorização for genérica, ou seja, não estiver especificado a utilidade dos dados, esta será nula.

Havendo qualquer mudança na finalidade para o tratamento de dados pessoais do indivíduo que não sejam compatíveis com o consentimento original, a empresa deverá informar previamente o cliente sobre as mudanças de finalidade. Além disso, o cliente poderá revogar o consentimento a qualquer momento e sem custos, e também poderá solicitar à empresa quais os dados que a mesma possui de sua pessoa, sendo dever da empresa de informar com transparência e agilidade.

Sua entrada em vigor estava prevista para agosto de 2020, mas com Medida Provisória 959/2020 esta data seria prorrogada para janeiro de 2021, porém o artigo que previa este adiamento foi retirado da MP pois já havia sido objeto de votação

pelos senadores quando aprovaram o PL 1.179/2020, que se converteu na Lei 14.010/2020. A LGPD então passou a vigorar a partir de 18 de setembro de 2020, porém, suas sanções só poderão ser aplicadas a partir de agosto de 2021, em decorrência da aprovação da Lei 14.010/2020.

Após breve análise da evolução histórica das legislações no que tange a proteção de dados, o próximo capítulo será dedicado a tratar sobre a Lei Geral de Proteção de Dados.

# 3 BREVE ANÁLISE SOBRE A LGPD

A Lei 13.709/18 – LGPD, é considerada no ambiente jurídico uma das leis mais importantes a ser incorporada em nosso ordenamento em maio de 2021, ela irá dispor quanto ao tratamento e proteção de dados pessoais, será a partir dela que empresas terão de se adequar para que fiquem em conformidade.

Neste capítulo será abordado os principais pontos da legislação, os direitos que os titulares dos dados possuem, o que é um vazamento de dado e quais as sanções caso isso ocorra, e sobre as boas práticas que as empresas deverão adotar a partir de então para que fiquem adequadas à legislação.

## 3.1 DIREITO DOS TITULARES DE DADOS

A Lei deixa claro em seu próprio nome que o maior objetivo é assegurar a proteção da pessoa natural e o livre desenvolvimento de sua personalidade, resultando em um capítulo dedicado a tratar exclusivamente dos direitos dos titulares. Entretanto, verifica-se que os direitos e garantias elencados no Capítulo III da Lei 13.709/2018, foram vinculados à alguns direitos fundamentais do art. 5° da Constituição Federal, deixando claro que não houve por parte do legislador maior preocupação em garantir estes direitos de forma exclusiva.

Outro ponto importante a ser destacado é sobre a impossibilidade da desvinculação dos dados pessoais quando estes já estiverem sendo tratados pelo operador ou controlador. “Ainda que o titular, voluntariamente, disponibilize irrestritamente os seus dados pessoais, mesmo que publicamente, subsiste a ele a plena titularidade, em liame indissociável.” (MALDONADO, 2019, p. 220)

Muitos dos direitos dos titulares podem ser vistos indiretamente na Lei antes mesmo do Capítulo III, mas é no art. 18 que tais direitos são mencionados de forma expressa, quais sejam:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;

> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
> § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
> § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

Segue o art. 18 da Lei 13.709/18, referido:

> § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
> § 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
> I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
> II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
> § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
> § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.
> § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
> § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor. (BRASIL, 2018)

Sempre que um dado for disponibilizado deverá haver o consentimento, que deve ser um termo claro, objetivo, de fácil entendimento ao titular e que tenha destacando a finalidade da coleta daquele dado. Como o titular tem direito ao livre acesso das informações, a qualquer momento ele poderá solicitar por meio da requisição uma atualização, alteração, correção ou exclusão de seus dados pessoais. O possuidor não é obrigado a cumprir com todas as requisições formuladas que receber, mas é

obrigado a responder mesmo que de forma negativa, neste caso informando o motivo pelo não cumprimento.

Assim como o titular fornece o consentimento ele tem o livre arbítrio para revogá-lo, esta revogação deve ser de forma simples e gratuita assim como o próprio consentimento. A revogação ratifica o tratamento realizado anteriormente, não produzindo efeitos quanto aos atos praticados sob a égide do consentimento licitante fornecido. (MALDONADO, p. 234, 2019).

> É importante ressaltar, contudo, que, apesar do titular ter a possibilidade de exercer seus direitos, conforme acima exposto, não existem direitos absolutos. Os dados pessoais poderão ser tratados sem a autorização do titular nos casos, por exemplo, que forem necessários para a execução de um contrato ou para o cumprimento de uma obrigação legal. Além disso, segredo comercial e industrial pode ser uma justificativa para que a instituição não forneça os dados. (BLANCHET; TAVARES, 2020, p. 03)

É evidente que a lei causará grandes impactos aos agentes de tratamentos de dados quanto ao assunto aqui tratado. Estes deverão se empenhar para que sejam fornecidos meios que viabilizem aos titulares o exercício de seus direitos de forma ampla, precisa e completa.

## 3.2 FISCALIZAÇÃO E VAZAMENTO DE DADOS

Conforme já mencionado anteriormente, um dos maiores objetivos da LGPD é proteger os dados do cidadão, e uma das formas de fazer isso é prevenir o vazamento de dados. Se um vazamento ocorre, a empresa detentora do dado terá todo um trabalho para detectar e reconhecer o problema que originou o vazamento, solucioná-lo, e notificar a todos os envolvidos, tendo que buscar uma reparação caso ocorra a violação dos direitos, além disso, a ANPD irá apurar o caso e responsabilizar o agente que deu causa ao dano.

De acordo com Cabral:

> O vazamento de dados acontece quando informações de caráter sigiloso se tornam públicas, de modo a prejudicar o titular do dado (cliente) e os demais usuários. Geralmente, isso ocorre devido à ação de invasores que encontram brechas de segurança da companhia, incluindo desde aplicativos até e-mail. As informações vazadas podem ser utilizadas por ativistas que objetivam comprovar e expor as falhas da empresa. Esses ataques podem ser feitos de

> diferentes maneiras, o que dificulta o rastreamento e, consequentemente, a punição dos responsáveis. (CABRAL, 2020, p. 02)

Assim como em muitas legislações, a aplicação da LGPD é estimulada a ocorrer em caráter preventivo. Para tanto, trouxe consigo dois capítulos destinados a tratar sobre o capítulo VIII – Da Fiscalização, e o capítulo IX – Da Autoridade Nacional De Proteção De Dados (ANPD) E Do Conselho Nacional De Proteção De Dados Pessoais E Da Privacidade, este tratando do Órgão Fiscalizador.

As sanções aplicáveis em caso de vazamento de dados variam, partindo de advertência até imputação de multa, e serão aplicadas após o procedimento administrativo para que se possibilite a ampla defesa. Conforme Pinheiro (2018), a imputação deve observar a proporcionalidade, pois será aplicada a diversos tipos e ramos de empresas, isso irá inibir um possível abuso de poder estatal.

Pinheiro (2018) ressalta ainda, que o fiscalizador da nova regulamentação deverá levar em conta alguns critérios que possam agravar ou amenizar a aplicação da sanção, já que a possibilidade de ocorrência de violação de dados, por violação de segurança é alta, em virtude do contexto digital em que vivemos. Por mais que o controlador ou operador siga as melhores práticas e a aplicação de controles não estará livre de ocorrer uma infração e o vazamento de dados pessoais.

O artigo 52 da LGPD nos traz todas as sanções que são passíveis de ocorrerem:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> VII - (VETADO);
> VIII - (VETADO);
> IX - (VETADO).
> X - suspensão parcial do funcionamento do banco de dados a que se refere

a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.
§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
II - a boa-fé do infrator;
III - a vantagem auferida ou pretendida pelo infrator;
IV - a condição econômica do infrator;
V - a reincidência;
VI - o grau do dano;
VII - a cooperação do infrator;
VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
IX - a adoção de política de boas práticas e governança;
X - a pronta adoção de medidas corretivas; e
XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.
§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica.

Segue o art. 52 da Lei 13.709/18, referido:

§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.
§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.
§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995.
§ 6º As sanções previstas nos incisos X, XI e XII do **caput** deste artigo serão aplicadas:
I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do **caput** deste artigo para o mesmo caso concreto; e
II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos.
§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. (BRASIL, 2018)

O que chama atenção neste artigo é a aplicação de multa, que poderá ser simples ou diária, além de um valor limite estipulado, o que representa uma gradativa evolução legislativa, diante de várias tratativas sobre o assunto que se deram em PL's antes da aprovação da LGPD. A aplicação da multa é limitada a 2% do faturamento do último exercício da empresa, limitado a R$ 50.000.000,00 por infração, sendo que, até mesmo a multa diária de que trata o inciso III deste artigo deverá observar este limite.

> Ainda que se queira entender fragilizado o poder de polícia da ANPD em face da instrumentalidade pecuniária mais singela que a de outras regulações, há que se considerar o aspecto reputacional da proteção de dados, além da irradiação de responsabilidade civil na cadeia de tratamento de dados pessoais – elementos que, por si, já poderão ser abalados com a simples notícia de incidente de violação de direitos de proteção de dados e, ainda mais, por eventual condenação administrativa ou judicial a respeito do mesmo assunto. (MALDONADO, 2019, p. 371)

A aplicação desta e das demais sanções caberá à Autoridade Nacional de Proteção de Dados (ANPD), que fará uma análise do caso e aplicará uma sanção proporcional. A ANPD será um órgão da Presidência da República, com 36 cargos, onde o mandato dos membros será de quatro anos, prorrogável uma vez, por igual período. Teve sua Diretoria confirmada pelo Senado no dia 20/10/2020, sendo divulgados os nomes para Presidente e Conselho.

A ANPD será um órgão que irá atuar a serviço do cidadão, tendo um canal de denúncias, consulta de dúvidas e sugestões ligadas a LGPD, será um elo entre a sociedade e o governo. Este canal também será direcionado às empresas, para que busquem suporte e apoio em relação à situações em que possam ou não tratar de dados pessoais, com esta autonomia a ANPD estará cumprindo com seu papel de garantidor do cumprimento da lei.

Para Doneda e Mendes (2018), a ANPD é de suma importância para garantir os direitos dos indivíduos, segundo eles:

> Além de a Autoridade ser um ponto de referência e orientação para o cidadão, ocorre que o tratamento de dados pessoais é uma atividade complexa e que muitas vezes acontece de forma opaca, sendo realizado por entidades e corporações cujas práticas não são suficientemente transparentes – e que

> podem ser abusivas. A existência de uma Autoridade que atue de forma coordenada para prevenir e reprimir abusos, fiscalizando e tutelando tratamentos de dados de inteiras coletividades é fundamental para diminuir a distância abissal entre o cidadão e os entes que tratam seus dados, evitando que sejam abertas demandas individuais pelo caminho geralmente longo (e custoso) da via judicial. (DONEDA; MENDES, 2018, p. 25)

Assim, a ANPD será uma Agência Reguladora atuando em busca do interesse público, para isso ela deverá ter poder normativo, autonomia financeira e poder regulamentar para que possa obrigar os possuidores de dados a realmente cumprirem a legislação e suas orientações. Sua atividade será de grande importância, visto a quantidade de dados pessoais que circulam no mercado nacional e internacional.

## 3.3 DA SEGURANÇA E DAS BOAS PRÁTICAS

A partir da LGPD, as empresas cada vez mais deverão estar em conformidade, e para isso deverão implementar medidas de segurança, medidas técnicas e administrativas que sejam realmente efetivas em proteger os dados de seus clientes. Para Pinheiro:

> Conforme os artigos 40, 41, 42 e 43, as medidas de boas práticas envolvem um sistema amplo e complexo de relações e previsões como instituição de mecanismos de educação e prevenção em face da segurança da informação, atuação de organismos de certificação e treinamento de equipes junto à atuação das autoridades supervisoras. (PINHEIRO, 2020, p. 106)

A LGPD dedicou um capítulo exclusivo para tratar sobre o assunto, sobre segurança, boas práticas e governança, o capítulo VII, e na Secção II expõe a necessidade da formulação de boas práticas e governança, com medidas que vão de encontro aos pilares de um programa de *compliance*. “Apesar de a lei instruir claramente o caminho a ser tomado para a conformidade e cabal aplicação das disposições legais, notamos uma cultura parcialmente construída de governança ou inexistente” (LOPES, 2020).

Ocorre que ainda existe uma certa dificuldade em algumas empresas em perceberem e aceitarem que não estão em conformidade, e mobilizarem-se para que isso seja revertido, é uma característica forte nas pequenas e médias empresas. É

claramente visível que as normas de segurança estabelecidas para um pequeno mercado de bairro, não serão as mesmas estabelecidas para um grande shopping.

> Há claramente um estímulo para que os agentes da iniciativa pública e privada formulem suas próprias regras e se autorregulem de acordo com as condições de as peculiaridades da organização e a sua forma de funcionamento. Isso porque, embora a LGPD seja soberana, a depender do setor econômico as normas de segurança e os padrões técnicos serão diferentes. (MALDONADO, 2019, p. 356)

A governança corporativa é uma relação horizontal que envolve a alta direção, conselhos administrativos, acionistas e demais interessados, através dela são criadas estratégias para o negócio. De acordo com o Instituto Brasileiro de Governança Corporativa – IBGC, em seu Código de Melhores Práticas:

> Governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum. (IBGC, 2018, p. 20)

Dentro da governança corporativa estão as boas práticas, regras que poderão ser formuladas pelos controladores e operadores de dados levando em consideração a relação com o tratamento de dados e os princípios indicados na própria lei. (BRASIL, 2018). Tudo isso se resume a um programa de *compliance*, que são instrumentos de controle criados para garantir o cumprimento de legislações e para prevenir os riscos em decorrência deste não cumprimento.

> As boas práticas de governança corporativa e *compliance* constituem a base necessária para a credibilidade dos nossos negócios. Nossa lição de casa é atuar acima de tudo sempre orientados pela ética, pela integridade e pela transparência. Assim, protegemos o maior patrimônio da organização, ou seja, salvaguardamos a reputação das marcas e conquistamos a confiança dos nossos clientes. (FRADE, 2019, p. 01).

Por mais que governança corporativa e um programa de *compliance* sejam muito semelhantes, não são a mesma coisa, mas sim se complementam. O programa de *compliance* é responsável pela conformidade com as regras, é um processo interno, já a governança corporativa é mais comprometida com questões relacionadas a reputação da empresa, relações internas e externas, prezando pela gestão eficiente e pela transparência. (FARINHO, 2018).

Diante de todas as mudanças trazidas pela lei o objetivo do *compliance* frente a LGPD é auxiliar as empresas a desvincularem-se das atuais práticas empregadas. Com um bom programa de adequação essas mudanças não impactaram as empresas de forma tão severa, servindo como um treinamento para as alterações no cenário de proteção de dados, adequando-se de forma mais fácil para atender de forma correta as demandas exigidas pela lei.

> Por fim, em decorrência da particularidade da LGPD, os métodos adotados para a sua adequação também deverão ser especificamente criados para função. Os conceitos de privacidade e proteção de dados deverão ser princípios a serem seguidos desde a concepção do programa até a sua execução, garantindo assim que os preceitos estipulados sejam de fato seguidos. Em decorrência da constante mutabilidade da disciplina de proteção de dados, os programas de integridade também deverão seguir esta característica. (NUNES, 2019, p. 64)

Conforme já mencionado anteriormente, a LGPD trouxe consigo sanções muito severas em caso de seu não cumprimento, de forma que estas podem impactar profundamente as empresas em se tratando de valores de multa, desta forma o não cumprimento de suas regras não se torna uma opção. Em razão disso implementar um programa efetivo de *compliance* é se suma importância, para auxiliar a empresa de forma que esta sempre esteja em conformidade e não venha a sofrer as sanções previstas na legislação.

Após analisar a LGPD e as consequências pelo vazamento de dados, o próximo capítulo será dedicado a tratar dos desafios e a melhor forma das empresas se adequarem as exigências impostas pela Lei geral de proteção de dados.

# 4 LGPD CONSEQUENCIAS E DESAFIOS PARA AS EMPRESAS

Assim como qualquer nova legislação que entra em vigor, a Lei 13.709/18 – LGPD, causará alguns impactos diante nos novos regulamentos trazidos. Neste capítulo serão abordados os principais efeitos que ela causará, e quais as melhores formas de adequação das empresas para que fiquem em conformidade.

## 4.1 *BIG DATA* E A LGPD

O volume de dados, a velocidade de processamento e a variedade de dados são apresentados como os alicerces do conceito de *Big Data*, são os três pilares principais que quando bem trabalhados geram valor para produtos e serviços das empresas. Conforme conceito abaixo:

> *Big Data* pode ser definido com base em grandes volumes de dados amplamente variados que são gerados, capturados e processados em alta velocidade. Como tal, esses dados são difíceis de processar usando as tecnologias existentes. Ao adotar tecnologias analíticas avançadas, as organizações podem usar *Big Data* para desenvolver insights, produtos e serviços inovadores (GUNTHER, 2017, p. 02).

*Big Data* nada mais é do que um conjunto de técnicas capazes de analisar grandes quantidades de dados, o que gera resultados importantes e estratégicos para as empresas, que em menores volumes dificilmente seria possível alcançar essa visão. Através dele as empresas conseguem respostas mais completas nas mais diversas áreas, melhorando a experiência entre fornecedor e consumidor.

Com ele é possível identificar padrões comportamentais de seus clientes, e através do resultado traçar perfis de forma a poder entregar ofertas de produtos e serviços personalizados de acordo com os vários tipos de consumidores. Também é possível a criação de estratégias de *marketing* de acordo com os dados levantados, auxiliando as empresas a encontrar potenciais clientes e descobrir as alterações de suas preferências. (WESTON, 2019).

Para que tudo isso seja possível faz-se necessário o uso de alta tecnologia, e investir nisso leva as empresas a lidarem de forma mais otimizada e eficiente com seus processos, aumentando suas vendas, seus clientes e consequentemente suas

receitas. Tudo isso é capaz de proporcionar uma grande vantagem competitiva de mercado, pois:

> É inegável que a informação tem hoje um valor econômico expressivo e o processo de criação e processamento de dados acaba por ser um empreendimento em si, cujos procedimentos muitas vezes podem invadir esferas de direitos, em especial o direito à privacidade. Na verdade, uma das características da Sociedade da Informação é o fato do valor econômico representado pelo conhecimento (cuja geração depende de informações) ser superior ao valor dos bens materiais confeccionados a partir dele. (SANTOS; PALHARES; FREITAS, 2019, p. 709)

Porém, com a entrada em vigor da LGPD, o *Big Data* traz preocupações relevantes sobre o seu uso, possíveis invasões de privacidade e discriminação de dados de forma indevida são dois grandes pontos negativos. A perda de autonomia, descaracterização do indivíduo, classificação das pessoas ou grupos de pessoas de forma desagradável, fornecimento unilateral de informação e o confronto com informações indesejadas são preocupações intrínsecas ao tratamento de dados. (MARTINS, 2019).

Outro risco associado ao *Big Data* é a imprecisão associada à criação de perfis, pois podem não ser fidedignos à realidade. Isso leva ao problema quando se trata em decisões automatizadas sem intervenção humana. Por não haver um processo contraditório, não há um devido processo legal, pois ambos os lados não são ouvidos. Nesses casos o ônus da prova cabe ao titular dos dados sendo ele quem tem de provar que não deveria pertencer ao grupo colocado pelo Estado ou corporações. (MARTINS, 2019).

Por fim, outro risco ligado à criação de perfis é o lado ruim humano onde pessoas que detém os dados de outras pessoas analisadas (membros do Estado, funcionários de corporações, hackers) 9 podem usá-los de forma abusiva. Isso piora quando um perfil pode ser associado com precisão a um indivíduo identificável. Logo um perfil antes particular que se torna público pode acarretar danos à reputação do indivíduo ou seus dados podem ser utilizados para fins nocivos. (MARTINS, 2019).

Diante disso, é possível verificar que o *Big Data* é mais invasivo, tendo em vista a capacidade de coletar, armazenar e tratar dados de maneira detalhista e minuciosa.

Os dados podem ser utilizados em ferramentas e softwares que importem comportamentos nãos espontâneos das pessoas, é possível influenciar ou até mesmo restringir a identidade pessoal.

> A noção de consentimento cristalizada na doutrina nacional e internacional possui como norte a ideia de manifestação livre, informada e inequívoca de concordância do titular com o tratamento de seus dados pessoais. No entanto, não há como anuir de forma livre, informada e inequívoca no contexto em que sensores, câmeras e demais dispositivos estão coletando dados pessoais de modo automático, uma vez que a compra dos produtos já poderá implicar o consentimento tácito da coleta de dados para o grande banco de dados. (MÁRTIN; SILVA; BARATIERI, 2019, p.11)

A LGPD causará grande impacto no *Big Data*, ainda existirão grandes oportunidades a serem exploradas nesta alta tecnologia, mas cada vez mais será necessário qualificar o processo de tratamento de dados dessas informações, para que gerem resultados efetivos para os negócios e também para que as práticas estejam alinhadas e de acordo com a LGPD.

> Assim, neste cenário de intensa valorização e proteção de dados pessoais, a exploração de *Big Data* impõe a necessidade de implementação de medidas técnicas para assegurar o *compliance* com as normas jurídicas. Isso porque as próprias características inerentes ao *Big Data*, merecem atenção especial, no intuito de evitar a aplicação das sanções previstas em casos de incidentes envolvendo o vazamento de dados ou pelo desrespeito aos dispositivos das normas de proteção de dados pessoais, tanto aqueles previstos no Regulamento Europeu (GDPR), quanto aqueles previstos na norma nacional (Lei 13.709/2018). (CERVANTES; RODRIGUES, 2020, p. 21)

Inicialmente será causado um impacto negativo nas atividades de coleta e tratamento de dados pela LGPD no *Big Data*, mas isso deve ser reduzido ao passo que as empresas consigam aplicar e estruturar seus programas de *compliance* e integridade de dados, se adequando as regras trazidas pela LGPD. Após isso, existirá um ambiente mais seguro, confiável e adequado à proteção dos direitos fundamentais de liberdade e privacidade da sociedade.

## 4.2 POLÍTICAS DE PRIVACIDADE

As políticas de privacidade serão outra importante adequação das empresas frente à LGPD, pois faz parte da estrutura de documentos para a proteção de dados. Tem como principal objetivo dar visibilidade ao tratamento de dados pessoais em um determinado serviço, atendendo aos princípios da LGPD. É um documento público endereçado aos usuários de determinado serviço.

O conteúdo dessas políticas tem o direito de informar, o direito de ser informado, a faculdade de receber informação e a faculdade de investigar (não só o fato, mas a própria informação), que são os responsáveis por transformarem o recebedor da informação de mero espectador para sujeito de direitos, além de serem de fácil compreensão. (DE CARVALHO, 2002, p. 554).

No momento da compra ou prestação de qualquer serviço, é importante que não seja levado em consideração apenas a efetivação do direito de consumo, não se resume apenas a condições materiais. Pressupõe que no ato de consumo sejam respeitadas a dignidade, saúde e segurança do consumidor, a proteção de seus interesses econômicos, a melhoria de sua qualidade de vida e, sobretudo, a transparência e harmonia nas relações de consumo (DORINI, 2010, p. 934).

> A política de privacidade, por sua vez, descreve, especificamente, os tratamentos de dados pessoais que serão realizados e sua extensão, na medida em que o titular consentir com os termos de uso. Por conseguinte, a função dessa espécie de documento é esclarecer como os dados do usuário serão utilizados e para qual finalidade. (CARVALHO, 2014, p.23).

Quanto ao conteúdo que deve constar na política, de acordo com Freitas (2019), é preciso observar as seguintes informações:

> Informações sobre a organização responsável pelo tratamento;
> Dados pessoais e respectivas finalidades do tratamento, inclusive os dados não informados pelo usuário (exemplo: IP, localização, etc);
> Base jurídica do tratamento;
> Prazo de retenção dos dados pessoais;

> Informações de contato do *Data Protection Officer* (DPO) ou encarregado de proteção de dados da organização. (FREITAS, 2019, p.02)

Além disso, também deve constar uma orientação a respeito da forma que o titular será atendido, informando como ele pode acessar, retificar, solicitar a exclusão de seus dados, transferir, limitar ou até mesmo se opor ao tratamento e retirar o seu consentimento. Ela deve estar disponível ao titular antes do início do tratamento do dado, permitindo que ele possa avaliar os termos quando necessário for.

> É importante garantir que a política esteja facilmente disponível. Dessa forma, a organização demonstra profissionalmente seu compromisso com a transparência no tratamento dos dados pessoais. E o usuário deve demonstrar seu expresso consentimento e concordância com os termos da política antes do início desse tratamento. (FREITAS, 2019, p. 02)

Para auxiliar as empresas neste ponto, a Secretaria de Governo Digital está desenvolvendo uma ferramenta onde órgãos e entidades da administração pública poderão responder um questionário com algumas informações, e ao final terão o texto completo para o termo de uso e política de privacidade. O objetivo buscado é facilitar a elaboração desses documentos para os serviços públicos prestados por meio de aplicações, sítios, sistemas e aplicativos. (FREITAS, 2019).

Apesar desta ferramenta gerar um texto completo, o Guia ressalta que cada serviço possui características especificas que não podem ser abordadas através da ferramenta. Dessa forma, o termo gerado será editável, e dependerá de uma análise técnica de cada instituição pois pode precisar de ajustes necessários para incluir maiores informações, mais precisas e detalhadas do serviço prestado.

## 4.3 COMO AS EMPRESAS DEVEM SE ADEQUAR AS NOVAS EXIGÊNCIAS

O fornecimento de dados ampliou-se ainda mais com o desenvolvimento eletrônico de relações humanas, e essa circulação traz ameaças a privacidade, muitos autores afirmam que a proteção de dados pessoais encerrou um aspecto fundamental de uma nova face de liberdade – a liberdade informática. Assim surgiu a LGPD e juntamente com ela diversos desafios às empresas dos mais diversos segmentos.

Como consequência da ampla previsão de direitos previstos na Lei Geral de Dados, as empresas deverão adotar medidas de controles e notificações até então não tomadas, para que estejam em conformidade com aquilo que prevê a legislação. Conforme art. 50 da referida Lei, as empresas deverão ter um programa de governança em privacidade seguindo alguns parâmetros regulamentados.

Dentre os principais desafios da LGPD está a missão de conscientizar a sociedade de que o dado pessoal é um bem de valor, que assim como qualquer outro também deve ser protegido, sob pena de acarretar prejuízos ao indivíduo caso utilizado de forma indevida e para fins diversos do que foi concedido pelo titular, é uma mudança de "*mind set*".

Outro ponto importante é a complexidade das ações de adequação da LGPD nas empresas, considerando todos os ajustes que terão de serem feitos em seus sistemas internos e procedimentos, conforme já abordado nos capítulos anteriores.

Cada vez mais as empresas deverão estar em *compliance*, como vimos no capítulo anterior, e para isso a Associação Brasileira de Anunciantes elencou os principais pontos que devem conter um programa de governança adequado à LGPD, que se enquadram para qualquer ramo empresarial:

> a. demonstrar o comprometimento da empresa 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. ser aplicável a todo o conjunto de dados pessoais que estejam sob o controle da empresa, independentemente do modo como se realizou sua coleta;
> c. ser adaptado à estrutura, à escala e ao volume das operações da empresa, bem como à sensibilidade dos dados tratados;
> d. estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
> e. ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
> f. estar integrado a sua estrutura geral de governança de forma a estabelecer e aplicar mecanismos de supervisão internos e externos;
> g. contar com planos de resposta a incidentes e remediação; e
> h. ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas. (MANUAL ABA, 2019, p.17).

Algumas destas práticas podem ser adotadas com recursos audiovisuais, que otimizam a clareza e objetividade das informações, gerando maior flexibilidade ao usuário e disponibilidade para empresa. Sobre estes recursos, pode-se adotar a utilização de vídeos, imagens e infográficos para ilustrar processos e tratamentos de dados pessoais tornam as informações mais atrativas e compreensíveis aos usuários. Da mesma forma, informações simples e diretas, evitando ambiguidades e termos demasiadamente técnicos auxiliam a compreensão (MANUAL ABA, 2019).

Como o usuário terá a liberdade de concordar ou não com o fornecimento de seus dados pessoais e gerenciar suas escolhas de privacidade, outra prática interessante a ser adotada é a de flexibilizar ao usuário esta escolha por meio de painéis de controle (*dashboards*) ou ferramentas similares. Entretanto, não deve ser apresentado *checkboxes* pré marcadas, bem como não é recomendada coleta de dados excessivos ou desnecessários (MANUAL ABA, 2019).

Diante dessa liberdade do usuário também é preciso que a empresa esteja sempre disponível, o que nos leva a outra prática que é a criação de um canal de atendimento e comunicação, para que os usuários consigam entrar em contato com a empresa de maneira fácil e simplificada, para que possam sanar suas dúvidas com mais agilidade (MANUAL ABA, 2019).

Estas são algumas práticas que auxiliarão as empresas na adequação, é evidente que por trás de tudo isso haverá grande trabalho e esforço principalmente para aquelas que terão de começar do zero, mas é um trabalho imprescindível, que trará resultados e evitará penalizações.

## 5 CONCLUSÃO

A presente pesquisa teve como principal objetivo estudar a nova Lei 13.709/2018, mais conhecida como LGPD, que regulamenta qualquer tipo de coleta e tratamento de dado pessoal, para, a partir de então, analisar qual será sua aplicabilidade nas relações sociais e verificar os efeitos que causará no mercado de consumo da atualidade.

Inicialmente, no primeiro capítulo buscou-se compreender o que é um dado pessoal, este “novo petróleo” como é exibido em muitas mídias. O dado pessoal nada mais é do que toda e qualquer informação relacionada a pessoa natural identificada ou identificável, não limitando-se apenas a nome e sobrenome, mas sim a qualquer informação que seja capaz de identificar uma pessoa, como dados de localização por exemplo.

Contextualizando a evolução histórica da legislação de proteção de dados, revelou-se, que este já é um tema regulamentado em diversos países há muito tempo, porém, a legislação mais importante e que serviu de exemplo para o Brasil é recente, a General Data Protection Regulation – GDPR, surgiu na Europa em 2016. Após ela, muitos países se inspiraram e lançaram a própria regulamentação, tendo sido o Brasil um dos últimos países da América Latina a implementar uma legislação específica sobre o tratamento de dados.

No que concerne a legislação em específico, no segundo capítulo esta pesquisa se deteve a uma breve análise sobre a LGPD. No ambiente jurídico, ela é considerada uma das leis mais importantes a ser incorporada em nosso ordenamento, deixando claro em seu próprio nome que o maior objetivo é assegurar a proteção da pessoa natural e o livre desenvolvimento de sua personalidade. Ela dedica um capítulo exclusivo para tratar sobre os direitos dos indivíduos, e a partir daí evidenciou-se que muitos deles foram vinculados à alguns direitos fundamentais do art. 5° da Constituição Federal.

É interessante frisar que se trata de uma legislação com severas penalidades caso ocorra o seu descumprimento, as sanções aplicáveis em caso de vazamento de dados, por exemplo, partem de advertência administrativa podendo chegar a multa de até 2% do faturamento do último exercício da empresa. O que levou a criação da

ANPD – Autoridade Nacional de Proteção de Dados, que será a responsável por toda fiscalização, e análise em caso de autuação por desconformidade.

No terceiro capítulo desta pesquisa, foi explicitada as consequências e os desafios que as empresas terão para se adequar a legislação. Foi destacado a questão do *Big Data*, que é o termo utilizado para análises de dados em grandes escalas através de alta tecnologia, gerando índices mais assertivos e eficientes para as empresas. Este sofrerá grandes impactos com a LGPD, em razão de que o titular do dado deve fornecer um consentimento para o tratamento deste, que deve ser claro, objetivo e que tenha destacado a finalidade da coleta daquele dado, ou seja, não poderá ser um termo genérico.

As empresas deverão adotar políticas de privacidade para que possam dar visibilidade do tratamento de dados aos usuários, o que também será um trabalho a ser desenvolvido por muitas empresas que até então não possuíam este tipo de regulamento, principalmente para as de pequeno porte. Considerando todos os ajustes necessários para que as empresas se adequem, pode-se afirmar que terão que despender de ações complexas para adaptarem-se.

Diante da pesquisa realizada, conclui-se que a LGPD será aplicada em toda e qualquer relação que exista, seja ela de consumo ou não, envolvendo o uso, coleta ou tratamento de um dado pessoal. Por mais que estes dados sempre circularam livremente, com o passar do tempo eles foram mais requisitados pelas empresas por fins estratégicos, pois com o avanço da tecnologia muitos processos se tornaram possíveis de serem feitos com a utilização de dados.

Muitos autores relatam que o Brasil se ateve a criar uma legislação específica para o tratamento de dados pois estava encontrando diversos empecilhos em negociações com países estrangeiros que possuíam regulamentação para tanto. Mas através deste estudo, percebeu-se que expomos nossos dados com muita facilidade, e na maioria das vezes acaba sendo desnecessário, por isso, a LGPD se faz necessária para regulamentar este tipo de comportamento.

Ficou claro que o maior desafio com a vigência da LGPD será o das empresas que terão de se adequar, afinal, para os indivíduos proprietários dos dados pessoais ela só trouxe benefícios, garantindo que ninguém utilize seu dado de maneira indevida

ou para fins diversos daqueles acordados. Já as empresas deverão adotar diversas práticas para demonstrar comprometimento em assegurar o cumprimento da legislação, consequentemente passando maior confiança aos usuários de seus serviços.

As boas práticas de governança serão muito importantes neste momento, deve-se começar olhando para a política de privacidade e criando uma, caso esta não exista, isso é exigido pela LGPD por fazer parte da estrutura de documentos para a proteção de dados. É importante que cada empresa possua a sua de acordo com seu ramo e as atividades desenvolvidas, por mais que o tratamento de dados seja o mesmo para diversos setores, cada um possui a sua particularidade, e uma política clara e precisa facilitará na adequação do restante.

Além disso, um programa de *compliance* se mostra mais efetivo agora com a entrada em vigor da LGPD, ele é o responsável pela conformidade com as regras, e por prover uma organização interna e externa adequada aos normativos e regulamentações. Tendo isso, os impactos causados pela adequação não serão tão severos pois através dele será possível verificar o que está em desconformidade. Um programa efetivo será capaz de manter a empresa sempre de acordo com a legislação vigente evitando que venham a ocorrer algumas sanções.

Diante dessa percepção, as empresas possuem muito trabalho pela frente, mas devem saber aproveitar o momento para se adequarem por algo que não tem mais volta, o dado pessoal é e será cada vez mais disputado. Espera-se que o estudo desta pesquisa possa contribuir de algum modo para uma melhor compreensão da legislação, e também para que torne todo este processo de adequação mais descomplicado e célere.

## REFERÊNCIAS


AGÊNCIA SENADO. **Senado confirma primeira diretoria da Autoridade Nacional de Proteção de Dados.** 2020. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/10/20/senado-confirma-primeira-diretoria-da-autoridade-nacional-de-protecao-de-dados
Acesso em: 22 novembro de 2020.

BALLICO, Louise Finger; REDECKER, Ana Cláudia. **O PAPEL DOS AGENTES NA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)**. 2020. Disponível em: https://www.cidp.pt/revistas/rjlb/2020/5/2020_05_0125_0170.pdf
Acesso em: 22 novembro de 2020.

BLANCHET, R.; TAVARES, D. **Os 10 principais direitos dos titulares previstos na LGPD.** CIO FROM IDG, 2020. Disponível em: https://cio.com.br/tendencias/os-HYPERLINK "about:blank"10-principais-direitos-dos-titulares-previstos-na-lgpd/
Acesso em: 17 de outubro de 2020.

BRASIL, Constituição (1998). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1998.

BRASIL, **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília/DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
Acesso em: 17 de outubro de 2020.

BRASIL, **Medida Provisória nº 936, 2020.** Institui o Programa Emergencial de Manutenção do Emprego e da Renda e dispõe sobre medidas trabalhistas complementares para enfrentamento do estado de calamidade pública reconhecido pelo Decreto Legislativo nº 6, de 20 de março de 2020, e da emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020, e dá outras providências. Brasília/DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv936.htm
Acesso em: 17 de outubro de 2020.

BRASIL, **Projeto de Lei 1.179 de 2020**. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do Coronavírus (Covid-19). Brasília/DF. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8081779 HYPERLINK "about:blank"& HYPERLINK "about:blank"ts=1587403348718 HYPERLINK "about:blank"& HYPERLINK "about:blank"disposition=inline
Acesso em: 20 de outubro de 2020.

CABRAL, T. LGPD E VAZAMENTO DE DADOS: COMO A LEI PODE ATUAR? **Athena Security.** Disponível em: https://blog.athenasecurity.com.br/lgpd-vazamento-de-dados/
Acesso em: 23 de novembro de 2020.

CAETANO, J. V. L. O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (GDPR): UMA ANÁLISE DO EXTRATERRITORIAL SCOPE À LUZ DA JURISDIÇÃO INTERNACIONAL. **Cadernos Eletrônicos Direito Internacional sem Fronteiras**. v. 2, n. 1, 2020.

CAPEZ, F. Lei Geral de Proteção de Dados: origem histórica. **Economia**. 2020. Disponível em: https://economia.ig.com.br/colunas/defesa-do-consumidor/2020-06-01/lei-geral-de-protecao-de-dados-origem-historica.html
Acesso em: 20 de outubro de 2020.

CARVALHO, A. THAIS. **APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS E DA METODOLOGIA PRIVACY BY DESIGN NOS TERMOS DE USO E DE POLÍTICA DE PRIVACIDADE**. Vitória: FDV, 2019. Disponível em: http://repositorio.fdv.br:8080/bitstream/fdv/781/1/TCC%20-%20Thais%20Abreu.pdf
Acesso em: abril de 2021.

CERVANTES, Vinicius; RODRIGUES, Fernando David. As ciências jurídicas e a regulação das relações sociais. **BIG DATA E PROTEÇÃO DE DADOS: O DESAFIO ESTÁ LANÇADO**, Belo Horizonte, v. 2, 2020. Disponível em: http://www.direitorp.usp.br/wp-content/uploads/2019/06/IInovacao-BigData-Cervantes-Rodrigues.pdf.
Acesso em: abril de 2021.

DONEDA, Danilo; MENDES, Laura Schertel. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da Proteção de Dados no Brasil. **Revista de Direito do Consumidor**, vol. 120/2018, 2018.

DONEDA, Danilo Cesar Maganhoto et al. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. V. 2. Brasília. 2010. Disponível em: https://legado.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf
Acesso em: 20 de outubro de 2020.

FARINHO, Domingos Soares; FRAZÃO, Ana de Oliveira. **Programas de integridade e governança das empresas estatais**: uma visão portuguesa no contexto da União Europeia. Belo Horizonte, 2018)

FAUSTINO, A. A proteção de dados pessoais no Brasil: Breve histórico do direito comparado até a atual realidade brasileira. **Âmbito Jurídico**. 2016. Disponível em: https://ambitojuridico.com.br/edicoes/revista-154/a-protecao-de-dados-pessoais-no-brasil-breve-historico-do-direito-comparado-ate-a-atual-realidade-brasileira/
Acesso em: 28 de outubro de 2020.

FERRARI, Rosane F. [et al.] (Org**.). Manual de normas técnicas para a produções acadêmicas da URI** [Recurso eletrônico]. Frederico Westphalen, RS: URI, 2017. Disponível em: http://www.uricer.edu.br/site/informacao.php?pag_invoked=buscar_principal.
Acesso em: 15 de novembro de 2020.

FILHO, D. R. A Diretiva Europeia sobre proteção de dados pessoais. **Jus.com.br**, 2013. Disponível em: https://jus.com.br/artigos/23669/a-diretiva-europeia-sobre-protecao-de-dados-pessoais/
Acesso em: 28 de outubro de 2020.

FRADE, M. Aba Lança “Manual Aba Para Adequação à LGPD: Orientações e Boas Práticas de Governança de Dados Para Publicitários". **Pinheiro Neto Advogados**. 2019. Disponível em: http://www.pinheironeto.com.br/imprensa/aba-lanca-manual-aba-para-adequacao-a-lgpd-orientacoes-e-boas-praticas-de-governanca-de-dados-

para-publicitarios
Acesso em: 15 de novembro de 2020.

FRAZÃO, Ana de Oliveira. A nova Lei de Proteção de Dados Pessoais: Principais Repercussões para a Atividade Empresarial, Parte I. **JOTA**, 2020 Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/novalgpd-principais-repercussoes-para-a-atividade-empresarial-29082018
Acesso em: 28 de outubro de 2020.

FREITAS, Carla. Serpro e LGPD: Segurança e Inovação. **Como elaborar uma política de privacidade aderente à LGPD?, 2019.** Disponível em: https://www.serpro.gov.br/lgpd/noticias/2019/elabora-politica-privacidade-aderente-lgpd-dados-pessoais
Acesso em: 10 de abril de 2021.

GÜNTHER ET AL, Wendy Arianne. **Debating big data: A literature review on realizing value from big data.** sciencedirect. 2017. Disponível em: https://www.sciencedirect.com/science/article/pii/S0963868717302615. Acesso em: 10 de abril de 2021.

**IBGC.** Código das melhores práticas de governança corporativa. **Disponível em:** https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21138
**Acesso em: 15 de novembro de 2020.**

LOPES, E. Os desafios da LGPD diante da não conformidade corporativa. **Consultor Jurídico**. 2020. Disponível em: https://www.conjur.com.br/2020-set-29/everton-lopes-lgpd-nao-conformidade-corporativa
Acesso em: 15 de novembro de 2020.

MALDONADO, Viviane Nóbrega et al. **LGPD Lei Geral de Proteção de Dados Comentada**. 2. ed., São Paulo: Thomson Reuters Brasil Conteúdo e Tecnologia Ltda, 2019.

MALDONADO, Viviane Nóbrega; GUTIERREZ, Andrei. A estratégia brasileira para a transformação digital e as questões que dela emergem no que se refere à proteção de dados pessoais. **Revista dos Tribunais**. São Paulo; v. 993, p.293-304, jul. 2018.

MANUAL ABA para adequação à LGPD: orientações e boas práticas de governança de dados para Publicitários. **Associação Brasileira de Anunciantes – ABA.** 2019. Disponível em: http://aba.com.br/wp-content/uploads/2020/07/Manual_LGPD_04_junho.pdf
Acesso em: abril de 2021.

MÁRTIN M., Taynara; SILVA, Arceno; LUCAS, Baratieri Francisco. Congresso Internacional de Direito e Contemporaneidade. **Big Data e Proteção de Dados: Uma Relação Possível(?)**, Santa Maria/RS, set. 2019.
Acesso em: abril de 2021.

MARTINS, Daniel. **BigData, revolução digital e o Direito**. mercurylbc. 2019. Disponível em: http://mercurylbc.com/bigdata-revolucao-digital-e-o-direito/.
Acesso em: abril de 2021.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13. 709/2018) e o Direito do Consumidor. **Revista dos Tribunais**. São Paulo; v. 1009, p. 173-222, nov. 2019.

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?**. Rio de Janeiro: Instituito Igaparé, dez. 2018.

NETTO, T. Sanções e Fiscalização na LGPD: O Relatório de Impacto à Proteção de Dados Pessoais. **Instituto de Direito Real**. 2020. Disponível em: https://direitoreal.com.br/artigos/sancoes-e-fiscalizacao-na-lgpd-o-relatorio-de-impacto-a-protecao-de-dados-pessoais
Acesso em: 15 de novembro de 2020

NUNES, G. V. M. **GOVERNANÇA E BOAS PRÁTICAS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: DOS PROGRAMAS DE COMPLIANCE.** 2019. 51 f. Trabalho de Conclusão de Curso (Especialização)–Universidade de Brasília, Brasília, 2019. <Disponível em: https://www.bdm.unb.br/bitstream/10483/25080/1/2019_GabrielaVictoriaMirandaNunes_tcc.pdf>.
Acesso em: 15 de novembro de 2020.

NUNES, M. Natalia. **10 princípios da LGPD para o tratamento de dados pessoais. 2019**. Disponível em: https://ndmadvogados.jusbrasil.com.br/artigos/698194397/10-principios-da-lgpd-para-o-tratamento-de-dados-pessoais
Acesso em: 10 de novembro de 2020.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais Comentários à Lei N. 13.709/2018 (LGPD)**. São Paulo: Saraiva, 2018.

REANI, V. Impactos da Lei Geral de Proteção de Dados para os negócios e as pessoas. **Consultor Jurídico**. 2018. Disponível em https://www.conjur.com.br/2018-out-25/valeria-reani-impactos-lei-protecao-dados-negocios
Acesso em: 28 de outubro de 2020.

Revista Jurídica Cesumar. **Big Data e a Proteção do Direito à Privacidade no Contexto da Sociedade da Informação**, São Paulo, v. 19, n. 3, set./dez. 2019.

SERPRO. **Quem vai regular a LGPD?** Brasília. Disponível em: https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd
Acesso em: 10 de novembro de 2020.

SILVA, L. B; SILVA, R. L. A PROTEÇÃO JURÍDICA DE DADOS PESSOAIS NA INTERNET: análise comparada do tratamento jurídico do tema na União Europeia e no Brasil. **XXII Encontro Nacional do CONPEDI / UNICURITIBA**. 2013. Disponível em: http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65
Acesso em: 10 de novembro de 2020.

VARELLA, L. TUDO sobre a Lei Geral de Proteção de Dados (LGPD). **Compugraf**. 2019. Disponível em: https://www.compugraf.com.br/tudo-sobre-a-lei-geral-de-protecao-de-dados-lgpd/
Acesso em: 28 de outubro de 2020.

WESTCON. **Quais os benefícios do big data analytics para os negócios?** Brasil, 2019. Disponível em: https://blogbrasil.westcon.com/quais-os-beneficios-do-big-data-analyticspara-os-negocios.
Acesso em: 15 de abril de 2021.