PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

MONOGRAFIA

A PROTEÇÃO DOS DADOS E A LGPD:

DESAFIOS NA IMPLEMENTAÇÃO DA LGPD

ORIENTANDO: KAIO ALVES CAIRES

ORIENTADORA PROFª. DRA. FATIMA DE PAULA FERREIRA

GOIÂNIA-GO

2023

KAIO ALVES CAIRES

A PROTEÇÃO DOS DADOS E A LGPD

DESAFIOS NA IMPLEMENTAÇÃO DA LGPD

Monografia Jurídica apresentado à disciplina Trabalho de Curso II, da Escola de Direito , Negócios e Comunicação da Pontifícia Universidade Católica de Goiás(PUC GOIÁS).
Profª. Orientadora Dra. FATIMA DE PAULA FERREIRA.

GOIÂNIA-GO

2023

RESUMO

Com a entrada em vigor da Lei Geral de Proteção de Dados (Lei 13.709/2018, a “LGPD”) muitas empresas têm se deparado com desafios para a sua implementação. A Lei exige que as organizações passem a adotar procedimentos claros e medidas técnicas adequadas para proteção de dados este trabalho tem como objetivo fazer uma análise sobre a Lei de Proteção de Dados – LGPD, e como está sendo implementada no Brasil. A análise aborda, como os dados pessoais se tornaram tão importantes na era digital, como o direito à privacidade e à proteção de dados pessoais está sendo tratado, como surgiu a necessidade da criação de uma lei de proteção a esses dados, sua estrutura, seus elementos e como está sendo a sua implementação por parte das instituições. Neste intuito, realizou-se um trabalho a partir da exploração da legislação vigente, da pesquisa bibliográfica e documental sobre o referido tema.

Palavras chave: Proteção de Dados, Desafios, Implementação, LGPD

LISTA DE ABREVIATURAS E SIGLAS

LGPD

GPDR

DPO

ANPD

SUMÁRIO

INTRODUÇÃO

O tema proteção de dados tem ganhado grande relevância diante dos avanços tecnológicos e da sua expansão, bem como do uso dos meios digitais na disseminação da informação, da comunicação e das redes sociais.

Desde o seu surgimento, as tecnologias trouxeram grandes transformações nas relações humanas e nos costumes sociais. O seu uso tornou-se imprescindível nos mais diversos setores: na educação, na medicina, no trabalho, no entretenimento. As pessoas, independentemente de sua geração, não conseguem mais viver sem a tecnologia e com isso, a experiencia humana foi otimizada. A vida se tornou mais conveniente com a tecnologia.

A cada acesso à internet, o usuário deixa registrado vários dados pessoais, o que se torna informação. A informação passou a ser um ativo de grande relevância no ambiente virtual e despertou grande interesse por parte das instituições. Mas o que é feito com essas informações despertou na sociedade a necessidade de proteção aos seus dados. E de uma lei que regulamentasse seus direitos à privacidade e a proteção de dados.

Em 2018, o Brasil estabeleceu sua Lei Geral de Proteção de Dados LGPD (Lei 13.709 de 2018) e entrou em vigor em 18 de setembro de 2020.

Com o objetivo principal é destacar como a lei geral de proteção de dados age para garantir aquilo que lhe é previsto, visto que o objetivo dela é a proteção e tratamento correto dos dados pessoais.

A pesquisa analisou minuciosamente o fato de que nos meios digitais são uma das principais formas de transmitir e receber informações, contendo inúmeros dados pessoais nesses dispositivos, como também a necessidade de algumas mudanças em relação ao tratamento de dados fornecidos pelos

usuários, existindo as sanções e punições para aqueles que não cumpre o previsto em lei.

O método utilizado na pesquisa foi o hipotético-dedutivo, visto que foi analisado a Lei 13.709/18, seus termos e objetivos, levando em consideração o cenário atual com relação a implementação nos meios digitais e tecnologias bem como a proteção de tais dados pessoais.

A LGPD – Lei de Proteção de Dados Pessoais, alcança todos os processos que de alguma forma tratam dados pessoais digitais e analógicos dos titulares que se relacionam com qualquer instituição. O seu objetivo é garantir direitos fundamentais dos titulares, tais como privacidade, igualdade, autodeterminação informativa e liberdade. Ela veio garantir segurança e proteção jurídica ao titular dos dados diante de sua vulnerabilidade perante os agentes de tratamento.

O presente artigo tem como objetivo fazer uma análise da Lei Geral de Proteção de Dados e dos desafios na sua implementação. A análise aborda, como os dados pessoais se tornaram tão importantes na era digital, como o direito à privacidade e à proteção de dados pessoais está sendo tratado, como surgiu a necessidade da criação de uma lei de proteção a esses dados, sua estrutura, seus elementos e como está sendo a sua implementação por parte das instituições. Neste intuito, realizou-se um trabalho a partir da exploração da legislação vigente, da pesquisa bibliográfica e documental sobre o referido tema.

No momento atual, e passados mais de dois anos desde que entrou em vigor, o cumprimento da lei é encarado como uma atividade obrigatória. No entanto, pela alta complexidade e quantidade de detalhes existentes sobre a legislação, é compreensível a dificuldade que muitas empresas possuem em entender se todos os pontos dela estão sendo seguidos**.** Elas têm se deparado com desafios para a implementação. A Lei exige que as organizações passem a adotar procedimentos claros e medidas técnicas adequadas para proteção de dados, representando uma verdadeira mudança em todas as áreas da organização.

Estar por dentro de tudo o que diz respeito a LGPD pode ser um verdadeiro desafio para as empresas que lidam diretamente com os dados dos

titulares, tendo em vista ainda as constantes mudanças e atualizações encontradas.

Apesar de ser um desafio, pois exige um cuidado intenso e contínuo, adequar-se à LGPD trata-se de um passo fundamental não apenas para obedecer a Lei, mas para oferecer uma experiência mais eficiente e alinhada com as expectativas e necessidades do cliente final.

Com isso se mostra evidente a necessidade da efetiva aplicação da lei de proteção de dados, para que os dados sejam usados de forma correta e idônea não causando nenhum prejuízo ao cidadão, como também a criação de leis mais especificas, se adaptando a evolução da tecnologia, buscando assim a solução do problema proposto.

CAPÍTULO I

A IMPORTÂNCIA DOS DADOS PESSOAIS, PRIVACIDADE E PROTEÇÃO DE DADOS NA ERA DIGITAL

Com os avanços tecnológicos, suas inovações, como também sua expansão por todo o mundo, chegamos à era digital. A era da informação. Tornando-se possível, através da tecnologia, transmitir em velocidade instantânea, conhecimento e informação para a sociedade, sem a limitação de tempo e espaço.

Com a criação da internet móvel, as pessoas elegeram o celular como o principal dispositivo de acesso à internet e um bem indispensável no seu cotidiano. Atualmente, nem todas as residências, nem todos os comércios, tem computador, mas o celular está presente em quase todos os lugares. Utilizando os smartphones, ou outros tipos de aparelhos, as pessoas ficaram cada vez mais conectadas e os usuários passaram a utilizar os meios digitais para acesso a todo tipo de conhecimento, transações, comunicações. Em qualquer lugar que estejam, fazem uso de serviços, de compras de produtos, de comunicação, de transmissões em tempo real, de transações negociais, enfim, uma infinidade de acessos ao longo do dia, em busca de facilidade e satisfação pessoal.

Mas o uso" gratuito" dos produtos e serviços *on-line*, passa a ser lucrativo para os negócios, pois carrega em si uma infinidade de informações. Ao fazer uso desses serviços várias informações estão sendo coletadas e agregadas, assim há a inserção dos dados pessoais na economia da informação, passando a ser o vetor central da publicidade comportamental. A informação passou a ser um ativo de grande importância e; em meio a diversidade de informações geradas no ambiente virtual, está o fornecimento de dados pessoais.

Dessa forma, afirma-se que o pagamento pelos serviços utilizados, são os dados do usuário.

Segundo Stefano Rodotá (2008, p. 113):

> A contrapartida necessária para se obter um bem ou um serviço não se limita mais à soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações. Nessa troca, então, não é mais somente o patrimônio de uma pessoa que está envolvido. A pessoa é obrigada a expor seu próprio eu, sua própria persona, com consequências que vão além da simples operação econômica e criam uma espécie de posse permanente da pessoa por parte de quem detém as informações a seu respeito

Nesse cenário há um movimento de empresas que buscam captar a maioria de informações dos usuários. Por meio de diversas ferramentas tecnológicas, entre elas destaca-se os *cookies*, tornou-se possível rastrear a

navegação do usuário, e assim, identificar seus interesses, podendo correlaciona-los aos anúncios publicitários. O registro dessa navegação dos usuários na internet retrata suas preferencias, de forma que se possa personalizar seu perfil de consumo.

Conforme RODOTÁ (2008 p.184):

> Quanto mais os serviços são tecnologicamente sofisticados, mais os indivíduos deixam nas mãos do fornecedor do serviço uma cota relevante de informações pessoais; quanto mais a rede de serviços se alarga, mais crescem as possibilidades de interconexões entre banco de dados e de disseminação internacional das informações coletadas.

Mas o titular dos dados não sabe exatamente como será feito o uso dos seus dados, ou com quais outras informações poderão ser cruzadas.

Por conta disso, a necessidade de se ter um instrumento normativo que trate desse tema, decorre da forma como o modelo atual de negócios da sociedade digital está sustentado. Da importância da informação dos dados pessoais como instrumento de troca pela utilização de produtos e serviços digitais.

1.2 PRIVACIDADE E PROTEÇÃO DE DADOS

Cada vez mais, as atividades de processamento de dados têm ingerência na vida das pessoas. Atualmente, vivemos numa sociedade que se orientam e movimentam a partir do “dossiê digital” do cidadão. Um tipo de cadastro que contém informações pessoais de um indivíduo, suas preferencias, sua localização, seus acessos habituais.

A história da humanidade demanda não somente as inovações tecnológicas, mas também a proteção dos indivíduos. E a proteção de dados veio como uma resposta aos excessos de coleta e processamento e tratamento de informações e dados pessoais das pessoas.

Entre os direitos fundamentais, consagrados em todas a constituições do mundo, a privacidade foi um deles. Mas a proteção de dados é fruto do amadurecimento da sociedade, da necessidade de regulação da proteção de dados pessoais dos indivíduos.

A privacidade está intimamente ligada com aquilo que somos, temos, queremos, e com aquilo que queremos que outras pessoas saibam de nós. De forma geral, protege o indivíduo da intromissão ao seu espaço pessoal, enquanto a proteção de dados regulamenta o processamento dos seus dados, sendo privados ou não.

Ainda que a privacidade seja um direito universal, tratado inclusive no artigo 12 da Declaração Universal do Direitos Humanos, o fato é que a privacidade do indivíduo é um direito relacionado a sua esfera pessoal.

A privacidade não beneficia somente o indivíduo, mas também a sociedade, revelando-se como um elemento constitutivo da própria vida em sociedade.

Proteção de dados difere de privacidade na medida em que impõe controle do Estado sobre que trata, e não somente controle do cidadão sobre sua própria informação.

Os dados pessoais não estão relacionados somente com a privacidade. Estão ligados ao controle de informações pessoais do que seja algo íntimo ou privado do sujeito.

Evidenciou-se, no mundo, um crescimento significativo do risco e ocorrências de vazamentos de dados pessoais, coleta de dados em excesso, tratamento sem consentimento, entre outras ameaças ao direito da privacidade, devido a crescente integração de plataformas digitais,

Com o advento do mundo "*Big Data"* que proporcionou volume de informações em massa, a proteção de dados e a segurança da informação passaram a ostentar posição de protagonismo empresarial, legislativo, social e econômico, considerando que a circulação de informações, principalmente em âmbito digital, se tornou atrativa para criminosos virtuais

Segundo LIMA (2021 p48):

> Cada vez mais os modelos de negócios são construídos em torno do tratamento de dados, de modo que a regulação da atividade empresarial, não há nenhuma dúvida, passa pela reflexão sobre a necessidade de uma Autoridade de Proteção de Dados e – o que talvez seja mais desafiador – sobre a avaliação de seu papel nesses mercados permeados por modelos de negócio estruturados quase que exclusivamente na consideração do valor dos dados coletados e de seu tratamento por empresas especializadas se em um contexto empresarial dito off-line, a coleta de
> informações ocorria basicamente a partir do fornecimento de dados pelo cliente, as empresas que atuam na rede podem coletar informações sem o seu conhecimento, utilizando esse tipo de informação para personalizar sua atividade de acordo com as necessidades do cliente ou mesmo efetuar a troca dessas informações com os seus parceiros. Não é preciso maiores digressões para estimar o potencial desse tipo de conduta em matéria de aferição do valor comercial de uma empresa ou de seus ativos.

Diante disso vemos que as grandes empresas procuram obter lucros com a coleta dos dados pessoais, fazendo-se presente a necessidade da efetiva aplicação das normas da Lei 13.709/18.

1.2 PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

A demanda regulatória no que concerne a proteção de dados pessoais emerge com mais ênfase devido a preocupação com o processamento massivo dos dados pessoais do cidadão. O rápido desenvolvimento e a expansão da tecnologia no mundo, trouxe como consequência a importância da informação para as instituições, e com isso, a violação da privacidade de seus usuários diante do acesso e da coleta de seus dados.

No Brasil, a proteção de dados não é algo inovador. Em relação às normas internas, o Brasil já previa algum tipo de proteção de dados por meio de alguns instrumentos, tais como:

1.2.1 Código de Defesa do Consumidor

O Código de Defesa do Consumidor relata em seu artigo 43 sobre o banco de dados e o cadastro dos consumidores. Esse normativo vai muito além de uma determinação de prazo para armazenamento de informações negativas do consumidor para obtenção de crédito perante as instituições financeiras, mas também confere ao consumidor direito de controlar as suas informações pessoais.

Ainda no artigo 43, disciplina também que o consumidor deverá ser notificado a respeito da abertura de um banco de dados por ele não solicitado. Assim, esse dever de comunicação permitirá ao consumidor o acompanhamento e a circulação de seus dados pessoais.

O operador do banco de dados deverá garantir ao consumidor o acesso aos seus dados, à exatidão das informações, caso contrário, o consumidor pode solicitar a correção dos mesmos, deverá também garantir que o banco de dados se restrinja a finalidade clara e verdadeira, como também que as informações negativas sejam limitadas a um período de cinco anos para o seu armazenamento.

1.2.1 Lei do Cadastro Positivo

A Lei 12.414 de 2011, trata sobre a formação de um banco de dados sobre pessoas físicas ou jurídicas relativos a operações financeiras e de adimplemento, para que se forme um histórico de crédito com a finalidade de embasar decisões das de concessão de crédito. Assim, a situação econômica do indivíduo, não é mais analisada somente por informações de inadimplência, mas também por informações positivas, por seu histórico de adimplência. Por isso, ficou conhecida como “Cadastro Positivo” devido sua abrangência permitir que a avaliação do crédito do consumidor tenha uma visão positiva, atraindo assim, o interesse das instituições que tendem a facilitar a concessão de crédito àqueles consumidores que pagam as suas dívidas pontualmente.

1.2.2 Lei de Acesso à Informação

Em 2011, surgiu a Lei n. 12.527, norma infraconstitucional que regula com mais detalhes a relação entre acesso à informação e direito à privacidade, além de destacar que este último se refere a todos os dados de natureza pessoal do indivíduo.

Conhecida como Lei de Acesso à Informação, essa norma tem como destinatário específico o Estado, englobando seus órgãos públicos e entidades, o que não impede que suas disposições sirvam de inspiração para o tratamento de dados em outros âmbitos.

De acordo com a Lei 12.527, cabe aos órgãos e às entidades do poder público assegurar a gestão transparente da informação. Para isso, torna obrigatória a divulgação de dados de interesse da população em sites oficiais desses órgãos na internet.

1.2.3 Marco Civil da Internet

A Lei 12.965, conhecida como Marco Civil da Internet, foi sancionada em 2014 após a publicação das ações de espionagem sofridas pela então presidente Dilma Rousseff pela Agência Nacional de Segurança dos EUA.

O Marco Civil da Internet disciplina os princípios, garantias, direitos e deveres para uso da internet no Brasil. Não é um documento normativo específico sobre privacidade e proteção de dados, mas tem muitos artigos que trata desses temas chegando a ser considerado uma das mais avançadas legislações sobre a internet do mundo.

Temas como privacidade e proteção dos dados são abordados nos capítulos I e II, sendo mais especificamente nos artigos 3º, 7º e 8º. O artigo 3º declara os princípios da proteção da privacidade e da proteção dos dados

pessoais para o uso da internet no Brasil, assim como a preservação e garantia da

neutralidade, da estabilidade, segurança e funcionalidade da rede, entre outros.

Em relação à privacidade e proteção de dados, destaca-se que o artigo 7º trata

não só da inviolabilidade da intimidade e da vida privada e do sigilo do fluxo de comunicações privadas que circulam pela internet, como também da proteção dos registros de conexão e acesso a aplicações de internet que devem estar descritas nos contratos de prestação de serviços.

Também determina a necessidade de esclarecer ao usuário sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que não devem ser fornecidos a terceiros, exceto por meio de consentimento livre, expresso e informado em cláusula contratual destacada.

O artigo 8º finaliza o capítulo II, que trata dos direitos e garantias dos usuários, instituindo que “a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso.

1.2.4 Lei Geral de Proteção de Dados Pessoais

Essas Leis Setoriais de proteção de dados citadas anteriormente, não cobriam setores importantes da economia, e dentre aqueles cobertos, não havia uniformidade em seu regramento.

Em 2018, o Brasil estabeleceu sua Lei Geral de Proteção de Dados LGPD (Lei 13.709 de 2018). Essa Lei consolidou, em um mesmo instrumento normativo, as regras sobre proteção de informações pessoais, garantido aos cidadãos maior controle sobre suas informações pessoais e sobre a utilização, o armazenamento, a recuperação e transferência deles. Essa estratégia vai além

do consentimento do titular de dados, que autoriza o seu uso, mas tão importante quanto esse elemento é assegurar que o fluxo informacional atendas as suas legitimas expectativas.

Nossa Lei Geral de Proteção de Dados, LGPD (Lei nº 13.709 de 2018), foi inspirada pela General Data Protection Resolution (GPDR) [Regulamento Geral sobre Proteção de Dados] da União Europeia. Que por sua vez, também foi uma evolução de uma diretiva que já havia desde 1995, mas que não era suficiente para garantir a proteção de dados perante os Estados Membros da União Européia. O que levou a rever o sistema jurídico. No Velho Continente, eles veem a GPDR como o mais importante instrumento jurídico já elaborado para a privacidade de dados do cidadão da Comunidade Europeia em mais de duas décadas de ações legais nessa área.

Importante salientar, também, como influência para a promulgação da LGPD, a oportunidade de o Brasil entrar na Organização para a Cooperação e Desenvolvimento Econômico ou Econômico – OCDE, conhecida popularmente como grupo dos países ricos. Tal organização, já em meados dos anos de 1980, possuía orientações acerca da transferência internacional de dados pessoais, bem como de seu uso adequado. Para que uma nação faça parte deste grupo, é necessária uma adequação que inclui dar sua palavra de que seguirá as diretrizes por ela propostas. Assim, na conjetura do Brasil não possuir uma legislação específica no que tange à questão da proteção de dados, dificultaria a entrada deste na referida organização.

.A LGPD foi criada com a finalidade de aumentar o controle sobre os dados pessoais. Logo, conta com normas que asseguram os direitos e autonomia dos titulares, e evitam o uso inadequado das suas informações. É uma lei abrangente. Elaborada para fazer frente ao desafio de proteger dados pessoais na era digital, esta nova regulamentação apresenta grande impacto na forma como as empresas e Estados operam. Afeta a tudo e a todos. Tem que ser obrigatoriamente cumprida por quem trate dados pessoais. Essencialmente é uma lei de controle, de conformidade.

CAPITOLO II

2.ESTRUTURA E ELEMENTOS DA LGPD

Entre os principais objetivos da LGPD estão:

proteção à privacidade — garantir o direito da privacidade e proteger os dados pessoais das pessoas com a implementação de práticas consideradas mais seguras;

transparência — propor regras claras sobre como os dados são coletados e tratados;

desenvolvimento — estimular o crescimento tecnológico e financeiro das empresas;

padronização das normas — criar regras únicas sobre como o tratamento de dados deve ocorrer, incluindo as responsabilidades dos agentes e controladores envolvidos na atividade;

segurança jurídica — aumentar a credibilidade das relações jurídicas e confiabilidade dos titulares dos dados quanto às instituições, o que contribui para fomentar a livre iniciativa;

concorrência — incentivar a concorrência e liberdade econômica com base na portabilidade de dados.

O tema proteção de dados pessoais, na LGPD, tem como fundamentos (art. 2º, LGPD):

- respeito à privacidade, ao assegurar os direitos fundamentais de inviolabilidade da intimidade, da honra, da imagem e da vida privada;
- a autodeterminação informativa, ao expressar o direito do cidadão ao controle, e assim, à proteção de seus dados pessoais e íntimos;
- a liberdade de expressão, de informação, de comunicação e de opinião, que são direitos previstos na Constituição brasileira;
- desenvolvimento econômico e tecnológico e a inovação, a partir da criação de um cenário de segurança jurídica em todo o país;
- a livre iniciativa, a livre concorrência e a defesa do consumidor, por meio de regras claras e válidas para todo o setor privado; e
- os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas

Os seguintes princípios (art. 6º, LGPD) devem ser observados na hora de tratar dados pessoais:

Finalidade- Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Adequação - Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Necessidade- Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Livre acesso - Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Qualidade dos dados - Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento

Transparência - Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

Segurança - Utilização de medidas 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 difusão

Prevenção - . Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Não discriminação - - Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos

Responsabilização e prestação de contas - Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Logo tais divisões são necessárias para um bom funcionamento dos armazenamentos dos dados pessoais desta forma visando a adoção de medidas que coíbem o uso das informações de modo ilícito ou abusivo.

2.1 Dados pessoais

A LGPD divide os dados em 4 tipos: Dados pessoais; Dados pessoais sensíveis; Dados anonimizados e Dados pessoais provenientes de crianças e adolescentes.

Dados pessoais: Entende-se como dados pessoais toda informação que está atrelada a uma pessoa natural, identificável ou identificada, de direito público ou privado, inclusive pessoas de outras nacionalidades. Esse é um ponto que precisa ser destacado devido a quantidade de empresas que lidam com dados de consumidores e organizações parceiras devido ao número quantitativamente alto de consumo de serviços e bens materiais que nem sempre são adquiridos em territórios brasileiros.

Os dados que possam identificar pessoas jurídicas, por sua vez, não estão cobertos pelo conceito explícito de dado pessoal presente na LGPD. O art. 5º, inc. I, da LGPD é claro quanto a isso ao definir dado pessoal como "informação relacionada a pessoa natural identificada ou identificável".

Dados pessoais sensíveis: são os dados pessoais que tratam de características subjetivas e muito particulares do indivíduo.

Quanto a isso, o art. 5º, II, da LGPD indica que os dados pessoais sensíveis são aqueles relativos a: Origem racial ou étnica; Convicção religiosa; Opinião política; Filiação a sindicato ou a organização de caráter religioso, filosófico ou político; Dado referente à saúde ou à vida sexual; Dado genético ou biométrico, quando vinculado a uma pessoa natural.

Dados anonimizados: são aqueles dados que, embora sejam de pessoa natural, não tornam possível a identificação da mesma (a titular).

Quanto aos dados anonimizados, a LGDP define que:

"Art. 5º, III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;"

Dados pessoais provenientes de crianças e adolescentes :esses dados possuem tratamento especial, em virtude da condição jurídica das mesmas no ordenamento brasileiro.

Eles devem sempre atender o melhor interesse da criança e devem ser obtidos mediante consentimento específico dos responsáveis.

2.2 Tratamento de dados pessoais:

O tratamento de dados é toda operação realizada com dados pessoais.

O art. 5, V, faz essa elucidação e exemplifica quais são os principais tipos de operações de dados pessoais.

Entre esses exemplos estão a coleta, produção, reprodução, transmissão, avaliação, modificação e arquivamento dos dados.

O art. 14 da LGPD informa que:

> "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.
> § 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."

Em seu teor, a LGPD inclui a existência de quatro sujeitos distintos e diretamente vinculados aos seus dados pessoais:

> **A)Titular**: pessoa física que forneceu, expressamente, os dados a determinada empresa;
>
> B)**Controlador:** pessoa, física ou jurídica, de direito público ou privado, que detém o poder de decidir sobre como os dados pessoais serão tratados e para quais finalidades eles serão direcionados no processo interno da empresa;
>
> C) **Operado**r: pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados de acordo com as orientações dadas pelo controlador – ou seja, o operador atua ela opera o tratamento dos dados.
>
> **D)Encarregado:** pessoa física indicada pelo controlador e pelo operador para atuar como elo entre o titular dos dados e a Autoridade Nacional de Proteção de Dados.

A organização dês do titular dos dados até o encarregado pessoa que vai operar e conduzir os dados, tem como objetivo de cuidar e proteger os dados mantendo assim uma maior rigidez no saneamentos de cada etapa

2.3 Titular de dados: - pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Somos todos nós, cidadãos, pessoa natural a quem se refere as informações fornecidas a uma empresa a fim de fazer parte da base de dados dessa organização, com uma finalidade específica

Um dos objetivos da LGPD é dar mais controle ao titular, sobre como os seus dados são utilizados. Por isso, a lei prevê também uma série de direitos ao titular.

Diante disso, o Art. 18, da LGPD, traz a ratificação com maior amplitude dos direitos dos titulares dos dados pessoais que devem ser garantidos de forma acessível e eficaz, como:

> 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.

Temos agora o direito à autodeterminação informativa. Um direito constitucional que se materializa com o que a LGPD prevê.

As organizações deverão respeitar e se adequar a essas exigências da legislação, a fim de evitar penalizações.

Além disso, o próprio indivíduo passa a ter o direito de pedir determinadas informações por parte do controlador (a empresa que usa e armazena os dados do cliente). A qualquer momento, ele pode solicitar o acesso, a correção, a anonimização, a eliminação ou a portabilidade dos dados dele, entre outros pontos.

O titular de dados também pode solicitar que a instituição controladora dos seus dados revogue o consentimento do uso dos seus dados, como também a correção de dados errados e que a empresa utilize apenas para a finalidade para a qual foram coletados.

É perceptível a vulnerabilidade dos cidadãos em exercer o controle dos seus dados pessoais, desde a captura das suas informações como também a forma de utilização deles. Por isso, é necessário que a empresa utilize as informações de forma segura evitando falhas, vazamentos, se precavendo quanto a riscos da melhor maneira que a situação exigir.

Sendo assim, a empresa deve estar pronta para fornecer essas informações sempre que forem solicitadas.

2.4 Consentimento

O consentimento para o tratamento dos dados pessoais é um dos pontos principais da LGPD. Está previsto no art. 5, XII, da Lei, que indica que o consentimento é a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;”

A partir dele, o indivíduo indica, expressamente, se os seus dados podem ser tratados pela pessoa física ou jurídica que está coletando.

A única exceção para o consentimento é referente aos dados manifestamente públicos do indivíduo. “Art.7 § 4º É dispensada a exigência do

consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.”

Fora essa exceção, o consentimento precisa ser requisitado para a maior parte dos casos em que é realizado o tratamento de dados.

Apesar da requisição do consentimento ser uma prática utilizada há bastante tempo pelos sites e plataformas digitais. No entanto, com a LGPD, o consentimento precisa de uma atenção ainda maior por parte das pessoas físicas ou jurídicas e dos responsáveis que forem realizar o tratamento dos dados.

Ele precisa ser claro e atender às finalidades específicas expressas no momento da requisição, informar também em relação ao ciclo de vida dos dados do usuário. O ciclo de vida dos dados do usuário nada mais é do que a definição clara de como os dados são coletados, armazenados e excluídos pela pessoa jurídica ou física que realiza o tratamento. Esse processo precisa ser descrito de forma clara aos usuários, a fim de que seja possível avaliar como os dados são tratados.

Ao ser demonstrado, devem ser expostas, também, todas as medidas técnicas tomadas para a proteção e segurança dos dados durante a coleta**,** o armazenamento e a exclusão dos mesmos.

Nesse sentido, de acordo com o art. 6, inc. VII, da LGPD, a segurança dos dados é definida como “utilização de medidas 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 difusão”

2.5 Agentes de tratamento

Controlador - é a própria Empresa que exigirá das pessoas físicas e das pessoas jurídicas, de Direito Público ou Privado, com quem se relaciona, o cumprimento dessa política quando aquelas estiverem tratando dados pessoais.

Operador- pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Ao tratar de medidas técnicas para proteção dos dados, a Lei Geral de Proteção de Dados é clara nos termos do seu artigo 46, no qual informa que os responsáveis pelo tratamento das informações pessoais devem adotar medidas de segurança, técnicas e administrativas, a fim de proteger os dados pessoais de acessos não autorizados e de situações geradas por incidentes de segurança de forma acidentais ou ilícitas que acarrete destruição, perda, alteração, comunicação ou de qualquer forma que venha oferecer tratamento inadequado ou ilícito.

O artigo 5º, IX, cita que são considerados agentes de tratamento o controlador e o operador. Destaque-se que o mesmo artigo elucida que são esses sujeitos: sendo o controlador uma pessoa, podendo ser natural ou jurídica, bem como de direito público ou privado. Em verdade, o controlador é o responsável direto, é o sujeito que indica quais dados serão captados, tratados e desenvolvidos, razão pela qual possui maior responsabilidade e autonomia, devendo cumprir todas as obrigações legais e os deveres anexos.

O operador, por outro lado, é o "técnico" que realiza a operação propriamente dita. Pode ser pessoa física ou jurídica, de direito privado ou público. A responsabilidade do operador, em regra, é mais branda que a do controlador.

2.5.1 Sanções administrativas

É essencial mencionar as sanções administrativas trazidas pela nova lei, com aplicação àqueles chamados agentes que fazem o tratamento de dados. Caso estes violem alguma norma preconizada na legislação, terão como responsabilidade o que diz o artigo 52:

> 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" (BRASIL, LGPD, 2022).

Desta forma a Lei 13.709/18 traz uma segurança maior parao titular dos dados, responsabilizando as empresas que estão com o controle dos mesmos, utilizando multas e advertências mais severas.

2.6 Encarregado sobre a Proteção de Dados

Dentre as novas obrigações da LGPD, está a nomeação de um Encarregado da Proteção de Dados, que também é conhecido por **Data Protection Officer -DPO.** Ele possui a função de atuar como canal de comunicação entre instituição, titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

> Suas atribuições, conforme o Artigo 41, da LGPD são:
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

O DPO ou Encarregado vai ser a comunicação entre a entidade, a LGPD e o titular. Além disso, terá a função de aceitar as requisições dos titulares, responder à ANPD, orientar os servidores. Porém, o cargo não precisa ser de apenas uma pessoa. A instituição pode formar um comitê multidisciplinar e distribuir essas funções do DPO entre os integrantes.

Independentemente do tamanho da empresa, desde uma micro empresa a uma multinacional, a presença de um DPO traz uma segurança maior e evita que pessoas da organização que não possuam tanto conhecimento sobre a lei, recebam uma demanda que não possuem o costume e a cultura da proteção e segurança dos dados.

A presença de um DPO, ou encarregado de dados, foi um dos feitos de maior alteração quando falamos da Lei. Nos últimos quatro anos a profissão foi popularizada a ponto de ser oficialmente reconhecida pelo Ministério do Trabalho.

O feito evidencia a importância de existir um especialista, ou ainda um time inteiro, da área para cuidar dos assuntos relacionados com a legislação e a manutenção da mesma nos negócios.

2.7 Autoridade Nacional de Proteção de Dados – ANPD

É importante salientar, que não basta ter uma lei de proteção de dados. É preciso entender, interpretar. É preciso educar, capacitar. Por isso, apesar de no centro de todo o sistema da proteção de dados estar o titular, é relevante o papel orientativo da Autoridade Nacional da Proteção de Dados, a ANPD,

De início, ao ser sancionado pela Presidência da República, alguns artigos da lei de proteção de dados proposta originalmente foram vetados, o que a descaracterizou e gerou discussões.

Uma das questões mais debatidas foi sobre o veto sobre a criação da Autoridade Nacional de Proteção de Dados (ANPD), vinculada ao Ministério da

Justiça, e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

Esses órgãos seriam reguladores e deveriam zelar e fiscalizar a proteção dos dados pessoais, aplicando sanções em caso de tratamento de dados realizado em descumprimento à legislação, além de propor diretrizes para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade.

Antes mesmo da promulgação da lei, indicaram que a não criação de uma autoridade independente para fiscalizar a aplicação da lei traria problemas para o país de adequação em relação ao GDPR, para atrair investimentos internacionais, como também criar um entrave nas relações comerciais.

Visando corrigir esse ponto polêmico, em 2019 o Senado aprovou a medida provisória n. 869/2018 que trouxe algumas alterações à LGPD, sendo a principal delas a reinserção da criação da Autoridade Nacional de Proteção de Dados (ANPD).

No mesmo ano, a Lei Federal n. 13.853 instituiu a ANPD; a obrigação do encarregado, também conhecido como Data Protection Officer (DPO), ter conhecimento jurídico regulatório na matéria; a possibilidade de proibição das atividades de tratamento de dados para entidades infratoras; a flexibilização no compartilhamento de dados de saúde e dados pessoais publicamente acessíveis, dentre outras.

A ANPD tem o papel de atuar junto à sociedade e as instituições, trazendo mais segurança e estabilidade para a aplicação da Lei Geral de Proteção de Dados. (PATRICIA PECK, 2020, p. 49), ao abordar o tema, esclarece que:

> A ANPD tem um papel fundamental como elo entre diversas partes interessadas que vão do titular ao ente e ao ente público, passando pela necessidade alinhamento com demais autoridades reguladoras e fiscalizadoras, bem como os três poderes Executivo, Legislativo e Judiciário que deverão continuar a compreender a temática da dinâmica dos dados pessoais em um contexto não apenas nacional mas principalmente

> internacional para que o Brasil saiba se posicionar no mercado digital global

Tem sido notada com grande relevância a atuação das Autoridades de Proteção de Dados, principalmente, no que se refere às tomadas de decisões, aplicação de sanções e multas proporcionalmente consideradas consoante os poderes que lhe são atribuídos.

Tendo em vista que os dados são necessários à economia digital e incremento à inovação, reforça a importância da ANPD e sua atuação de modo a garantir padrões de conduta que agregam confiança e cuidado no uso dos dados, de forma a garantir a segurança no compartilhamento de dados.

De acordo com Cintia Lima (2021, p.125):

> O desafio em se estabelecer limites às atividades das empresas, nesses mercados de tecnologia para a coleta, uso e tratamento de dados, é evidente, exatamente porque confronta interesses heterogêneos e impõe, na maior parte das vezes, que se opte pela prevalência de um ou de outro. No entanto, reconhecer como objetivo da LGPD o tratamento do poder econômico e a regulação da atividade das empresas de tecnologia constitui o início de um percurso inevitável. Do mesmo modo, a análise dos dados e informações como um ativo da empresa, em especial, sua base de dados, deve ser não apenas reconhecido pelo sistema de proteção de dados, como também levado em conta na aplicação de todo o Direito Comercial.

Logo o desafio da implementação da LGPD, visto o constante crescimento das tecnologias , fazendo com que os órgãos reguladores estejam sempre se atualizando a aplicação da Lei.

CAPITOLO III

3. A LGPD E OS DESAFIOS DE SUA IMPLEMENTAÇÃO

A Lei Geral de Proteção de Dados traz diversos novos desafios e cuidados para o dia a dia das empresas. A Lei provocou mudanças em instituições de diferentes portes, levando-as a realizar alterações no sistema interno e a ter mais cautela com as novas informações pessoais coletadas.

Mesmo depois da implementação da LGPD muitas empresas dos mais variados segmentos apontam ainda estarem passando por um momento confuso quanto às práticas e cumprimento da Lei.

Analisando o levantamento com as questões da pesquisa, além das respostas mais detalhadas, fica claro que o tratamento de dados baseado no que a LGPD requisita ainda tem um longo caminho para se estabelecer. Fica entendido também que é preciso mais clareza por parte dos órgãos responsáveis; assim, as empresas e os próprios profissionais conseguirão estar mais preparados, fazendo com que a LGPD beneficie toda a sociedade.

Apesar dessa pesquisa já ter algum tempo de realizada, atualmente a situação não se encontra muto diferente. O processo de adaptação é repleto de desafios. Envolve novas demandas, cuidados e tecnologias que devem ser implementadas, fazer um planejamento de adequação da lei, treinamento de pessoal, tratar as informações fazendo uso do consentimento e com transparência, fortalecimento do sistema de segurança, criação de canais de atendimento ao titular de dados. Tudo isso tem um custo alto para muitas empresas.

Como fica claro diante dos desafios apresentados até agora, seguir devidamente a LGPD e preparar a empresa para as demandas da Lei exige a implementação de diversos novos processos e procedimentos dentro da empresa.

Esses esforços serão diários e devem alcançar cada colaborador, e não apenas aqueles diretamente envolvidos com a segurança de dados. Mesmo quem não vai atuar com os processos da Lei deve entender seus pontos principais.

Nesse sentido, o artigo 49 da LGPD recomenda a implementação de um programa de governança em privacidade. Ele deve demonstrar o comprometimento da empresa na adoção de processos e políticas internas assegurando o cumprimento da Lei.

A Lei destaca ainda que o programa deve ser “aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta” e “adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados”, entre outros pontos.

Para estar de acordo com a LGPD será necessária não só a reorganização da empresa e a adoção do tratamento dos dados existentes, mas uma revisão de contratos com fornecedores e parceiros. Estes também terão que estar adaptados à nova legislação para evitar problemas com a Justiça. “Não adianta a empresa estar de acordo com a lei se os parceiros não estiverem. Se houver qualquer incidente de vazamento de dados por esses parceiros, a empresa responde solidariamente.

Não investir em Segurança da Informação é um erro que pode custar caro. O desafio é identificar e implantar medidas que sejam coerentes com as necessidades do negócio.

A Segurança da Informação é um dos princípios da LGPD e, assim, é um requisito para estar em conformidade com a lei.

3.1 Adequação à LGPD é um desafio continuo

Em determinadas situações, as organizações, após implementarem a LGPD, acabam afrouxando seus controles ou, em muitos casos, passam a ignorá-los. Como a atualização contínua é uma determinação legal (art. 50, §2º, I, h, da LGPD), essa atitude acaba por deixar as empresas em desacordo com a legislação, o que pode ter graves consequências, como multas ou outras penalidades.

No art. 50, §1º, a LGPD deixa claro que a ANPD pode reduzir o peso das sanções levando em conta, entre outros critérios, a adoção reiterada de

mecanismos para minimização do dano e voltados para o tratamento seguro de dados, a adoção de boas práticas e governança e a pronta adoção de medidas corretivas. Como a lei traz o princípio da responsabilização e prestação de conta (art. 6º, X, LGPD), é possível que os parâmetros para multas administrativas também venham a ser usados em demandas judiciais.

A conformidade contínua com a LGPD é de suma importância também por diversas outras razões, como o ingresso de novos funcionários na empresa, mudança de atividades ou processos desenvolvidos pela organização, o que leva a atualização do tratamento de dados, como também na mudança de riscos ao longo do tempo, especialmente em contextos dinâmicos, no campo da tecnologia e da inovação, é necessário revisar análise e gestão de riscos de forma periódica, a fim de não ser surpreendido com violações de dados pessoais por causa de programas de privacidade desatualizados.

CONSIDERAÇÕES FINAIS

É de grande relevância para o cidadão, estar atento às informações prestadas pela instituição que trata os seus dados, como também ter ciência dos seus direitos e de que é garantido ao titular dos dados a consulta gratuita sobre a forma e a duração do tratamento, bem como sobre a integridade de seus dados pessoais.

Tanto as empresas, como as entidades, do setor público ou privado, têm que se adequar às normas da LGPD. Implementar uma estrutura e uma política interna de *complice* para fazer o tratamento adequado os dados dos seus clientes.

Por parte das organizações, dar o passo inicial para a implementação desta lei é essencial, e é possível ter um resultado satisfatório, profissional, responsável, buscando estar em conformidade com a lei e gerando muito valor para a empresa.

Nesta monografia foi analisado que a LGPD é para o cidadão ter um controle sobre suas próprias informações, para as empresas, os órgãos públicos, controle a oferecer em resposta as constantes evoluções das novas tecnologias.

Isso tudo tem consequências positivas. E quem ganha com isso é a sociedade. Se hoje, o maior ativo da sociedade mundial é a informação, um controle sobre esse ativo tem que ser compatível proporcionalmente com o valor desse tipo de propriedade.

Torna-se relevante destacar a importância da LGPD para proteger a privacidade dos indivíduos. Assim, a atuação do Poder Legislativo visando regular a questão concernente a proteção de dados demonstra a atuação estatal voltada a garantir aos cidadão a liberdade em um Estado Democrático de Direito.

Todavia, diante da análise realizada os desafios na implementação da LGPD entre as diferentes realidades brasileiras são constantes e precisamos ainda preencher algumas lacunas na legislação. Ainda há muito que se discutir sobre essa Lei. Mas vale ressaltar que a intenção da LGPD não é atrasar ou complicar procedimentos e processos que já estão na rotina das empresas, mas, sim, tornar o ambiente mais seguro e referência dentro da proteção de dados. Para assegurar a conformidade com a lei, portanto, não basta a criação de um programa de conformidade com a lei, a implementação de algumas medidas e, depois, esquecer o assunto. É preciso atenção constante para o avanço contínuo das práticas de compliance com a LGPD.

REFERÊNCIAS

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento – 3. ed. – Rio de Janeiro: Forense, 2021.

PECK, Patrícia. **Proteção de dados pessoais**.2. ed. São Paulo: Editora Saraiva, 2020.

RODOTÁ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

LIMA, Cíntia Rosa Pereira D. ANPD e LGPD: Desafios e perspectivas. [Digite o Local da Editora]: Grupo Almedina (Portugal), 2021. E-book. ISBN 9786556272764. Disponível em: https://unibb.minhabiblioteca.com.br/#/books/9786556272764/. Acesso em: 20 set. 2022.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. Segurança de Redes em Ambientes Corporativos.São Paulo: Novatec Editora, 2007.

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm acesso em 29/05/2022

https://www.neoenergia.com/pt-br/te-interessa/tecnologia/Paginas/lei-geral-protecao-dados-lgpd.aspx acesso em 05/06/2022

https://www.bb.com.br/pbb/pagina-inicial/minha-privacidade/politicas-de-uso-e-privacidade#/acesso em 05/06/2022

https://www.gov.br/iti/pt-br/acesso-a-informacao/encarregado-pelo-tratamento-de-dados-pessoais acesso em 05/06/2022

https://www.pmgacademy.com/blog/noticias/pesquisa-as-empresas-estao-se-adaptando-a-lgpd/acesso em 22/09/2022

https://periodicos.fapam.edu.br/index.php/RPE/article/view/391/249 acesso em 25/09/2022

https://ouvidoresemacao.com.br/2021/08/13/lgpd-3-anos-e-muitos-desafios-de-implementacao/acesso em 25/09/2022

https://www.lgpdbrasil.com.br/4-anos-de-lgpd-o-que-mudou-desde-a-publicacao-da-lei/acesso em 06/10/2022

https://www.lgpdbrasil.com.br/como-alinhar-privacidade-e-seguranca-dos-dados-as-estrategias-esg/acesso em 06/10/2022