CENTRO UNIVERSITÁRIO
ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

LIMITES E RESPONSABILIDADES DAS EMPRESAS PELA COLETA, UTILIZAÇÃO E VENDA DOS DADOS PESSOAIS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS

Alex Remor Alves

Presidente Prudente/SP
2021

CENTRO UNIVERSITÁRIO
ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

LIMITES E RESPONSABILIDADES DAS EMPRESAS PELA COLETA, UTILIZAÇÃO E VENDA DOS DADOS PESSOAIS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS

Alex Remor Alves

Monografia apresentada como requisito parcial de conclusão do curso e obtenção do grau de Bacharel em Direito, sob a orientação do Prof. Wilton Boigues Corbalan Tebar.

Presidente Prudente/SP
2021

LIMITES E RESPONSABILIDADES DAS EMPRESAS PELA COLETA, UTILIZAÇÃO E VENDA DOS DADOS PESSOAIS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS

Monografia apresentada como requisito parcial para obtenção do grau de Bacharel em Direito.

Wilton Boigues Corbalan Tebar
Orientador

Lucas Pires Maciel
Examinador 1

Guilherme Prado Bohac de Haro
Examinador 2

Presidente Prudente, _____.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por ter confiado a mim o dom da vida e ter me proporcionado saúde, força e coragem para conquistar minhas metas, além de me orientar nos momentos difíceis pelos quais passei.

Agradeço imensamente aos meus pais, Anfilóquio e Mônica, que batalharam arduamente para dar a mim e aos meus irmãos todas as ferramentas, ensinamentos e oportunidades necessárias para alcançarmos tudo aquilo que desejamos para nossas vidas.

Reforço os agradecimentos a minha mãe, pois ela foi quem mostrou a mim a importância do estudo e acreditou em meu potencial, investindo sempre nas melhores escolas, nos melhores cursos e livros para o meu aprendizado.

Sou grato à faculdade, por sua excelência e interesse nos alunos, e por oferecer um corpo docente extremamente qualificado e uma estrutura magnífica para atender as necessidades dos estudantes.

Ao meu orientador Wilton Boigues Corbalan Tebar, que demonstrou ser mais que um professor, mas um amigo, que me incentivou a estudar, e me auxiliou na produção deste trabalho.

Aos demais parentes e amigos que estiveram comigo durante esta jornada, me apoiando e me dando forças para seguir em frente.

RESUMO

O presente trabalho visa realizar um estudo acerca da Lei Geral de Proteção de Dados, abordando os principais temas dessa legislação e explicando de maneira didática qual o seu intuito e suas consequências na sociedade atual. Para que esse objetivo seja alcançado, serão abordados temas como o panorama histórico-evolutivo da proteção de dados, os conceitos que essa lei traz em seu corpo, a importância dos dados na atualidade, quais os tipos de dados e como eles são coletados, assim como os requisitos para o tratamento de dados se efetuar, os direitos e garantias dos titulares de dados e quem são os responsáveis pela fiscalização e aplicação das sanções previstas na LGPD. O método científico utilizado será o método dedutivo, utilizando-se de estudos históricos, artigos científicos, jurisprudência, legislações, doutrinas e outros meios de informação para elaborar as conclusões do trabalho.

Palavras-chave: Armazenamento de Dados. Autoridade Nacional de Proteção de Dados. Coleta de Dados. Lei Geral de Proteção de Dados. Tratamento de Dados.

ABSTRACT

The present work aims to carry out a study about the General Data Protection Law, approaching the main themes of this legislation and explaining in a didactic way what its purpose and its consequences in today's society. In order to achieve this goal, topics such as the historical-evolutionary panorama of data protection, the concepts that this law brings in its body, the importance of data today, what types of data and how they are collected, will be addressed. how the requirements for the processing of data to be carried out, the rights and guarantees of the data subjects and who is responsible for the inspection and application of the sanctions foreseen in the LGPD. The scientific method used will be the deductive method, using historical studies, scientific articles, jurisprudence, legislation, doctrines and other means of information to draw up the conclusions of the work.

Keywords: Data collect. Data Processing. Data Storage. General Data Protection Law. National Data Protection Authority.

SUMÁRIO

1 INTRODUÇÃO

Com o avanço tecnológico que se desenvolveu de maneira exponencial nos últimos anos, o mundo digital tem se tornado cada vez mais presente no cotidiano humano. Apresentando inúmeras oportunidades em diversas áreas como no comércio, relações sociais e saúde, a internet proporcionou de maneira significativa um encurtamento das distâncias e diminuição das barreiras que bloqueavam o avanço nos empreendimentos desenvolvidos pela raça humana, facilitando os estudos para realização de novas descobertas que tornam a vida na terra mais confortável e com uma qualidade de vida maior.

Sendo assim, esse mundo digital acessado através da internet, que antes carregava consigo a fama de ser uma “terra sem lei”, se tornou objeto de estudo do ponto de vista jurídico, uma vez que, tornou-se impossível continuar ignorando a sua existência em virtude de sua popularização e democratização do seu acesso.

Estudos realizados pelo Instituto Brasileiro de Geografia e Estatística (IBGE), em 2019, apontam que 82,7% dos domicílios nacionais possuem acesso à internet e, em média, o brasileiro gasta 5.4 horas por dia em aplicativos, de acordo com um estudo realizado pela agência App Annie e divulgado pela Forbes.

Nesse sentido, países do mundo inteiro se viram obrigados a criar legislações que regulamentem o acesso, permanência e os atos praticados através dos ambientes virtuais, visando a segurança e o bem estar social de suas nações.

No Brasil a legislação criada no dia 14 de agosto de 2018, e que passou a vigorar no dia 18 de setembro de 2020, chamada Lei Geral de Proteção de Dados é a responsável por regular as atividades de tratamento de dados pessoais. Em virtude de sua recente entrada em vigor e de sua complexidade intrínseca, a LGPD causou inúmeras repercussões no meio jurídico, digital e social, gerando uma série de dúvidas sobre o que ela é, qual seu objetivo e como se dará sua aplicação, o que a torna um excelente objeto de estudo e discussão para elucidar as dúvidas que permeiam sobre essa lei e tentar aprimorá-la o máximo possível, para que sua finalidade primordial seja de fato alcançada.

Diante todo o exposto, o presente trabalho visou, de maneira clara e objetiva, apresentar a origem e o panorama evolutivo da Lei 13.709/18, assim como as fontes materiais e formais que serviram de inspiração para sua criação, além da

importância dos dados pessoais na atualidade e os impactos causados pela sua utilização.

Em seguida, foi realizado um estudo sistemático sobre a composição da Lei Geral de Proteção de Dados, abordando seus conceitos e terminologias, sua função e aplicação, e os agentes responsáveis pela guarda, utilização e da fiscalização do tratamento de dados.

Por fim, uma breve análise acerca dos tipos de dados pessoais que serão coletados e armazenados, como são coletados esses dados, os direitos conferidos aos titulares pela LGPD, como será feito o armazenamento e quais medidas de proteção deverão ser adotadas pelos agentes de tratamento, bem como a responsabilização daqueles que não estiverem em conformidade com a Lei Geral de Proteção de Dados.

Ademais, com o objetivo de elucidar as problemáticas expostas, utilizou-se o método científico dedutivo, por meio do qual serão coletadas premissas gerais através de doutrinas, notícias, artigos científicos, legislações e outros meios de informação para produção do presente trabalho monográfico.

Insta salientar que, por ser uma novidade legislativa e por ser um tema que está em constante desenvolvimento e mutação, não foi possível o esgotamento de maneira completa e definitiva da presente investigação científica.

2 PANORAMA EVOLUTIVO DA PROTEÇÃO DE DADOS

Inicialmente, faz-se necessário realizar um estudo acerca do surgimento da Lei Geral de Proteção de Dados, de modo a apresentar quais legislações influenciaram mais fortemente em sua criação, traçando paralelos entre tais legislações e a LGPD a fim de identificar semelhanças e diferenças que contribuíram para sua formação.

Assim como expor a importância dos dados pessoais na sociedade contemporânea e quais impactos têm sido causados pelo seu uso.

2.1 Apontamentos Históricos Relevantes

Desde os primórdios, os litígios que aconteciam no plano fático serviam de inspiração para a criação de regras de conduta social, princípios e leis, sejam elas positivadas ou não. Elas eram criadas a fim de evitar que problemas passados tornassem a ocorrer e, caso ocorressem, já houvesse uma solução prévia para esse mesmo conflito ou outro que fosse semelhante, na tentativa de tornar a convivência na sociedade a mais harmoniosa e segura possível.

Esse paradigma se repete na criação da Lei Geral de Proteção de Dados, ou seja, os acontecimentos que antecederam essa lei serviram de inspiração para a sua criação de maneira a torna-la a mais assertiva, protética e eficaz possível. Portanto, para melhor compreensão desse estudo, faz-se necessário de antemão, apresentar um panorama geral histórico-evolutivo dos fatos importantes que contribuíram para formação da atual Lei Geral de Proteção de Dados, além de discutir qual a importância e os impactos socioculturais que essa prática tem causado.

2.1.1 Direito à privacidade (1890)

O mais antigo alicerce relacionado a proteção de dados é o Direito a privacidade. Ele surgiu inicialmente nos Estados Unidos da América e ganhou relevância a partir de um artigo publicado na revista Harvard Law Review, em 15 de dezembro de 1890, escrito pelo advogado Samuel D. Warren e Louis D. Brandeis (1890, p. 03), intitulado “The Right of Privacy”. Nesse artigo os autores discutiam

sobre o advento das novas tecnologias como a máquina fotográfica e dos jornais que invadiam a e expunham a vida privada das pessoas:

> [1]"instantaneous photographs and news paper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops"

Interessante salientar que os motivos que fizeram emergir a discussão sobre privacidade em 1890, são basicamente os mesmos motivos que serviram para criação das atuais leis que visam proteger dados, ou seja, o descontentamento com os veículos de informação e entidades que coletam, armazenam e veiculam informações pessoais, usufruindo delas para seu benefício próprio, sem consentimento dos usuários.

No Brasil, o direito à privacidade encontra-se na Constituição Federal de 88, no seu artigo 5º inciso X, apontando que "X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (Brasil, 1988). É também mencionado na LGPD em seu 2º artigo, inciso I, dizendo que "A disciplina da proteção de dados pessoais tem como fundamento : I – o respeito à privacidade" (Brasil, 2018).

Para se ter uma noção mais precisa é importante conceituar o que seria a privacidade. Nas palavras de Celso Bastos, privacidade seria:

> faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano (1989, p. 63)

Dessa maneira, é possível entender que o direito à privacidade está intimamente ligado com o intuito da LGPD em proteger os dados pessoais, uma vez que, esse direito vem atuar no sentido de proteger o cidadão de quaisquer violações pertinentes à sua privacidade como um todo, seja no meio digital ou não, estabelecendo limites para a interferência do Estado e de terceiros na vida cotidiana.

---

[1] fotografias instantâneas e empresas de jornal invadiram os recintos sagrados da vida privada e doméstica; e inúmeros dispositivos mecânicos ameaçam cumprir a previsão de que "o que é sussurrado no armário será proclamado dos telhados das casas".

2.1.2 Hessisches Datenschutzgesetz (Ato de Proteção de Dados de Hesse) (1978)

A Lei de Proteção de Dados de Hesse, também conhecido pela sigla HDSG, entrou em vigor em 1970. Foi a primeira lei a abordar o assunto de proteção de dados, ainda que de forma genérica, sendo aplicada somente ao Estado de Hesse.

Ela é responsável por regular quando e como o governo de Hesse poderia realizar o tratamento de dados e seu principal objetivo era assegurar o direito do indivíduo de se proteger sobre a divulgação e o uso de seus dados de forma ilegal.

No §2º da lei estão algumas definições que são de suma importância para sua compreensão, ainda mais por se tratar da primeira lei de proteção de dados onde o conhecimento acerca do tema não era amplo e divulgado.

Entre as definições expostas estão as de: “1) dados pessoais são detalhes individuais sobre circunstancias pessoais e factuais de uma pessoa física específica ou identificável (titular dos dados); 2) Processamento de dados é qualquer uso de armazenamento ou pretensão de armazenar de dados pessoais; 3) Coleta é a aquisição de dados sobre o titular dos dados; 4) Destinatário é qualquer pessoa ou organismo que recebe os dados; 5) terceiro é qualquer pessoa ou organismo externo ao organismo de processamento de dados, com exceção de pessoas afetadas; 6) arquivo é qualquer documento usado para realizar uma tarefa que não faz parte do sistema automatizado”. É comum que as legislações sobre proteção de dados definam conceitos e expressões técnicas utilizadas por elas (Alemanha, Hesse, 1970).

Outra semelhança com a LGPD encontra-se no §4º que informa que o contratante só pode usar os dados pessoais para alcançar a finalidade do processamento estabelecida, devendo informar o titular sobre essa finalidade e sobre eventuais violações sobre seus dados, além do nome e endereço do órgão de processamento, o tipo de dados armazenados, o grupo de pessoas afetadas, as medidas técnicas e organizacionais para o tratamento, o prazo para a finalização e exclusão dos dados e o resultado fundamentado da investigação.

Assim como a LGPD e outras legislações de tratamento de dados, alguns requisitos devem ser cumpridos para que essa operação seja realizada de maneira legal. No caso da HDSG, o processamento de dados só é permitido se: “1) uma disposição legal anterior a esta lei prevê isso ou o torna obrigatório; 2) essa lei permite isso; 3) a pessoa em causa consentiu sem qualquer dúvida, devendo o consentimento ser escrito, a menos que outro formulário seja necessário devido a circunstâncias especiais; 4) a pessoa em questão deve ser informada de maneira adequada; 5) no caso de transferências pretendidas, o dever de informar também inclui o destinatário dos dados; 6) as partes afetadas devem ser informadas, explicando as consequência legais, que recusam o seu consentimento e pode ser revogado a qualquer momento com efeito para o futuro.” (Alemanha, Hesse, 1970).

O HDSG também faz ressalvas sobre alguns tipos de dados como os de origem étnica, opiniões políticas, crenças religiosas ou filosóficas, a filiação a um sindicato ou para a saúde, que somente serão usados em casos específicos entre eles: para fins de pesquisa científica, quando são do interesse público na realização de projetos de pesquisa, quando é do interesse do empregador do titular para determinadas finalidades de acordo com a lei e para transmissão de dados a órgãos de sociedades religiosas de direito público, respeitando o procedimento legal.

Os direitos do titular dos dados e das pessoas afetadas pelo tratamento encontram-se no §8 da HDSG, e se assemelham com os direitos previstos pela Lei Geral de proteção de Dados. São eles: 1) direito à informação e notificação dos dados pessoais armazenados sobre ele; 2) revisão do processamento legal de seus dados com base em razões pessoais e especiais; 3) inspeção do diretório de procedimentos; 4) correção, bloqueio ou exclusão dos dados pessoais armazenados sobre ele; 5) indenização por dados e 6) recurso para o responsável pela proteção de dados. Em adição, o Ato de Proteção de Dados de Hesse proíbe o tratamento de dados para finalidades que não lhe foram destinadas.

Assim como a LGPD, o HDSG informa que a responsabilidade da segurança e tratamento dos dados pertence ao órgão transmissor que realiza o processamento desses dados, como está disposto no §14 da lei.

Por fim, analisando o Ato de Proteção de Dados de Hesse, é possível concluir que ele serviu de inspiração para o desenvolvimento de legislações subsequentes a essa, visto que, ele elenca algumas diretrizes que são reproduzidas em diversas outras leis, inclusive na Lei Geral de Proteção de Dados. Entre essas

diretrizes estão: a)definição de conceitos e nomenclatura utilizadas pela lei; b)necessidade do consentimento e da conscientização do titular acerca do tratamento de dados sobre como é realizado, origem dos dados, finalidade do tratamento e os tipos de dados armazenados; c) manutenção dos dados somente durante o período em que eles estiverem em tratamento, devendo ser realizado o descarte após esse período; d) direito a correção, modificação e exclusão de dados incorretos; e) limitação da finalidade do tratamento de dados, devendo ser utilizados somente para aquele fim; f) exigência de requisitos legais para a realização do tratamento. Fazendo parte das origens da Lei Geral de Proteção de Dados.

2.1.3 Código de Defesa do Consumidor (1993)

O Código de Defesa do Consumidor foi instituído pela Lei nº 8.078, em 11 de setembro de 1990 e entrando em vigor no dia 11 de março de 1991, conferindo ao ordenamento jurídico brasileiro uma política que visava regulamentar as relações de consumo.

As relações de consumo anteriores a essa lei eram reguladas pelo Código Civil vigente na época. Entretanto, devido as mudanças sociais e econômicas que ocorriam cada vez mais rápido e, por consequência, tonavam as relações de consumo mais complexas, foi necessária a criação de uma legislação mais apropriada, que pudesse atender essas necessidades específicas. Surge então, o Código de Defesa do Consumidor, que tem como principal objetivo a proteção do consumidor, que em regra é considerado como parte vulnerável, visando tornar a relação de consumo equilibrada entre o consumidor e o fornecedor de produto e/ou serviço. Outros objetivos e princípios estão elencados no artigo 4º do Código de Defesa do Consumidor, que dispõe:

> Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios: (Redação dada pela Lei nº 9.008, de 21.3.1995)
> I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo;
> II - ação governamental no sentido de proteger efetivamente o consumidor:
> a) por iniciativa direta;
> b) por incentivos à criação e desenvolvimento de associações representativas;

> c) pela presença do Estado no mercado de consumo;
> d) pela garantia dos produtos e serviços com padrões adequados de qualidade, segurança, durabilidade e desempenho.
> III - harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores;
> IV - educação e informação de fornecedores e consumidores, quanto aos seus direitos e deveres, com vistas à melhoria do mercado de consumo;
> V - incentivo à criação pelos fornecedores de meios eficientes de controle de qualidade e segurança de produtos e serviços, assim como de mecanismos alternativos de solução de conflitos de consumo;
> VI - coibição e repressão eficientes de todos os abusos praticados no mercado de consumo, inclusive a concorrência desleal e utilização indevida de inventos e criações industriais das marcas e nomes comerciais e signos distintivos, que possam causar prejuízos aos consumidores;
> VII - racionalização e melhoria dos serviços públicos;
> VIII - estudo constante das modificações do mercado de consumo.
> IX - fomento de ações direcionadas à educação financeira e ambiental dos consumidores; (Incluído pela Lei nº 14.181, de 2021)
> X - prevenção e tratamento do superendividamento como forma de evitar a exclusão social do consumidor. (Incluído pela Lei nº 14.181, de 2021)

A partir da leitura do artigo exposto acima, é possível notar fortes semelhanças entre a LGPD e o Código de Defesa do Consumidor, uma vez que, a LGPD também visa a proteção do usuário que possui seus dados coletados pelas empresas e sites de maneira indevida, sendo ele considerado vulnerável, além de incentivar e promover o acesso à informação dos direitos e deveres garantidos aos usuários e as empresas.

O segundo ponto em comum entre a LGPD e o Código de Defesa do Consumidor é em relação a privacidade de dados visto que no artigo 43 desse código está expresso o seguinte:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
> § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

> § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
> § 6º Todas as informações de que trata o **caput** deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (Incluído pela Lei nº 13.146, de 2015).

Observa-se extrema semelhança com o exposto no artigo 18 da LGPD que explana sobre a necessidade de notificação do titular sobre a existência do tratamento de dados, o acesso facilitado aos seus dados e informações disponibilizadas e a correção dos mesmos caso estejam incompletos, inexatos ou desatualizados.

Outra similaridade entre o CDC e a LGPD está presente na produção de provas, onde é garantido a parte hipossuficiente a inversão do ônus da prova, ou seja, quando presentes os requisitos, quais sejam: o juiz acreditar ser a alegação do fato pelo titular dos dados ou consumidor verossímil, houver hipossuficiência para fins de produção de prova ou quando a produção de prova resultar extremamente onerosa para o titular/consumidor o juiz poderá inverter o ônus da prova. Essa alegação encontra seu fundamento jurídico no Código de Defesa do Consumidor em seu artigo 6º inciso VIII, e na Lei Geral de Proteção de Dados em seu artigo 42 §2º.

Diante todo o exposto é possível notar que o Código de Defesa do Consumidor influenciou drasticamente na criação e no processo de elaboração da Lei Geral de Proteção de Dados, visto que, ambos convergem em diversos pontos como na questão da proteção da parte vulnerável da relação sendo o consumidor e o titular dos dados, a disseminação dos direitos e deveres acerca desses temas, a privacidade e a possibilidade de retificação dos dados do titular, a necessidade de notificação acerca da guarda dos dados e a inversão do ônus probatório. Sendo assim, é prudente dizer que o Código de Defesa do Consumidor pavimentou o caminho para a criação e formação da Lei Geral de Proteção de Dado.

2.1.4 Diretiva 95/46/CE da União Europeia (1995)

Antes de iniciar as explicações acerca da legislação em si, é importante destacar o significado das diretivas na União Europeia. De acordo com o site EUR-Lex, a diretiva se trata de:

> [2]A diretiva faz parte do direito derivado da UE. É, por conseguinte, adotada pelas instituições da UE com base nos tratados fundadores. Uma vez adotada a nível da UE, a diretiva é incorporada — ou transposta — pelos países da UE, passando a vigorar como lei nesses países.
> Por exemplo, a diretiva relativa à organização do tempo de trabalho estabelece períodos de descanso obrigatórios e um limite relativo ao tempo de trabalho semanal autorizado na UE.
> No entanto, cabe a cada país a elaboração de legislação própria para determinar o modo como estas regras serão aplicadas.

Sendo assim, a diretiva trata-se de um objetivo geral que deve ser alcançado pelos países que compõem a União Europeia, devendo cada um deles criar sua própria legislação para atingir esse objetivo.

Assim, a Diretiva 95/46/CE da União Europeia, criada no dia 24 de outubro de 1995, tinha o intuito principal de proteger os direitos e as liberdades das pessoas no que diz respeito ao tratamento de dados pessoais, através da adoção dos critérios essenciais que conferem licitude ao tratamento e dos princípios relativos à qualidade dos dados (União Europeia, 1995).

É interessante destacar a visão a longo prazo que esta Diretiva apresenta desde aquela época, já prevendo os avanços tecnológicos e criando de antemão uma legislação capaz de acompanhar esse desenvolvimento. Definindo conceitos profundos e complexos sobre o tratamento de dados.

2.1.4.1 Dos princípios da Diretiva 95/46/CE da União Europeia

Primeiramente, é de grande relevância citar os princípios presentes na Diretiva Europeia relativos à qualidade dos dados ostentados no artigo 6º, segundo o qual:

> 1. Os Estados-membros devem estabelecer que os dados pessoais serão:
> a) Objeto de um tratamento leal e lícito;
> b) Recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades. O tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-membros estabeleçam garantias adequadas;

[2] Link de acesso para o artigo: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al14527

> c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente;
> d) Exatos e, se necessário, atualizados; devem ser tomadas todas as medidas razoáveis para assegurar que os dados inexatos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente, sejam apagados ou retificados;
> e) Conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente. Os Estados-membros estabelecerão garantias apropriadas para os dados pessoais conservados durante períodos mais longos do que o referido, para fins históricos, estatísticos ou científicos.

Interessante notar que a base principiológica desta diretiva se assemelha com o artigo 6º da Lei Geral de Proteção de Dados que trata justamente sobre a boa-fé e os princípios que devem ser observados no tratamento de dados aqui no Brasil, devendo cumprir com a sua finalidade, que inclui o tratamento legítimo, explicito e informado ao titular, não podendo ser realizado de forma incompatível com tais finalidades. Além da adequação e necessidade do tratamento, sendo indispensável o acesso facilitado, claro e objetivo sobre as informações pertinentes ao tratamento dos dados e os respectivos agentes responsáveis. Prezando pela segurança dos dados e adotando medidas de prevenção, para que o titular não seja prejudicado durante o tratamento.

Ainda nesse sentido, no artigo 7º da Diretiva, estão enunciados os princípios relativos à legitimidade do tratamento de dados, no qual:

> Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efetuado se:
> a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento; ou
> b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou
> c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; ou
> d) O tratamento for necessário para a proteção de interesses vitais da pessoa em causa; ou
> e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; ou
> f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º.

Uniformemente, na LGPD, o artigo 7º ressalta quais hipóteses o tratamento de dados poderá ser realizado e, assim como na Diretiva, só será realizado mediante o consentimento do titular, para cumprimento de alguma obrigação legal, para e realização de interesses públicos específicos, para execução de contratos de interesse do titular ou interesse legítimo do controlador ou de terceiros, ou ainda para a proteção da vida ou incolumidade física do titular ou de terceiros.

Através da análise dos princípios elencados na Diretiva 95/46/CE da União Europeia, fica evidentemente clara a interferência que esta causou na LGPD pois, basicamente, os mesmos princípios estão presentes na Lei Geral de Proteção de Dados. Demonstrando mais uma vez como a legislação europeia influenciou na brasileira.

2.1.4.2 Definições terminológicas da Diretiva 95/46/CE da União Europeia

Ademais, é possível citar o artigo 2º da Diretiva 95/46/CE, que trata das definições terminológicas referentes ao tratamento de dados, segundo o qual: “Para efeitos da presente diretiva, entende-se por:

> a) «Dados pessoais», qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;
> b) «Tratamento de dados pessoais» («tratamento»), qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;
> c) «Ficheiro de dados pessoais» («ficheiro»), qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, que seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;
> d) «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios do tratamento sejam determinadas por disposições legislativas ou regulamentares nacionais ou comunitárias, o responsável pelo tratamento ou os critérios específicos para a sua nomeação podem ser indicados pelo direito nacional ou comunitário;
> e) «Subcontratante», a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que trata os dados pessoais por conta do responsável pelo tratamento;

> f) «Terceiro», a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que não a pessoa em causa, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão habilitadas a tratar dos dados;
> g) «Destinatário», a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que receba comunicações de dados, independentemente de se tratar ou não de um terceiro; todavia, as autoridades susceptíveis de receberem comunicações de dados no âmbito duma missão de inquérito específica não são consideradas destinatários;
> h) «Consentimento da pessoa em causa», qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento." (União Europeia, 1995).

A LGPD, por sua vez, definiu os conceitos em seu artigo 5º, possuindo forte semelhança com o artigo exposto acima, explicando o que seria dado pessoal, dado pessoal sensível, banco de dados, titular, controlador, operador, encarregado, agentes de tratamento, anonimização, consentimento, bloqueio, eliminação, uso compartilhado e transferência de dados. Possuindo semelhanças inclusive com a descrição dos conceitos expostas no Diretiva Europeia.

Outro ponto de convergência dessas leis encontra-se no artigo 3º da Diretiva Europeia e o artigo 4º da LGPD. Na Diretiva Europeia artigo 3º nº 2, está estipulado que "A presente diretiva não se aplica ao tratamento de dados pessoais: efetuado no exercício de atividades não sujeitas à aplicação do direito comunitário, tais como as previstas nos títulos V e VI do Tratado da União Europeia, e, em qualquer caso, ao tratamento de dados que tenha como objeto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse tratamento disser respeito a questões de segurança do Estado), e as atividades do Estado no domínio do direito penal." (União Europeia, 1995).

A LGPD em seu artigo 4º inciso III também afirmou que a lei não se aplicaria ao tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividade de investigação e repressão de infrações penais, entre outras hipóteses mencionadas no artigo. Sendo notável mais uma vez como a Diretiva 95/46/CE serviu de inspiração para a formação da LGPD.

O artigo 8º da Diretiva explana sobre as categorias específicas de dados e quando eles poderão ser objeto de tratamento. Segundo ele:

> 1. Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções

> religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual.
> 2. O nº 1 não se aplica quando: a) A pessoa em causa tiver dado o seu consentimento explícito para esse tratamento, salvo se a legislação do Estado-membro estabelecer que a proibição referida no nº 1 não pode ser retirada pelo consentimento da pessoa em causa; ou b) O tratamento for necessário para o cumprimento das obrigações e dos direitos do responsável pelo tratamento no domínio da legislação do trabalho, desde que o mesmo seja autorizado por legislação nacional que estabeleça garantias adequadas; ou c) O tratamento for necessário para proteger interesses vitais da pessoa em causa ou de uma outra pessoa se a pessoa em causa estiver física ou legalmente incapaz de dar o seu consentimento; ou d) O tratamento for efetuado, no âmbito das suas atividades legítimas e com as garantias adequadas, por uma fundação, uma associação ou qualquer outro organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, na condição de o tratamento dizer unicamente respeito aos membros desse organismo ou às pessoas que com ele mantenham contatos periódicos ligados às suas finalidades, e de os dados não serem comunicados a terceiros sem o consentimento das pessoas em causa; ou e) O tratamento disser respeito a dados manifestamente tornados públicos pela pessoa em causa ou for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial.
> 3. O nº 1 não se aplica quando o tratamento dos dados for necessário para efeitos de medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamentos médicos ou gestão de serviços da saúde e quando o tratamento desses dados for efetuado por um profissional da saúde obrigado ao segredo profissional pelo direito nacional ou por regras estabelecidas pelos organismos nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de segredo equivalente.
> 4. Sob reserva de serem prestadas as garantias adequadas, os Estados-membros poderão estabelecer, por motivos de interesse público importante, outras derrogações para além das previstas no nº 2, quer através de disposições legislativas nacionais, quer por decisão da autoridade de controlo referida no artigo 28º.
> 5. O tratamento de dados relativos a infracções, condenações penais ou medidas de segurança só poderá ser efetuado sob o controlo das autoridades públicas ou se o direito nacional estabelecer garantias adequadas e específicas, sob reserva das derrogações que poderão ser concedidas pelo Estado-membro com base em disposições nacionais que prevejam garantias específicas e adequadas. Contudo, o registo completo das condenações penais só pode ser mantido sob o controlo das autoridades públicas. Os Estados-membros podem estabelecer que o tratamento de dados relativos a sanções administrativas ou decisões cíveis fique igualmente sujeito ao controlo das autoridades públicas.
> 6. As derrogações ao nº 1 prevista nos números 4 e 5 serão notificadas à Comissão.
> 7. Cabe aos Estados-membros determinar as condições em que um número nacional de identificação ou qualquer outro elemento de identificação de aplicação geral poderá ser objeto de tratamento.

Inicialmente, nota-se que a definição exposta no artigo 8º sobre a natureza desses dados é muito parecida com a do artigo 5º inciso II da LGPD, que explica o que seria “Dado Pessoal Sensível”, com a diferença que este último apresenta um conceito mais completo em virtude das mudanças ocorridas na

sociedade no decorrer dos anos, entre 1995 e 2018, respectivamente as datas de criação da Diretiva Europeia e da LGPD.

O artigo 11 da Lei Geral de Proteção de Dados, por sua vez, explica quais serão as ocasiões em que o tratamento de dados sensíveis poderá ser realizado e lembra muito o nº2 do artigo 8º da Diretiva que trata das hipóteses onde será realizado o tratamento de dados específicos.

2.1.4.3 Dos direitos do titular na Diretiva 95/46/CE da União Europeia

Em sequência, os artigos 10 e 11 da Diretiva Europeia, dizem respeito à algumas informações que o titular dos dados tem direito de receber durante o tratamento quando ele estiver presente, ou não, respectivamente. Por isso, cabe transcrever somente o artigo 11, visto que ele possui a mesma redação do 10º com a diferença adicional do nº2 que informa quando o artigo não será aplicado. De acordo com o artigo 11, “1. Se os dados não tiverem sido recolhidos junto da pessoa em causa, os Estados-membros estabelecerão que o responsável pelo tratamento, ou o seu representante, deve fornecer à pessoa em causa, no momento em que os dados forem registados ou, se estiver prevista a comunicação de dados a terceiros, o mais tardar aquando da primeira comunicação desses dados, pelo menos as seguintes informações, salvo se a referida pessoa já delas tiver conhecimento: a) Identidade do responsável pelo tratamento e, eventualmente, do seu representante; b) Finalidades do tratamento; c) Outras informações, tais como: as categorias de dados envolvidos, os destinatários ou categorias de destinatários dos dados, a existência do direito de acesso aos dados que lhe digam respeito e do direito de os retificar, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir à pessoa em causa um tratamento leal dos mesmos. 2. O nº 1 não se aplica quando, nomeadamente no caso do tratamento de dados com finalidades estatísticas, históricas ou de investigação científica, a informação da pessoa em causa se revelar impossível ou implicar esforços desproporcionados ou quando a lei dispuser expressamente o registo dos dados ou a sua divulgação. Nestes casos, os Estados-membros estabelecerão as garantias adequadas.” (União Europeia, 1995).

A LGPD, em seu artigo 9º, aborda basicamente a mesma ideia. Conferindo o direito do titular a ter acesso claro e facilitado às informações sobre o

tratamento de seus dados, assim como as informações acerca da finalidade do tratamento, sua forma e duração, a identificação e informações de contato do controlador, as responsabilidades dos agentes de tratamento e os direitos conferidos a ele na qualidade de titular dos dados.

Dando continuidade, o artigo 12 da Diretiva 95/46/CE estabelece os direitos de acesso do titular, no qual: “Os Estados-membros garantirão às pessoas em causa o direito de obterem do responsável pelo tratamento: a) Livremente e sem restrições, com periodicidade razoável e sem demora ou custos excessivos: a confirmação de terem ou não sido tratados dados que lhes digam respeito, e informações pelo menos sobre os fins a que se destina esse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados, a comunicação, sob forma inteligível, dos dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem dos dados, o conhecimento da lógica subjacente ao tratamento automatizado dos dados que lhe digam respeito, pelo menos no que se refere às decisões automatizadas referidas no nº 1 do artigo 15º; b) Consoante o caso, a retificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na presente diretiva, nomeadamente devido ao carácter incompleto ou inexato desses dados; c) A notificação aos terceiros a quem os dados tenham sido comunicados de qualquer retificação, apagamento ou bloqueio efetuado nos termos da alínea b), salvo se isso for comprovadamente impossível ou implicar um esforço desproporcionado.” (União Europeia, 1995).

Já na LGPD, esses direitos são tratados no artigo 18, que garante ao titular a confirmação de existência do tratamento, acesso aos dados, correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessário ou tratados em desconformidade com a lei, entre outros direitos que serão abordados de maneira mais profunda no decorrer do presente trabalho

Em síntese, é possível afirmar que a Diretiva 95/46/CE da União Europeia serviu como um guia legislativo para a criação e formação da Lei Geral de Proteção de Dados e de diversas outras legislações referentes ao tema, por conter regras adequadas e suficientes para que o tratamento seja realizado de forma segura e eficiente, além de ser simples, o que possibilita que outros países

consigam adotá-la fazendo as devidas alterações para se adequar ao seu ordenamento jurídico.

2.1.4.4 Lei 12.527 de Acesso à Informação (2011)

A Lei nº 12.527, também conhecida como Lei de Acesso à informação, foi sancionada em 18 de novembro de 2011, regulamentando o direito constitucional dos cidadãos de acesso as informações públicas ou armazenadas por órgãos e entidades da União, Estados, Distrito Federal e Municípios, elencado no artigo 5º inciso XXXIII, artigo 37 §3º inciso II e artigo 216 §2º da Constituição Federal de 1988.

O Ministério da Educação informa que:

> A Lei institui como princípio fundamental que o acesso à informação pública é a regra, e o sigilo somente a exceção. Para garantir o exercício pleno do direito de acesso previsto na Constituição Federal, a Lei define os mecanismos, prazos e procedimentos para a entrega das informações solicitadas à administração pública pelos cidadãos. A Lei igualmente determina que os órgãos e entidades públicas deverão divulgar um rol mínimo de informações proativamente por meio da internet

Dessa forma, a Lei nº12.527/11 consagra o direito do cidadão de acessar as informações públicas, sendo aplicável aos poderes Legislativo, Executivo, as Cortes de Contas, e Judiciário e do Ministério Público. Além das Autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios, de acordo com o artigo 1º da Lei de Acesso à Informação (Brasil, 2011).

Em um primeiro momento a Lei de Acesso à Informação parece possuir uma antinomia jurídica em relação a LGPD, uma vez que, a LAI visa dar maior transparência e publicidade as informações públicas enquanto a LGPD tem como objetivo o sigilo e a proteção dos dados. Entretanto, com uma breve análise de ambas as legislações, é possível perceber que elas se complementam ao invés de se contradizerem. Por exemplo, ao tratar de informações sigilosas a LAI, em seu artigo 25 diz que:

> Art. 25. É dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção. (Regulamento)
> § 1º O acesso, a divulgação e o tratamento de informação classificada como sigilosa ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas na forma do regulamento, sem prejuízo das atribuições dos agentes públicos autorizados por lei.
> § 2º O acesso à informação classificada como sigilosa cria a obrigação para aquele que a obteve de resguardar o sigilo.
> § 3º Regulamento disporá sobre procedimentos e medidas a serem adotados para o tratamento de informação sigilosa, de modo a protegê-la contra perda, alteração indevida, acesso, transmissão e divulgação não autorizados.

Em adição ao artigo 25, é possível citar o artigo 31, segundo o qual:

> Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
> I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
> II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
> § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.
> § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:
> I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
> II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
> III - ao cumprimento de ordem judicial;
> IV - à defesa de direitos humanos; ou
> V - à proteção do interesse público e geral preponderante.
> § 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.
> § 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

Portanto, tanto a LAI quanto a LGPD asseguram a privacidade do cidadão, com a diferença que a Lei de Acesso à Informação permite a devida transparência ao realizar o tratamento de dados, podendo ser realizado somente mediante previsão legal ou autorização do titular, com a obrigação de realizar o

tratamento de forma transparente, respeitando os direitos e garantias individuais de cada pessoa.

Nesse sentido, Ilderlândio Teixeira (2020, s.p) afirma que:

> Observa-se que não existe uma superioridade de uma lei sobre a outra, mas particularidade em ambas: uma em garantir o acesso à informação; em regra; e a outra em assegurar a privacidade dos dados pessoais.
> É notório que ambas buscar resguardar a informação pessoal de terceiros não autorizados, porém apenas a LGPD decanta na preocupação em ter análise de impacto de privacidade documentada, políticas de privacidade e proteção documentada, políticas de respostas a incidentes.
> Desta forma, nota-se que as leis, apesar de suas peculiaridades, mais contribuem para a proteção de dados pessoais comuns e especiais do que se repelem

Em síntese, é possível afirmar que elas são compatíveis entre si, conferindo maior autonomia para o titular sobre o fornecimento ou não de seus dados e sobre a transparência durante o tratamento deles. Sendo a LAI uma legislação antecessora a LGPD que já previa alguns direitos em relação a proteção de dados pessoais de forma mais abrangente, dando enfoque principalmente na transparência das informações públicas, mas contribuindo de forma positiva na criação da Lei Geral de Proteção de Dados.

2.1.4.5 Lei 12.737 Carolina Dieckmann (2012)

A lei 12.737 de 30 de novembro de 2012, popularmente conhecida como Lei Ana Carolina Dieckmann, é responsável por tipificar criminalmente os delitos informáticos, causando uma alteração no Código Penal Brasileiro.

No corpo de seu texto ficaram estipulados os crimes de “Invasão de dispositivo informático”, “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública” e Falsificação de documento particular”.

O crime de Invasão de dispositivo informático está no artigo 154-A do Código Penal, e recebe a seguinte redação:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput .
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.”

O crime de Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública consta no artigo 266 do Código Penal, que expõe:

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
> § 1 º-Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. (Incluído pela Lei nº 12.737, de 2012) Vigência
> § 2 º-Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública. (Incluído pela Lei nº 12.737, de 2012) Vigência

Por sua vez, o crime de Falsificação de documento particular está descrito no artigo 298 do Código Penal, que tipifica a conduta de: “Falsificar, no todo ou em parte, documento particular ou alterar documento particular” com pena de reclusão de um a cinco anos, e multa (Brasil, 1940).

Diferente de outras leis, essa não possui princípios ou grandes semelhanças na sua redação com a LGPD. Contudo, ela possui sua devida importância, uma vez que serviu para tipificar condutas que prejudicam com certa frequência na vida cotidiana de pessoas comuns. Além de fomentar a discussão acerca do tema, devido a grande repercussão do caso, o que contribuiu para alertar a população sobre os riscos e os cuidados que se devem tomar na proteção de seus

dados pessoais e, consequentemente, auxiliou na criação da Lei Geral de Proteção de Dados.

2.1.5 Marco Civil da Internet (2013)

A Lei 12.965/2014, também conhecida como Marco Civil da Internet, foi aprovada e sancionada em abril de 2014. Seu surgimento se deu através de uma consulta pública realizada pela Secretaria de Assuntos Legislativos do Ministério da Justiça. A ideia basilar era a criação de princípios, direitos, deveres e garantias conferidos aos usuários da internet o que resultaria em uma “Constituição da Internet”.

Entretanto, após diversos debates e alterações na Lei 12.965/2014, ocorreu que ela teve seu propósito desvirtuado e ao invés de conferir direitos, garantias e deveres passou a regular uma série de atividades realizadas na internet. Nas palavras de Rick Falkvinge (2012, s.p) :

> O Marco Civil deixou de ser um projeto de lei que garantia à próxima geração de indústrias, o terreno fértil que eles precisavam, e aos cidadãos, a garantia de acesso aos serviços públicos e à liberdade de expressão. Passou a ser apenas um projeto de lei que permite a rastreabilidade habilitada à indústrias obsoletas entrincheiradas contra o futuro e seus sucessores. Foi um desastre.[3]

De qualquer forma, é possível notar de maneira evidente a contribuição que o Marco Civil da Internet teve na elaboração da LGPD visto que, a partir da leitura do texto da lei, nota-se diversos pontos em comum como no caso do artigo 3º do Marco Civil da Internet que estipula os princípios da lei, segundo os quais:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;

[3] Artigo disponível em: https://falkvinge.net/2012/11/21/brasil-desperdica-chance-de-exercer-influencia-geopolitica-mata-o-projeto-de-lei-do-marco-civil-da-internet-em-fiasco-politico/

> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Se relacionando muito com os fundamentos e princípios da LGPD, já mencionados anteriormente.

Outro artigo que possui profunda ligação com a LGPD é o artigo 7º do Marco Civil da internet que dispõe o seguinte:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
> V - manutenção da qualidade contratada da conexão à internet;
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
> XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Nele estão contidas diversas diretrizes que norteiam principalmente os artigos 6º e 7º da LGPD além de influenciar outros artigos de maneira geral, que

dizem respeito justamente a qualidade das informações prestadas sobre o tratamento de dados ao usuário, o não fornecimento de dados pessoais a terceiros, salvo nas hipóteses previstas em lei, o consentimento expresso do usuário para que possa ser realizado o tratamento de dados e a exclusão dos dados pessoais quando cessados os motivos para seu armazenamento. Ficando evidente o elo de complementariedade entre o Marco Civil da Internet e a LGPD.

2.1.6 GDPR europeu (2018)

O General Data Protection Regulation (Regulamento Geral de Proteção de Dados) é uma lei que foi aprovada em 2016 e entrou em vigor no dia 25 de maio de 2018, obrigando as empresas a se adequarem a essa nova legislação que possui o escopo de proteger a privacidade e os dados pessoais dos cidadãos da União Europeia proibindo que empresas armazenem informações que possam identificar o usuário sem que ele tenha dado consentimento para isso. Dessa forma, a lei permite que o usuário tenha maior autonomia em relação ao uso de seus dados, uma vez que, para a empresa utiliza-los de maneira legal será necessário o consentimento do mesmo, além de ser clara e objetiva a finalidade do uso de seus dados.

Como o GDPR e a Diretiva 95/46/CE tem origem na União Europeia existem diversas semelhanças entre elas, e consequentemente com a LGPD, uma vez que ambas serviram de base para sua criação.

A primeira semelhança, que se encontra nas três legislações inclusive, é referente as definições dos termos que são usados no decorrer da lei. Na GDPR eles estão presentes no artigo 4º que traz inúmeras descrições, mas as que coincidem com a LGPD são:

> 1. «Dados pessoais», qualquer informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); uma pessoa física identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador, como um nome, um número de identificação, dados de localização, um identificador online ou um ou mais fatores específicos para o físico, fisiológico, identidade genética, mental, econômica, cultural ou social dessa pessoa física;
> 2. 'processamento' significa qualquer operação ou conjunto de operações que é realizado em dados pessoais ou em conjuntos de dados pessoais, seja ou não por meios automatizados, tais como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou de outra forma disponibilizando, alinhamento ou combinação, restrição, apagamento ou destruição;

> 5. 'pseudonimização' significa o processamento de dados pessoais de tal forma que os dados pessoais não possam mais ser atribuídos a um titular de dados específico sem o uso de informações adicionais, desde que tais informações adicionais sejam mantidas separadamente e estejam sujeitas a medidas técnicas e organizacionais garantir que os dados pessoais não sejam atribuídos a uma pessoa singular identificada ou identificável;
> 6. «Arquivo», qualquer conjunto estruturado de dados pessoais acessíveis de acordo com critérios específicos, sejam eles centralizados, descentralizados ou dispersos numa base funcional ou geográfica;
> 7. «responsável pelo tratamento», a pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que, individualmente ou em conjunto com outros, determina as finalidades e os meios de tratamento dos dados pessoais; sempre que os fins e os meios desse tratamento sejam determinados pela legislação da União ou dos Estados-Membros, o responsável pelo tratamento ou os critérios específicos para a sua nomeação podem ser previstos na legislação da União ou dos Estados-Membros;
> 8. «processador», uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que trata dados pessoais em nome do responsável pelo tratamento;
> 11. 'consentimento' do titular dos dados significa qualquer indicação dada livremente, específica, informada e inequívoca dos desejos do titular dos dados, pela qual ele ou ela, por uma declaração ou por uma ação afirmativa clara, significa concordar com o processamento de dados pessoais relacionados a ele ou ela.

Cabe dizer que na GDPR existem diversas outras definições que não constam na LGPD e que algumas recebem títulos diferentes, mas possuem a mesma função, como é o caso dos números 2, 5, 6, 7 e 8, que na LGPD recebem respectivamente os nomes de: tratamento, anonimização, banco de dados, controlador e operador.

A segunda semelhança diz respeito aos princípios relativos ao tratamento de dados. No GDPR estão elencados no artigo 5º que diz:

> 1. Os dados pessoais devem ser:
> a) processados de forma lícita, justa e transparente em relação ao titular dos dados ('legalidade, justiça e transparência');
> b) coletados para fins especificados, explícitos e legítimos e não processados posteriormente de maneira incompatível com esses fins; o tratamento posterior para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos não deve, nos termos do artigo 89.º, n.º 1, ser considerado incompatível com os objetivos iniciais («limitação da finalidade»);
> c) adequados, relevantes e limitados ao que é necessário em relação aos fins para os quais são processados ('minimização de dados');
> d) precisos e, quando necessário, atualizados; devem ser tomadas todas as medidas razoáveis para garantir que os dados pessoais inexatos, tendo em conta os fins para que são tratados, sejam apagados ou retificados sem demora («exatidão»);
> e) mantidos em uma forma que permita a identificação dos titulares dos dados por tempo não superior ao necessário para os fins para os quais os dados pessoais são processados; os dados pessoais podem ser armazenados por períodos mais longos, desde que sejam processados

> exclusivamente para fins de arquivamento de interesse público, para fins de pesquisa científica ou histórica ou para fins estatísticos, de acordo com o Artigo 89 (1), sujeito à implementação de procedimentos técnicos e organizacionais apropriados medidas exigidas pelo presente regulamento para salvaguardar os direitos e liberdades do titular dos dados («limitação de armazenamento»);
> f) processados de forma a garantir a segurança adequada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, utilizando medidas técnicas ou organizacionais adequadas ('integridade e confidencialidade').
>
> 2. O responsável pelo tratamento deve ser responsável e ser capaz de demonstrar o cumprimento do disposto no n.º 1 («responsabilização»).

Evidentemente, os princípios da LGPD seguem a mesma linha dos apresentados no GDPR, isso por que eles conferem um direcionamento na criação e cumprimento das normas de proteção de dados que deve alcançar um padrão de qualidade igual ou superior ao estabelecido pela GDPR e por isso os princípios teoricamente devem ser semelhantes.

No artigo 6º da GDPR estão os requisitos para que o processamento de dados seja feito de forma legítima. A LGPD apresentou o assunto em seu artigo 7º, sendo quase idêntico ao que consta na lei europeia.

Outra semelhança entre as duas legislações reside no fornecimento das informações quando os dados do titular são coletados. Tanto a Lei Geral de Proteção de dados (artigos 17 a 22) quanto ao General Data Protection Regulation (artigos 12 a 22) alegam que devem ser fornecidas ao titular informações como: a identidade e os dados de contato do responsável pelo tratamento; os dados de contato do responsável pela proteção de dados, quando aplicável; os fins do tratamento a que se destinam os dados pessoais, bem como a base jurídica para o tratamento; os interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros; os destinatários dos dados; o período de tratamento dos dados; o direito de retificação ou apagamento de dados incorretos, bem como a portabilidade dos dados; o direito de retirar o consentimento acerca do tratamento a qualquer momento; obrigação de notificação sobre o tratamento de dados e o direito de receber informações sobre o tratamento de dados realizado de forma automatizada.

É importante mencionar que as restrições no que tange a aplicação da lei europeia se encontram no artigo 23, informando que a lei não se aplica quando a restrição respeita os direitos e liberdades fundamentais e é necessária para salvaguardar: “a) segurança nacional; b) defesa nacional; c) segurança pública; d) a

prevenção, investigação, detecção ou repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública; e) outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo questões monetárias, orçamentais e fiscais, saúde pública e segurança social; f) a proteção da independência judicial e dos procedimentos judiciais; g) a prevenção, investigação, detecção e repressão de violações da ética para profissões regulamentadas; uma função de fiscalização, fiscalização ou regulação ligada, ainda que ocasionalmente, ao exercício da autoridade oficial nos casos referidos nas alíneas a) e) e g); i) a proteção do titular dos dados ou dos direitos e liberdades de terceiros; j) a execução de ações de direito civil." (União Europeia). A lei brasileira também apresenta algumas restrições em seu artigo 4º, mas estas se limitam a hipóteses em que o tratamento é: "I- realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II- realizado para fins exclusivamente: a) jornalístico e artísticos, ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III- realizado para fins exclusivos de: a) segurança pública b) defesa nacional; c) segurança do Estado e d) atividades de investigação e repressão de infrações penais." (Brasil,2018).

Existem semelhanças também relacionadas as funções de operador e controlador de dados. Ambas as legislações informam que o controlador e o operador devem manter registro das operações de tratamento contendo informações sobre o processo. Além disso, o operador deverá realizar o tratamento de acordo com as instruções fornecidas pelo controlador, que verificará as instruções e normas sobre a matéria. Essas regras estão expostas nos artigos 37 a 40 da LGPD, e nos artigos 24 a 32 do GDPR.

Outra preocupação diz respeito à segurança dos dados. Tanto uma quanto a outra visam garantir que os dados não sofram nenhum tipo de violação ao adotar medidas técnica e administrativas para evitar tal fatalidade, mas, caso haja de fato alguma violação aos dados, o artigo 48 da LGPD e o artigo 33 do GDPR advertem sobre a necessidade de notificação à autoridade responsável e competente, assim como ao titular dos dados, a ocorrência de incidente de segurança que acarrete risco ou dano relevante aos titulares. Nesse sentido, tanto o GDPR quanto a LGPD concordam em realizar avaliações de impacto sobre a

proteção de dados contendo a descrição dos processos de tratamento de dados que podem de alguma forma gerar riscos aos direitos e liberdades dos titulares.

Um ponto que se mostra relevante no estudo dessas legislações é quanto a transferência internacional de dados. É convergente o entendimento no sentido de que, para que haja a transferência internacional dos dados de maneira segura alguns pontos devem ser observados. Entre eles o mais importante é sobre a adequação de países estrangeiros para que propiciem um grau de proteção de dados semelhante ou superior ao previsto na lei, seja o General Data Protection Regulation ou a Lei Geral de Proteção de Dados.

Apesar da GDPR ter sido criada na União Europeia ela afeta diversos outros países, visto que, para empresas estrangeiras atuarem no território desse país é necessário que elas estejam em conformidade com a GDPR, como estipula o artigo 45 nº1 da GDPR:

> [1]A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. [2]Such a transfer shall not require any specific authorisation.[4]

Gerando assim, uma proteção de via dupla pois, caso um estrangeiro compre produtos de uma empresa da União Europeia ele estará amparado pela lei e, caso um cidadão europeu compre um produto internacional a empresa que fornecer esse produto para ele terá que se adequar a GDPR. Isso leva a uma segunda consequência da criação dessa lei, que é o efeito dominó em escala global, já que para que seja possível manter relações econômicas com a EU, será necessário que os países se adequem a essa nova legislação e criem sua própria lei de proteção de dados. A questão relativa à cooperação internacional para a proteção de dados pessoais é tão importante que foi tratada de maneira específica no artigo 50 da GDPR, expondo que:

4 1A transferência de dados pessoais para um país terceiro ou uma organização internacional pode ocorrer se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores especificados dentro desse país terceiro, ou a organização internacional em questão garantem um nível adequado de proteção. 2Tal transferência não exigirá nenhuma autorização específica.

> [5]In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:
> develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
> provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
> engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;
> promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

Dessa forma, é possível notar a partir da leitura do General Data Protection Regulation que a Lei Geral de Proteção de Dados possui grande semelhança com ele, evidenciando mais uma vez que a legislação europeia de proteção de dados serviu de inspiração para criação da Lei Geral de Proteção de Dados no Brasil, e poderá servir de inspiração para diversos outros governos criarem um diploma de lei acerca desse tema, sendo isso algo muito positivo, já que tende a padronizar a proteção de dados em diversos países, facilitando a transferência de dados, a comunicação e o comercio entre eles.

2.1.7 LGPD brasileira (2018)

Após todo exposto, é possível compreender a origem da Lei Geral de proteção de Dados, sendo ela composta por diversos diplomas de leis nacionais e internacionais, recentes e antigas, de forma a observar os defeitos e qualidades das legislações que antecederam a sua criação e tentar projetar da melhor forma possível os conhecimentos obtidos até o presente momento sobre esse assunto tão dinâmico e atual.

---

5 Em relação a países terceiros e organizações internacionais, a Comissão e as autoridades de supervisão devem tomar as medidas adequadas para:
desenvolver mecanismos de cooperação internacional para facilitar a aplicação efetiva da legislação para a proteção de dados pessoais;
fornecer assistência mútua internacional na aplicação da legislação para a proteção de dados pessoais, incluindo por meio de notificação, encaminhamento de reclamações, assistência investigativa e troca de informações, sujeita às salvaguardas adequadas para a proteção de dados pessoais e outros direitos e liberdades fundamentais;
envolver as partes interessadas relevantes em discussões e atividades destinadas a promover a cooperação internacional na aplicação da legislação para a proteção de dados pessoais;
promover o intercâmbio e a documentação de legislação e práticas de proteção de dados pessoais, incluindo sobre conflitos jurisdicionais com países terceiros.

Feito o breve estudo acerca do panorama histórico-evolutivo da LGPD, cabe agora analisar a sua importância na sociedade contemporânea, assim como suas consequências e, posteriormente, fazer um estudo mais técnico e aprofundado dessa lei.

2.2 Importância dos Dados na Atualidade

Atualmente a importância dos dados é indiscutível. Eles são utilizados em larga escala, principalmente com o avanço da internet pois, em um mundo cada vez mais competitivo e com recursos escassos, os dados, sejam eles de pessoais, climáticos, financeiros, ou qualquer outro tipo, influenciam e permitem que o processo decisório de empresas, governos, pessoas e até mesmo máquinas seja o mais assertivo possível, gerando uma taxa de sucesso maior ou menor com base na decisão que foi tomada.

De acordo com Leonardo de Souza:

> Dados são o novo petróleo do mundo e tem se provado cada vez mais relevante no atual mundo dos negócios. Eles precisam ser coletados com precisão, protegidos e usados com sabedoria. A utilização adequada do imenso volume de dados atualmente disponível pode gerar enormes benefícios para instituições e empresas do setor privado e público.

Isso acontece através do chamado “Big Data Analytics”. De acordo com a Gartner Group, empresa de pesquisa e consultoria que auxilia na tomada de decisões de empresas, big data seria:

> Big data são ativos de informações de alto volume, alta velocidade e/ou alta variedade que exigem formas inovadoras e econômicas de processamento de informações que permitem uma visão aprimorada, tomada de decisões e automação de processos[6]

Mas de nada adianta um enorme volume de dados se estes não estiverem organizados e não forem estudados com uma finalidade específica. Isso seria perda de tempo, dinheiro e memória computacional. Por esse motivo o Big Data Analytics existe.

O Big Data Analytics nada mais é do que: a análise dos dados que compõem o Big Data, afim de extrair informações que facilitem e tornem mais

[6] Definição encontrada em: https://www.gartner.com/en/information-technology/glossary/big-data

precisa a tomada de decisões. Sendo capaz também de antecipar tendências de um grupo ou um único indivíduo através de algoritmos e inteligência artificial que estudam o padrão comportamental e traçam um perfil para aquele usuário, definindo o que ele gosta ou não de fazer, comer, ouvir, estudar, praticar, etc. E, através desse estudo, em tese, seria possível prever quais as necessidades daquele indivíduo.

Na área empresarial isso é de grande valia pois, qualquer empresa que tenha uma governança inteligente busca a redução de custos e o aumento de lucros, o que gera uma margem de capital maior para empresa, aumentando seu valor. Mas para se ter uma governança inteligente um dos fatores de maior destaque é a qualidade das decisões, que podem alavancar a empresa ou destruí-la.

É nesse ponto em que a utilização dos dados entra, uma vez que, com um banco de dados de produtos, clientes, parceiros comerciais e outras informações, e com a ajuda de sistemas operacionais capazes de ler e interpretar esses dados apresentando as opções mais viáveis de produção a empresa consegue uma vantagem competitiva em relação aquelas que não fazem uso dessa tecnologia. Por exemplo, ao traçar o perfil de um cliente com base em seus dados coletados, a empresa pode fazer propagandas direcionadas a um público alvo que esteja predisposto a comprar determinado produto, aumentando taxa de conversão daquela propaganda em compras efetivamente realizadas, o que diminuiria o custo da propaganda evitando que ela fosse apresentada para clientes que não tem interesse nesse produto. Ou ainda, consultando o banco de dados a empresa seria capaz de descobrir qual distribuidora possui a matéria prima com o melhor custo-benefício e calcular qual seria o gasto para transportar essa matéria até o local onde ela será utilizada. Assim, a empresa seria capaz de decidir qual a melhor opção, garantindo uma margem de lucro maior.

Além da área comercial, a utilização de dados pode ser fundamental também no setor de saúde onde seu uso é destinado tanto a prevenção e diagnóstico, quanto na investigação clínica de doenças. É possível utilizá-lo também para organização de dados operacionais, clínicos, de exames, tratamentos, medicamentos, entre outros. Podendo estipular os custos gerados nesses processos, possibilitar a redução de despesas para hospitais e pacientes e, consequentemente, melhorar a qualidade dos serviços prestados, aumentando a porcentagem de sucesso na recuperação dos enfermos.

Na educação, é possível que o Big Data auxilie na criação de um sistema personalizado de estudo que atende as necessidades de cada estudante de maneira individual, avaliando suas métricas escolares e definindo qual matéria exigirá maior estudo e qual exigirá menos.

Em síntese, é possível compreender o motivo de se dar tanta importância aos dados na atualidade, afinal de contas, através da coleta e estudo desses dados grandes avanços em quase todas as áreas podem ser alcançados, facilitando a vida cotidiana das pessoas e reduzindo seu custo de vida.

Por outro lado, a utilização incorreta desse mecanismo pode gerar graves consequências para a sociedade como um todo. Um efeito negativo causado pelo uso inadequado e indiscriminado das tecnologias de coleta e análise de dados é a intolerância ideológica de grupos. Esse é um fenômeno antigo e advém da própria natureza humana, ou seja, o homem instintivamente procura associar-se a um grupo do qual entende ser semelhante a ele, pois assim terá maiores chances de sobreviver e reproduzir sua espécie. Essas duas necessidades básicas ocupam o 2º e 3º lugar em grau de importância de acordo com a pirâmide de Maslow, são as chamadas necessidades de segurança e social respectivamente. Porém, da mesma forma, é natural que o homem, ao encontrar indivíduos que sejam diversos do seu grupo, entre em conflito para assegurar sua sobrevivência.

Ao transportar esses conceitos científicos para a realidade atual, é possível compreender o por que o fenômeno da polarização ideológica está presente de maneira acentuada. Isso ocorre através de “bolhas sociais” criadas pelo mecanismo de *Profiling*, no qual as informações pessoais são analisadas de maneira a criar um “perfil eletrônico” que corresponde ao titular dos dados. Uma vez que esse perfil é criado com base nas preferências desse titular, as notícias, produtos, serviços e propagandas são selecionadas de forma a reforçar o paradigma preexistente daquele indivíduo e, em razão dos mecanismos de pesquisa de redes sociais, esse indivíduo tende a se socializar somente com pessoas que apreciam os mesmos interesses dele, criando assim uma bolha com um ideal definido. Por consumir conteúdos selecionados de maneira tendenciosa, as “bolhas” tornam-se intolerantes a opiniões e condutas adversas daquelas que lhes são apresentadas, gerando discussões e atritos com outros grupos que evoluem para conflitos violentos e afins. É importante mencionar que essa tendencia sempre existiu, mas foi potencializada em razão do avanço tecnológico.

Após a compreensão das leis nacionais e internacionais que deram origem a Lei Geral de Proteção de Dados, e da reflexão sobre a importância dos dados na atualidade, assim como as consequências das mudanças trazidas pela análise e tratamento dos dados. Será necessário um estudo para o aprofundamento técnico da LGPD em si, sobre o que ela trata, quais terminologias e conceitos são apresentados por ela, seus objetivos e aplicações, além de como ela será aplicada e por quem.

3 DO QUE SE TRATA A LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados foi promulgada pelo presidente Michel Temer no dia 14 de agosto de 2018 com o Projeto de Lei Complementar nº52/2018.

Para Patrícia Peck Pinheiro, a LGPD se apresenta como:

> A Lei n. 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas (2020, p. 15)

Complementando, ela define a LGPD como “uma legislação extremamente técnica, que reúne uma série de itens de controle para assegurar o

cumprimento das garantias previstas cujo lastro se funda na proteção dos direitos humano” (2020, p. 15).

Após o esclarecimento inicial do que é Lei Geral de Proteção de Dados, é de suma importância que seja feita a análise de seus dispositivos, para se alcançar de maneira objetiva a finalidade dessa lei.

No primeiro capítulo, que versa sobre as disposições preliminares, no artigo 1º e 2º encontramos o objetivo inicial e norteador no qual essa lei se baseará:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.
> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Em adição, o artigo 6º da Lei é de suma importância, pois dispõe os princípios que o tratamento de dados pessoais deverá observar de maneira mais objetiva, merecendo seu destaque:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - 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;
> IV - 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;
> V - 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;
> VI - 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;

> VII - 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;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - 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.

É possível extrair dos conceitos aqui expostos que a LGPD estabelece regras sobre coleta, armazenamento, utilização e compartilhamento de dados pessoais, de maneira a penalizar aqueles que não seguem as diretrizes dessa lei, seja pessoa natural ou jurídica, baseando-se nos direitos fundamentais como o direito à privacidade, liberdade e o livre desenvolvimento da personalidade da pessoa natural, que servem como alicerce para a fundamentação dessa lei, invocando a premissa da boa-fé e havendo a necessidade desses entes cumprirem em consonância com a lei uma série de princípios e controles técnicos para garantir a segurança desses dados e de seus titulares.

3.1 Conceitos e Terminologias Previstos pela LGPD

Superada a breve análise dos preceitos iniciais da LGPD, é importante para a continuidade do estudo, fazer uma elucidação sobre as terminologias e os conceitos utilizados por essa nova legislação, visto que ela foi responsável pelo surgimento de novos agentes e expressões no Direito Digital.

Esse estudo se faz tão importante que em seu artigo 5º a Lei Geral de Proteção de Dados aborda o significado de diversos termos empregados por ela, para elucidação dos prontos relevantes do trabalho e facilitação do entendimento da legislação.

Sendo assim, serão tecidos comentários acerca dos incisos deste artigo, a fim de tornar mais claro o possível o significado dos termos utilizados pela lei.

Dentre os novos termos, um dos mais importantes é o chamado “Titular”. Não é uma palavra nova no mundo jurídico, muito pelo contrário, é

extremamente comum e utilizada em diversas matérias, sendo elas de Direito ou não. Entretanto é importante destacar que é atribuído um outro sentido a ela, diferentemente daquele usual “titular de direito”. Aqui a palavra refere-se ao titular dos dados pessoais, ou seja, à pessoa natural que é dona dos dados que estão sendo tratados. Assim é definida no artigo 5º, inciso V, da própria Lei Geral de Proteção de Dados, sendo “titular”: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;” (Brasil, 2018).

Em sequência, o termo “Dados Pessoais” e suas subespécies são definidos nos incisos I, II e III da mesma lei, no artigo 5º:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre 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;
> 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;

A junção dos dados pessoais de um ou de vários titulares, compõem o ”Banco de Dados”, descrito no artigo 5º, inciso IV da LGPD como: “banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;” (Brasil, 2018).

Uma vez definido o que são os dados pessoais, quais são seus tipos e o que é um banco de dados, é necessário entender o que é o “Tratamento de Dados”, já que toda a lei foi criada pensando em sua regulamentação, sendo encontrado no inciso X e algumas ações relacionadas ao tratamento de dados nos incisos XI, XIII, XIV, XV, XVI:

> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um; dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
> XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

> XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
> XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

O tratamento de dados por sua vez, é realizado pelos agentes de tratamento, elencados no inciso IX e definidos no inciso VI e VII, sendo eles: “VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; e VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;” (Brasil, 2018).

Portanto o controlador tem a função de tomar as decisões referentes ao tratamento de dados, enquanto que o operador é responsável por executar essas decisões.

Vale destacar de maneira mais profunda uma das funções atribuídas ao controlador que é de extrema importância, sendo ela a produção do relatório de impacto à proteção de dados pessoais, destacada no inciso XVIII:

> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

Juntamente com esses dois agentes, atua um terceiro, chamado de “Encarregado”, funcionando como canal de comunicação entre o titular, o controlador e a Autoridade Nacional de Proteção de Dados. Esse terceiro agente está descrito no inciso VIII como: “encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);” (Brasil, 2018)

A Autoridade Nacional de Proteção de Dados, por sua vez, é explanada no inciso XIX, como sendo: “autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.” (Brasil, 2018)

Após o entendimento dos principais agentes, princípios e terminologias utilizadas pela Lei Geral de Proteção de Dados, faz-se necessário entender qual sua finalidade, quando e como ela será aplicada.

3.2 Objetivos e Aplicação da LGPD

No cenário atual, os dados pessoais tem ganhado valor, tonando-se sinônimo de poder e riqueza para empresas, pois empresas como Google e Facebook conseguem coletar esses dados a um custo extremamente baixo e vende-los a um preço altíssimo, tornando essa transação muito lucrativa para elas.

A venda desses dados para outras empresas, por sua vez, possibilita que elas tracem o perfil de seus usuários, podendo utilizar isso para diversas finalidades, seja para construir uma propaganda que atinja seu público de maneira eficaz, seja para apresentar notícias tendenciosas para uma massa de pessoas, como ocorre hoje com o fenômeno da polarização de ideias capaz de alterar drasticamente o curso de uma votação ou incitar o ódio e a intolerância entre indivíduos que possuem ideias opostos.

Do outro lado dessa relação, temos o usuário titular desses dados, que em sua maioria não tem conhecimento sobre as práticas realizadas por essas empresas, ficando à mercê da boa-fé dessas entidades ao coletarem e usarem seus dados como bem entenderem.

Nesse sentido, a Lei Geral de Proteção de dados tem como principal objetivo promover um ambiente seguro, de liberdade e autodeterminação em relação a coleta e utilização desses dados por meio digital ou físico, possibilitando maior autonomia ao titular em relação a disponibilidade e uso de suas informações.

Entretanto, para que a lei cumpra seu objetivo, é necessário que ela tenha eficácia. Inicialmente, foi sancionada em 14 de agosto de 2018 e entrou em vigor no mês de setembro de 2020, mas as penalidades previstas na lei começaram a ser aplicadas somente a partir do mês de agosto de 2021.

Em relação a aplicação material e territorial, a Lei Geral de Proteção de Dados dispôs em seu artigo 3º, incisos I, II e III, conforme exposto:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado,

> independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

É possível observar que a LGPD se preocupou em abordar um grande espectro de formas de tratamento de dados, seja por pessoa física ou jurídica, pública ou privada e independente do meio utilizado para essa prática, sendo a operação realizada no território nacional, ou com o objetivo de ofertar, fornecer bens ou serviços ou tratar dados de titulares localizados no Brasil, ou ainda dados que tenham sido coletados dentro do território nacional. Entretanto a lei não aborda algumas situações dispostas no artigo 4º, segundo o qual:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.
> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
> § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
> § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
> § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa

> de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.

Feita a análise do dispositivo observa-se que quando realizado por pessoa natural para fins particulares e sem interesse econômico, ou quando realizado para fins exclusivamente jornalístico, artístico ou acadêmico a Lei Geral de Proteção de Dados não será aplicada.

Em adição, o inciso III merece destaque, pois se tratando de interesses do Estado a LGPD não será aplicada, mas será aplicada legislação específica que proteja o titular e os interesses públicos, afim de preservar os direitos da sociedade e do cidadão já previstos nessa lei, segundo o §1º do artigo 4º, entretanto, vale destacar que essa legislação específica ainda não existe, o que existe atualmente é apenas um Anteprojeto de Lei sobre a Proteção de Dados na segurança pública e investigações criminais, que foi apresentado a Câmara dos Deputados e ainda se encontra em discussão. Já no §2º,é vedado o tratamento de dados a que se refere este inciso por pessoa de direito privado, com exceção de quando realizado sob a tutela jurídica de direito público ou por pessoa de direito privado que tenha capital integralmente constituído por pessoa de direito público, informando os procedimentos à autoridade nacional, que emitirá opiniões técnicas e recomendações, além de solicitar o relatório de impacto à proteção de dados pessoais.

Isso demonstra o extremo cuidado que os legisladores tiveram em relação a dados de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, visto que eles colocam em risco a segurança do país, comprovando mais uma vez a importância e necessidade de proteção dos dados pessoais de qualquer espécie e independente de seu titular.

3.3 Requisitos para Realização do Tratamento de Dados

No capítulo II, seção I da Lei Geral de Proteção de Dados estão descritos os requisitos para o tratamento de dados pessoais, dispostos no artigo 7º, segundo o qual:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

O inciso I trata sobre o consentimento, que é entendido, no inciso XII do artigo 5º da LGPD, como: “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (Brasil, 2018). Em adição, o artigo 8º da lei que estipula a forma como esse consentimento será fornecido, sendo de suma importância a transcrição do artigo:

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.
> § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Com a análise dos artigos citados acima, nota-se que o consentimento do titular dos dados não pode ser genérico, ele deve ser inequívoco e consciente. Mas no contexto atual, é evidente que o titular concede a permissão para uso de seus dados sem conhecimento nenhum de como eles serão usados. Isso confere uma as empresas a liberdade para fazer o que quiserem, sem maiores cuidados e preocupações com a privacidade dos titulares e responsabilizações que podem vir a sofrer.

Para exemplificar os termos de uso absurdos com os quais as pessoas concordam ao clicar naquele famoso botão “li e concordo” ou “aceito” quando acessam alguma página ou app da web, será transcrito um trecho da política de dados do Facebook:

> Coletamos o conteúdo, comunicações e outras informações que você fornece quando usa nossos Produtos, inclusive quando você se cadastra para criar uma conta, cria ou compartilha conteúdo, envia mensagens ou se comunica com outras pessoas. Isso pode incluir informações presentes ou sobre o conteúdo que você fornece (como metadados), como a localização de uma foto ou a data em que um arquivo foi criado. Isso pode incluir também o que você vê por meio dos recursos que fornecemos, como nossa câmera...[7]

Como foi exposto, o Facebook tem a permissão concedida pelo usuário para coletar a localização e data de fotos, arquivos, mensagens e transações financeiras realizadas dentro do app.

À vista disso, Paulo R. Roque, afirma que:

> De forma expressa, a LGPD veda consentimentos genéricos: é o chamado "consentimento informado livre e esclarecido". Não é o mero consentir, é o consentir qualificado. É o consentir que não autoriza consentimentos genéricos: tem que ser livre, informado e inequívoco. (Roque, 2021)[8]

A LGPD vem atuar justamente nesse sentido, de proteger o titular e os seus dados e conferir maior transparência em relação ao tratamento desses dados, vedando consentimentos genéricos dos quais as empresas, sites e outros possam se beneficiar (KHOURI, 2021, s.p).

Em consonância com o inciso I do artigo 7º, o parágrafo 3º do artigo 8 da lei veda o consentimento fornecido mediante algum vício.

---

[7] Informação encontrada em: https://pt-br.facebook.com/about/privacy.

[8] Link de acesso para o artigo citado: https://www.conjur.com.br/2021-mar-31/garantias-consumo-problema-consentimento-informado-lgpd

Para exemplificar melhor o que são vícios de consentimento, cabe transcrever as palavras de Hewdy Lobo sobre o assunto:

> São vícios do consentimento, como o erro, o dolo e a coação, que se fundam no desequilíbrio da atuação volitiva relativamente a sua declaração. Esses vícios aderem à vontade, aparecem sob forma de motivos que forçam a deliberação e estabelecem divergência entre a vontade real, ou não possibilitam que esta se forme.
> São assim mencionados porque o indivíduo está “viciado” no momento da manifestação da sua vontade. Se a pessoa, ou seja, o declarante tivesse real conhecimento da situação, não teria manifestado sua vontade da forma a qual foi declarada.

Por tanto, para fazer valer o dispositivo, a LGPD atribuiu ao controlador a de responsabilidade provar que o consentimento foi adquirido conforme a lei estipula. Gerando assim, mais um encargo para as empresas que coletam dados e fazendo com que a lei seja de fato cumprida pois, uma vez que o consentimento deve ser concedido de forma livre e inequívoca e, cabe ao controlador garantir isso, não resta outra alternativa para as empresas, a não ser respeitar o dispositivo ou não realizar o tratamento de dados. isso confere ao titular mais segurança no momento de confiar seus dados para terceiros.

Além disso, é conferido ao titular dos dados o direito de revogar seu consentimento, através de procedimento gratuito e facilitado, sendo essa, mais uma ferramenta a dispor do titular para que seja garantida sua proteção e de seus dados.

Em harmonia com os artigos 7º e 8º, o artigo 9º da Lei é o principal responsável por conferir a autodeterminação e a transparência ao titular em relação ao tratamento de seus dados. Segundo ele:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

> § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
> § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.
> § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Os incisos elencam quais as informações estarão disponíveis para uso do titular, entre elas: a finalidade, forma e duração do tratamento; identificação e informações acerca do controlador e do uso compartilhado dos dados e as responsabilidades dos agentes que desempenharão essa função, além de informar ao titular quais são seus direitos.

Já os parágrafos dispõem sobre a validade do consentimento dado pelo titular. O § 1º versa sobre os casos em que as informações dadas ao titular sejam enganosas ou abusivas, não sendo apresentadas com transparência, o consentimento dado pelo titular será considerado nulo. O § 2ºrefere-se aos casos em que houver mudança da finalidade para o tratamento de dados, sendo diversa da apresentada inicialmente, tendo o controlador o dever de avisar previamente o titular, o qual poderá revogar seu consentimento. Por fim, o § 3º aborda os casos em que o tratamento de dados é condição imposta para o fornecimento do produto ou serviço, sendo assim, o titular deverá ser informando sobre essa questão e sobre seus direitos elencados no artigo 18 da Lei Geral de Proteção de Dados, do qual poderá fazer uso.

Entretanto, há situações em que o consentimento do titular não é necessário, como no parágrafo 4º, artigo 7º já transcrito, que versa o seguinte: “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.” (Brasil, 2018).

No caso supra citado, quando o próprio titular disponibiliza esses dados, não é necessário o consentimento do mesmo para realizar o tratamento desses. Observando o princípio da proporcionalidade em relação ao consentimento do titular, nem sempre será necessário o consentimento expresso e inequívoco do

mesmo, ou seja, se a informação foi tornada pública por ele próprio, por qual motivo ele teria o direito de exigir que ela não fosse usada por terceiros, sabendo que a internet é local público e as informações podem ser salvas por qualquer um? Isso seria se beneficiar da própria torpeza, o que é vedado pelo Código Civil. Portanto, é preciso tomar cuidado com as informações que são publicadas sem o devido cuidado.

Mas ainda assim, a LGPD visa proteger o usuário e seus dados mesmo quando suas informações são tornadas públicas. Isso porque os agentes de tratamento de dados não ficam desobrigados a observar os princípios e garantias dos titulares quando for dispensada e exigência de consentimento, de acordo com o §6º , artigo 7º da LGPD:

> § 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Os demais incisos do artigo 7º tratam principalmente de hipóteses permitidas pela lei ou para o cumprimento de contratos e políticas públicas, como é o caso dos incisos II, III, V, VI, IX e X.

Os incisos IV, VII e VIII versam sobre a possibilidade de o tratamento de dados ser usado para realização de estudos por órgãos de pesquisa, e para proteção da vida e tutela da saúde de titular ou terceiro, respectivamente.

3.4 Agentes Responsáveis pela Guarda e Utilização dos Dados

A Lei Geral de Proteção de dados elencou alguns agentes para realizarem o tratamento de dados, entre eles: Agente Nacional de Proteção de Dados, Controlador, Operador e o Encarregado, que já foram brevemente explanados. Desta maneira, será realizado agora um desenvolvimento mais profundo desses entes.

A ANPD como já mencionado, é o órgão da administração pública vinculada à Presidência da República, responsável por zelar, implementar e fiscalizar o cumprimento da Lei nº 13.709/18, podendo fazer alterações nessa lei caso entenda necessário, cabendo à ela futura regulamentação de diversos artigos para que a LGPD tenha maior aderência social.

Em adição, a Autoridade Nacional de Proteção de Dados, servirá como intermediária das relações entre as diversas partes interessadas que vão desde o interessado, até o ente privado e público, se adequando as necessidades impostas pelas autoridades reguladoras e a tríade do poder Executivo, Legislativo e Judiciário, devendo se preocupar não só com a adequação da LGPD em âmbito nacional, mas internacional também.

Fazendo um comparativo entre a ANPD e as DPAs (*Data Protection Authorities*)[9] que são autoridades públicas e independentes que possuem amplo poder de fiscalização, responsáveis pela aplicação da GDPR na União Europeia. É possível traçar um perfil de atuação duplo para esses entes, sendo um direcionado para orientação/fiscalização, para que empresas do setor público e privado se adequem e sigam a legislação; e outro com o cunho punitivo, usado quando não ocorre a adesão correta da lei.

3.4.1 Composição dos agentes responsáveis pela guarda e utilização dos dados

O artigo 55-A ao 55-K da LGPD dispõe sobre a Autoridade Nacional de Proteção de Dados.

> "Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República.
> § 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República.
> § 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD.
> § 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias.
> Art. 55-B. É assegurada autonomia técnica e decisória à ANPD."

[9] Informações retiradas do site: https://iapp.org/resources/article/data-protection-authority/

A estrutura regimental da ANPD, está foi aprovada pelo Decreto nº 10.474 de 26 de agosto de 2020[10], segundo o qual:

> A **ANPD** é constituída pelos seguintes órgãos:
> I - Conselho Diretor;
> II - Órgão consultivo: Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;
> III - Órgãos de assistência direta e imediata ao Conselho Diretor:
> a) Secretaria-Geral;
> b) Coordenação-Geral de Administração; e
> c) Coordenação-Geral de Relações Institucionais e Internacionais;
> IV - Órgãos seccionais:
> a) Corregedoria;
> b) Ouvidoria; e
> c) Assessoria Jurídica; e
> V - Órgãos específicos singulares:
> a) Coordenação-Geral de Normatização;
> b) Coordenação-Geral de Fiscalização; e
> c) Coordenação-Geral de Tecnologia e Pesquisa.
> § 1º O Conselho Diretor é o órgão máximo de decisão da ANPD.
> § 2º Cabe ao Diretor-Presidente a gestão e a representação institucional da ANPD.

O artigo 55-D acrescenta que o Conselho Diretor da ANPD será composto de 5 diretores, incluindo o Diretor-Presidente.

Segundo o §1º, estes serão escolhidos e nomeados pelo Presidente da República após aprovação pelo Senado Federal, por voto secreto e arguição pública, nos termos da alínea ‘f’ do inciso III do artigo 52 da Constituição Federal (Brasil, 1988), e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores – DAS, no mínimo de nível 5.

O §2º aduz que esses membros serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados.

Já o §3º informa que o mandato dos membros do Conselho Diretor será de 4 anos.

É interessante mencionar o fato de que a participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante e não remunerada.

[10] Link de acesso ao Decreto: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226

Em relação a composição do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, pertencerão a ele diversos representantes, como disposto no artigo 58-A da LGPD:

> Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos:
> I - 5 (cinco) do Poder Executivo federal;
> II - 1 (um) do Senado Federal;
> III - 1 (um) da Câmara dos Deputados;
> IV - 1 (um) do Conselho Nacional de Justiça;
> V - 1 (um) do Conselho Nacional do Ministério Público;
> VI - 1 (um) do Comitê Gestor da Internet no Brasil;
> VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais;
> VIII - 3 (três) de instituições científicas, tecnológicas e de inovação;
> IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo;
> X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e
> XI - 2 (dois) de entidades representativas do setor laboral.

Finalizado o estudo sobre a composição dos agentes responsáveis pela guarde e utilização dos dados, é de suma importância também esclarecer quais a competências e atribuições desses agentes.

3.4.2 Competências e atribuições dos agentes responsáveis pela guarda e utilização dos dados

No que tange às competências da ANPD, é possível destacar o artigo 55-J, que atribui diversas funções, entre elas a de: zelar pela proteção de dados pessoais e pela observância dos segredos comerciais e industriais, fiscalizar e aplicar sanções nos casos de descumprimento da lei, apreciar petições de titular contra controlador, promover na população o conhecimento das normas, elaborar pesquisas sobre as práticas nacionais e internacionais de proteção de dados, dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, entre várias outras relacionadas a aplicação da LGPD que produzem resultados fáticos que atingem a sociedade como um todo.

Em adição, o artigo 55-K pontua que a aplicação de sanções previstas na LGPD será de competência exclusiva da ANPD.

O Conselho Diretor teve suas atribuições destacadas no artigo 4º do Decreto Nº 10.474, de 26 de agosto de 2020, no qual ficou responsável por: solicitar informações referentes as questões de tratamento de dados aos demais agentes envolvidos, como relatórios de impacto à proteção de dados pessoais; regulamentar o uso, portabilidade e compartilhamento de dados; dispor sobre padrões e técnicas utilizados no tratamento de dados; determinar o término do tratamento de dados e adoção de providências para proteção dos dados; encaminhar as petições de titulares de dados pessoais apresentados à ANPD contra o controlador, e informe com medidas cabíveis para resolução das violações por órgãos públicos; estabelecer prazos para o atendimento e normas complementares; emitir parecer técnico para garantia do cumprimento da lei; autorizar a transferência internacional de dados pessoais; avaliar os requerimentos sobre o nível de proteção de dados pessoais conferido por outros países ou organismo internacional, e o nível de proteção de dados destes; entre outras práticas administrativas relacionadas a verificação e fiscalização de organismos de certificação e atos praticados por esses, para permissão da transferência internacional de dados.

O Conselho Nacional de Proteção de Dados Pessoais, por sua vez, ficou incumbido das seguintes funções, dispostas no artigo 58-B da LGPD:

> Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade:
> I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;
> II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> III - sugerir ações a serem realizadas pela ANPD;
> IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e
> V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.

Por fim, fica evidente que a ANPD juntamente como seus órgãos de apoio, são essenciais para a aplicação da Lei Geral de Proteção de dados, uma vez que, cada um possui uma função específica, mas todos têm um objetivo em comum, qual seja de elucidar dúvidas acerca dessa nova legislação e fazer valer o que se encontra escrito nela.

4 LIMITAÇÕES IMPOSTAS PELA LGPD

Realizado o estudo sobre os conceitos, terminologias, objetivos e requisitos para a realização do tratamento, assim como, o estudo dos os agentes

responsáveis pela guarda e utilização dos dados, explanando sobre suas competências e atribuições. Será feita uma análise mais profunda das limitações impostas pela LGPD no armazenamento de dados, os tipos de dados que poderão ser coletados e armazenados, como é feita a coleta, armazenamento e proteção desses dados, os direitos dos titulares e quais as medidas de responsabilização e penalidades impostas pelo mau uso e armazenamento dos dados pessoais.

4.1 Quais Tipos de Dados Poderão ser Coletados e Armazenados

Como mencionado anteriormente, existem 3 principais tipos de dados que são abordados pela Lei Geral de Proteção de Dados. São eles: os dados pessoais, os dados sensíveis e os dados anonimizados. Além disso, existem os dados públicos, os dados de crianças e adolescentes e os pseudominizados, sendo eles subtipos dos dados pessoais. Dito isso, é importante que se faça um aprofundamento sobre esses dados, de forma a explicar o que de fato eles representam.

Dados pessoais são aqueles que permitem identificar, localizar ou contactar, direta ou indiretamente, um indivíduo. O Serviço Federal de Processamento de Dados (SERPRO) cita como exemplo de dados pessoais os seguintes:

> nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer; endereço de IP (Protocolo da Internet) e cookies, entre outros.

Dentro da categoria dos dados pessoais existe um tipo de dado que recebe tratamento diferenciado, são os chamados “Dados Pessoais de Crianças e Adolescentes” e necessitam de requisitos especiais para serem tratados. Sua importância é tamanha que a Lei nº 13.709/2018 aborda a questão em uma seção específica, sendo a seção III do capítulo II, ocupada inteiramente pelo artigo 14 da lei, que discorre o seguinte:

> 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.
> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

A partir da leitura do artigo acima citado, é possível fazer uma série de apontamentos relevantes.

Inicialmente, cabe discorrer sobre o princípio do melhor interesse mencionado no caput do artigo 14. Esse princípio decorre de outros dois, quais sejam: o princípio da proteção integral e o princípio da prioridade absoluta.

A proteção integral e da prioridade absoluta possuem seu marco no artigo 227 da Constituição Federal, segundo o qual:

> Art. 227**.** É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

Essa ideia é reforçada no Estatuto da Criança e do Adolescente, em seu artigo 4º, no qual:

> Art. 4º É dever da família, da comunidade, da sociedade em geral e do poder público assegurar, com absoluta prioridade, a efetivação dos direitos referentes à vida, à saúde, à alimentação, à educação, ao esporte, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária.

> Parágrafo único. A garantia de prioridade compreende:
> a) primazia de receber proteção e socorro em quaisquer circunstâncias;
> b) precedência de atendimento nos serviços públicos ou de relevância pública;
> c) preferência na formulação e na execução das políticas sociais públicas;
> d) destinação privilegiada de recursos públicos nas áreas relacionadas com a proteção à infância e à juventude.

É possível notar, portanto, que as crianças e adolescentes, em decorrência desses princípios, carregam consigo uma condição que permitem a elas um desenvolvimento mais seguro de riscos que possam comprometer suas garantias fundamentais em virtude da sua vulnerabilidade.

Em face disso, esse grupo vulnerável possui prioridade no atendimento aos seus interesses perante os demais e, entre os interesses apresentados, devem ser escolhidos aqueles que são mais benéficos para esse grupo.

Além dessas garantias, para maior proteção das crianças e adolescentes, o tratamento dos dados deverá ser realizado mediante consentimento específico do responsável legal. Isso ocorre devido a limitação cognitiva desse grupo por conta da idade, frente a complexidade do mundo digital que lhes é apresentado.

Para que o consentimento do titular do §1º possibilite o tratamento de dados, os controladores deverão fornecer informações sobre os tipos de dados coletados, sua utilização e os procedimentos para exercer os direitos previstos no artigo 18 da LGPD, fazendo valer mais uma vez o direito a autodeterminação informativa conferido pela lei, presente também no §6º do artigo 14, que estipula uma série de requisitos para que as informações disponibilizadas pelos controladores sejam válidas.

Há, no entanto, duas hipóteses em que a exigência de consentimento válido no tratamento de dados de crianças e adolescentes é mitigada. A primeira diz respeito a coleta de dados de crianças e adolescentes quando necessária para sua proteção ou para contatar os pais ou responsáveis legais, no qual não será exigido o consentimento destes, sendo vedado o armazenamento ou o repasse dessas informações para terceiros e, permitindo que esses dados sejam utilizados apenas uma única vez. A segunda ocorre no caso de jogos, aplicativos ou outras atividades que precisam de informações pessoais estritamente necessárias a atividade, nesse caso, os controladores não são obrigados a exigir a participação dos responsáveis pela criança ou adolescente que faz uso de tais ferramentas.

Por fim, cabe mencionar que o consentimento exigido no §1º do artigo 14 da LGPD, deverá ser verificado pelo controlador, que fica responsável por conferir se o consentimento realmente foi conferido pelo responsável da criança ou adolescente.

Existem também os dados públicos, que nada mais são do que dados pessoais que foram tornados públicos por vontade exclusiva do titular, como e-mails ou números de telefones utilizados para criar perfis em redes sociais, e que não necessitam do consentimento do titular para que sejam utilizados para tratamento de dados, conforme artigo 7º §4º da LGPD.

Por outro lado, não são considerados dados pessoais aqueles relacionados a uma pessoa jurídica, como CNPJ, endereço comercial, e-mail da empresa e outros.

Os dados sensíveis, por sua vez, estão elencados de maneira taxativa na LGPD, sendo eles relacionados a origem étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a pessoa natural, de acordo com o artigo 5º, inciso II da Lei 13.709, de 14 de agosto de 2018 (Brasil, 2018). De acordo com a lei eles merecem tratamento específico, assim como os dados de crianças e adolescentes, pois podem ser motivo de discriminação ao seu titular, por exemplo no caso de uma pessoa que tem informações espalhadas a seu respeito acerca de sua convicção religiosa e, por isso, é alvo de críticas e assédio moral em seu ambiente de trabalho.

Existem ainda os dados anonimizados que são aqueles relativos à titular que não possa ser identificado, considerando o uso de meios razoáveis e disponíveis para o tratamento. O SERPRO informa que:

> A Lei Geral de Proteção de Dados Pessoais cita ainda o dado anonimizado, que é aquele que, originariamente, era relativo a uma pessoa, mas que passou por etapas que garantiram a desvinculação dele a essa pessoa. Se um dado for anonimizado, então a LGPD não se aplicará a ele. Vale frisar que um dado só é considerado efetivamente anonimizado se não permitir que, via meios técnicos e outros, se reconstrua o caminho para "descobrir" quem era a pessoa titular do dado - se de alguma forma a identificação ocorrer, então ele não é, de fato, um dado anonimizado e sim, apenas, um dado pseudonimizado e estará, então, sujeito à LGPD.

O artigo 12 da LGPD corrobora com o exposto acima, dizendo que:

> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Ou seja, os dados anonimizados não podem ser ligados a uma pessoa, mesmo aplicando técnicas de engenharia reversa que tornaram um dado pessoal em um anonimizado. Caso seja possível reverter esse procedimento, o dado não seria de fato anonimizado, mas sim pseudominizado.

A pseudominização, segundo o artigo 13 §4º da LGPD, é:

> § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Por fim, cabe dizer que a anonimização de dados é importante tanto para as empresas quanto para os clientes pois, permite que os dados coletados sejam usados de maneira segura, evitando sejam expostos ou usados de maneira ilegal, agregando mais credibilidade para as empresas que adotam essa prática, e mais proteção para os clientes, já que não poderão ser atrelados a uma pessoa específica.

4.2 Como São Coletados Esses Dados

A coleta dos dados pode ocorrer de diversas maneiras, seja através da internet ou não. Sendo offline, a coleta se dá através de entrevistas, por telefone ou pessoalmente; por preenchimento de formulários e pesquisas de campo e até mesmo através de aplicativos que não necessitam de internet no momento da coleta, apenas posteriormente para compilar e organizar os dados. Existem alguns benefícios em realizar a coleta de dados offline, entre eles: adaptabilidade, pois permite que mesmo em áreas onde não há conexão com a internet seja possível coletar os dados; facilidade, pois pode ser realizada através de aparelhos mais simples que não necessitem de conexão com a internet ou mesmo utilizando papel e caneta; custo-benefício maior, uma vez que, como ela não é complexa os custos para sua realização são menores.

Já a coleta de dados online pode ser feita também por meio de pesquisas online, solicitando informações ao cliente através de seu computador; por

rastreamento online, no qual a empresa ou aplicativo possuem um provedor de hospedagem capaz de realizar essa tarefa ou um software de análise para coletar os dados permitindo que você veja quantas pessoas acessaram o site, o tempo de permanência nele, onde eles clicaram, etc.; por monitoramento de mídias sociais, no qual você pode examinar o perfil do público alvo a fim de coletar informações sobre o padrão de comportamento dele na internet; através de cookies que são arquivos de informações baixados do site para o computador do visitante, ficando armazenados no disco rígido e, enquanto durar a navegação na internet esses arquivos serão utilizados. De acordo com Adonis Batista[11], existem três tipos de cookies:

> 1. Cookies de Sessão: Também chamado de cookie transitório, é apagado quando você fecha o navegador de internet. Ele é armazenado na memória temporária do computador e não é retido depois que o navegador é encerrado.
> Os cookies de sessão não coletam informações do seu computador. Eles normalmente armazenam informações na forma de uma identificação que não coleta dados pessoais do usuário.
> 2. Cookies Persistentes: Também chamado de cookie permanente, é armazenado em seu disco rígido até expirar (cookies persistentes são definidos com datas de expiração) ou até você excluir.
> Os cookies persistentes são usados para coletar informações de identificação sobre o usuário, como comportamento de navegação na internet ou preferências para um site específico.
> 3. Cookies Maliciosos: Os cookies normalmente não comprometem a segurança, mas há uma tendência crescente de cookies maliciosos. Esses tipos de cookies podem ser usados para armazenar e acompanhar sua atividade online.
> Eles rastreiam você e seus hábitos de navegação ao longo do tempo, para construir um perfil de seus interesses. Uma vez que esse perfil contenha dados suficientes, há uma boa chance de que suas informações possam ser vendidas a uma empresa de publicidade que, em seguida, use esse perfil para segmentá-lo com anúncios específicos de interesse.

Por fim, cabe dizer que as técnicas de coleta de dados são inúmeras e, com certeza, com o passar do tempo, surgirão novas maneiras de coletar informações pois, o meio digital e tecnológico está em constante evolução, buscando cada vez mais rapidez e eficiência nas tarefas em que se propõe a fazer, restando aos indivíduos a tarefa de estudar e entender como são executadas essas práticas, e de conhecer quais os seus direitos para que possam se resguardar dos abusos que possam vir a ser praticados contra eles.

[11] CEO da empresa de análise de dados Hariken

4.3 Dos Direitos do Titular

A Lei Geral de Proteção de Dados é uma legislação que se utiliza de diversas outras fontes do Direito para sua composição. Nas palavras de Cíntia Rosa Pereira de Lima e Lívia Froner Moreno Ramiro:

> A Lei Geral de Proteção de Dados Pessoais do Brasil – LGPD, Lei n. 13.709, de 14 de agosto de 2018, pode ser considerada um microssistema, pois estabelece princípios e direitos específicos decorrentes do sistema protetivo de dados pessoais.

Assim, com o enfoque principal de proteger a privacidade e os interesses do titular dos dados, o capítulo III da LGPD, composto pelos artigos 17 a 22, versa sobre os direitos do titular.

Segundo o artigo 17 “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta lei” (Brasil, 2018). Isso garante que todos possuem o direito de ter seus dados protegidos de acordo com a lei.

Em sequência, o artigo 18 elenca o que o titular de dados poderá exigir do controlador a qualquer momento, mediante requisição. Entre essas exigências estão:

> 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.

Estes direitos pautam-se na autodeterminação informativa posta no artigo 2º, inciso II, que confere ao titular o direito de receber as informações necessárias acerca do tratamento de seus dados e possibilitar que ele exerça as

faculdades que lhe são garantidas durante o tratamento, possuindo relação direta com os incisos I e II do artigo 18.

Não obstante, o consentimento para a realização do tratamento de dados também está intimamente ligado com a autodeterminação informativa e com os direitos expostos no artigo 18 da LGPD, visto que ele é uma premissa básica para desencadear a rota do tratamento de dados, desde a coleta até o descarte das informações, permitindo a conscientização sobre o tratamento de seus dados e o exercício de direitos atinentes a tutela deles.

Um ponto importante e que merece destaque é o inciso III, que confere ao titular a possibilidade de correição de dados incompletos, inexatos ou desatualizados. Esse é o chamado “Direito de Correção”. Sendo assim, quando o titular sente a necessidade de complementar, corrigir ou atualizar as informações sobre ele presentes em um banco de dados, ele pode fazer isso através de uma solicitação ao controlador, que deverá realizar as mudanças pertinentes.

A anonimização, bloqueio ou eliminação de dados desnecessários ou tratados em desconformidade com a lei, previsto no inciso IV, é outro sistema que visa proteger a identidade, privacidade e interesses do titular mediante a limitação da guarda dos dados que não foram devidamente tratados. Essa limitação ocorre por não haver motivos suficientes para que o agente de tratamento permaneça com as informações do titular e, no caso de ocorrer um vazamento ou invasão do banco de dados, o dano seja o menor possível.

O inciso V, por sua vez, trata sobre a portabilidade dos dados de um fornecedor de produto ou serviço para o outro. Com isso, o indivíduo ganha a possibilidade de, por exemplo, solicitar a portabilidade de e-mails, senhas, fotos e arquivos de um aplicativo ou site para o outro. Impedindo a vinculação de um titular à um único fornecedor, conferindo maior autonomia sobre seus dados e reafirmando o direito à autodeterminação informativa. Vale ressaltar que essa portabilidade sofre uma limitação em relação aos dados já anonimizados, ou seja, caso os dados que estejam sendo objeto de tratamento já tenham sido anonimizados, o antigo fornecedor do produto ou serviço que estava em posse desses dados não será obrigado a transferi-los para o novo fornecedor. É o que estipula o §7º do artigo 18 da lei, segundo o qual: “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” (Brasil,2018).

Também é conferido ao titular o direito de eliminação dos dados pessoais, conforme o inciso VI do artigo 18. Os dados pessoais devem ser apagados, via de regra, quando estiverem presentes as hipóteses do artigo 15 da Lei Geral de Proteção de Dados, que trata sobre o término do tratamento, segundo o qual:

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
> I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
> II - fim do período de tratamento;
> III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
> IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Porém, caso não seja feito o devido descarte dos dados, o titular pode exigir do controlador a eliminação dos dados, com exceção dos casos apresentados pelo artigo 16 da LGPD, no qual:

> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
> I - cumprimento de obrigação legal ou regulatória pelo controlador;
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Nesses casos, é permitido a conservação dos dados, mesmo que o titular peticione a favor de exclusão desses.

O inciso VII confere ao titular dos dados a possibilidade de requerer informações sobre as entidades pública e privadas com as quais o controlador compartilhou seus dados. Mais uma vez o direito a autodeterminação informativa está presente, e possibilita uma igualdade entre as partes, visto que, as empresas, públicas ou privadas, que obtenham os dados de certo indivíduo, conferem ao mesmo tempo o direito de ele exigir informações sobre essas mesmas empresas.

Assim como o inciso VII, o inciso VIII tem relação direta com o direito da autodeterminação informativa, pois segundo ele o titular pode exigir do

controlador informações sobre a possibilidade de não fornecer consentimento e sobre as consequências dessa opção. ou seja, quando o indivíduo fazer uso de determinado site, aplicativo, produto ou serviço, ele poderá solicitar informações sobre a necessidade do consentimento para o tratamento de seus dados e, caso opte por não conceder essa permissão, ele deverá ser informado sobre quais implicações resultam da negativa no que tange ao consentimento, como restrições a determinadas ferramentas do site, produto ou serviço, ou simplesmente a impossibilidade de acessá-lo.

Em adição, o inciso IX confere ao titular o direito de revogar o seu consentimento, observado o disposto no §5º do artigo 8º da LGPD. Isso permite ao titular que ele revogue seu consentimento a qualquer tempo, através de procedimento gratuito e facilitado, mediante sua manifestação expressa, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do artigo 18 mencionado acima. Esse é um direito extremamente importante, ao passo que, caso o titular, por quaisquer motivo, não tenha interesse em continuar a permitir o tratamento de dados, basta que ele manifeste sua vontade através de requerimento direcionado para o agente de tratamento.

O §2º do artigo 18 da Lei Geral de Proteção de Dados diz que: “o titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nessa lei” (Brasil, 2018), reafirmando a tese de que essa legislação serve não só para proteger o titular de maneira passiva, mas também para dar-lhe a autonomia necessária para se defender dos excessos cometidos durante o tratamento de dados.

Em complementariedade com os direitos conferidos pelos incisos do artigo 18, os parágrafos esclarecem os meios pelos quais esses direitos podem ser alcançados. O §1º determina que “o titular dos dados tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional” (Brasil,2018), em adição o §8º alerta que esse peticionamento pode ser feito também perante organismos de defesa do consumidor. Já §3º instrui que “os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.” (Brasil, 2018). Ou seja, para que sejam efetivados esses direitos no contexto fático, é necessário que o titular dos dados ou seu representante legal manifeste sua vontade mediante

requerimento para o agente de tratamento competente perante a autoridade nacional ou organismo de defesa do consumidor. Esse procedimento não acarretará qualquer custo para quem o realiza, e deverá seguir os prazos e os termos previstos no regulamento, de acordo com o §5º.

Em continuidade, o §4º informa que:

> § 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.

Sendo assim, caso não seja possível atender a requisição feita pelo titular, o controlador deverá informar o motivo do não acolhimento do pedido ou, caso o requerente tenha cometido um equívoco em relação ao requerido, esse deverá informar qual o agente responsável, se possível.

O artigo 19, por sua vez, reitera o direito de informação do titular, dando a ele a possibilidade de obter a confirmação da existência de tratamento de dados ou o acesso a estes, em formato simplificado de maneira imediata, de acordo com o inciso I, ou por meio de declaração completa indicando a origem dos dados, inexistência de registro, os critérios utilizados e a finalidade do tratamento, observando os segredos comercial e industrial, fornecido no prazo de até 15 dias a partir do requerimento do titular, conforme o inciso II (Brasil, 2018). É ainda facultado ao titular, caso o tratamento tiver origem em seu consentimento ou em contrato, uma cópia eletrônica integral de seus dados pessoais, respeitando os segredos comercial e industrial, nos termos estipulados pela autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações, segundo o §3º deste artigo. Em adição, o § 4º adverte que a autoridade nacional poderá dispor de forma diferenciada sobre os prazos estipulados nos incisos I e II para os setores específicos.

O § 1º do artigo 19 da LGPD refere-se ao formato que os dados pessoais deverão ser armazenados, sendo obrigatório que esse formato favoreça o exercício do direito de acesso. Enquanto o § 2º do mesmo artigo faculta ao titular o acesso a essas informações por meio eletrônico ou sob forma impressa.

O artigo 20 da Lei Geral de Proteção de Dados aborda um tema extremamente delicado. Segundo ele:

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019)
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

O tratamento de dados avançou a tal ponto que se tornou possível a criação de perfis virtuais que representam as características físicas, emocionais, biológicas e de qualquer outra natureza de um determinado indivíduo. Esses perfis auxiliam as empresas na tomada de decisões, como por exemplo, um banco pode criar um perfil eletrônico de seu cliente, e com base nesse perfil e de análise de dados, decidir se o cliente terá ou não uma linha de crédito.

Ocorre que, a análise de dados e as tecnologias que permeiam esse universo não são perfeitas e se utilizam de estatísticas passadas na tentativa de prever as melhores decisões para o futuro. Entretanto, caso as informações utilizadas para alimentar a base de dados contenham erros, esses erros serão repetidos e em alguns casos até agravados pelo uso das máquinas e da tecnologia, aumentando a discriminação na tomada de decisões automatizadas e no padrão comportamental da inteligência artificial em uso.

Um exemplo prático a ser citado é o algoritmo que era utilizado pelo Twitter até o início de maio de 2021. Nesse caso, os usuários dessa rede social levantaram a tese de que, fazendo uma montagem com o recorte facial de pessoas de diversas cores e colocando essa montagem em um quadro de pré-visualização, onde somente uma parte da imagem é mostrada, o algoritmo do Twitter mostrava preferencialmente a parte de pessoas com pele branca. Em face disso, a empresa realizou um experimento para averiguar a situação, no qual fizeram o sistema de análise de fotos reconhecer rostos de pessoas brancas, pretas e de homens e mulheres. Teoricamente o algoritmo deveria fazer as escolhas de maneira igualitária,

sem favorecer nenhum aspecto, mas o que de fato aconteceu foi que o algoritmo mostrou 7% mais fotos de mulheres brancas em relação amulheres negras e, entre os homens, a diferença foi de 2%. Além disso, o algoritmo destacou 8% mais as fotos de mulheres do que de homens. Diante do ocorrido, o Twitter respondeu que o erro apontado pelos usuários serviu para desenvolver melhorias no sistema.

Visando evitar esse tipo de problema, a LGPD tratou desse assunto em seu artigo 20, possibilitando que o titular pudesse solicitar a revisão de decisões tomadas exclusivamente com base no tratamento de dados automatizado, obrigando o controlador a fornecer as informações sobre os critérios e procedimentos utilizados para a tomada de decisão, caso seja solicitado e, se a solicitação não for aceita é possível ainda a realização de uma auditoria para verificar a existência de aspectos discriminatórios no tratamento de dados automatizados, vedado pelo artigo 6º, inciso IX da lei.

O artigo 21 da LGPD reforça o ideal de não utilizar os dados pessoais em prejuízo aos seus titulares, informando que: “os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo” (Brasil, 2018).

Por fim, o artigo 22 da Lei Geral de Proteção de Dados menciona as formas de tutela dos interesses e dos direitos dos titulares. Expondo que: “Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.”

Em síntese, a LGPD conferiu ao titular dos dados uma série de direitos que, em sua maioria, se correlacionam com a autodeterminação informativa e a proteção de seus interesses individuais, complementando e reforçando direitos já existentes em outros diplomas de leis. Ademais, estipulou obrigações para os agentes de tratamento, criando um arcabouço robusto para a proteção do indivíduo e de seus dados na internet.

Ainda assim, é imprescindível que se faça um estudo sobre os métodos de armazenamento de dados e os cuidados e medidas de proteção que deverão ser observados.

4.4 Como Será Feito o Armazenamento de Dados e Quais Cuidados e Medidas de Proteção Deverão Ser Observados

O armazenamento de dados é de fundamental importância para qualquer pessoa, seja ela física ou jurídica, de direto privado ou público, que realize ou não o tratamento de dados. Isso porque, na atualidade, as pessoas e empresas necessitam dos dados para realizar tarefas diárias. Por exemplo, uma pessoa pode consultar sua agenda de contatos em seu celular de maneira rápida e simples caso precise fazer uma ligação de emergência, assim como uma empresa pode consultar em seu banco de dados as informações de um cliente ou parceiro comercial caso precise se comunicar com ele. Essas tarefas são possíveis graças ao armazenamento de dados.

No entendimento de G Somasundaram e Alok Shrivastava:

> Dados criados por indivíduos ou empresas devem ser armazenados a fim de que sejam facilmente acessados para posterior processamento. Em um ambiente computacional, dispositivos projetados para armazenar dados são chamados de dispositivos de armazenamento. O tipo de armazenamento usado varia de acordo com os tipos de dados e a velocidade em que são criados e usados. Dispositivos como a memória de um telefone celular ou câmera digital, DVDs, CD-ROMs e discos rígidos em computadores pessoais são exemplos de dispositivos de armazenamento (2011, p.27).

Fato é que o armazenamento de dados é muito importante e tem sido utilizado de maneira cada vez mais frequente com o passar dos anos, mas como é o processo de armazenamento de dados ?

Antes da utilização de computadores para o armazenamento de dados, os meios existentes para realizar essa tarefa se limitavam a papeis e arquivos físicos, o que resultava em uma árdua tarefa para organizar e extrair informações desses meios.

Com o avanço da tecnologia, os meios de armazenamento evoluíram e, atualmente, os arquivos e informações podem ser digitalizados e armazenados em dispositivos físicos ou digitais como a “nuvem”, sendo esse um modelo de computação que armazena dados na internet por meio de provedores. Esses dados, que antes eram físicos, passam agora a serem dados digitais.

Os dados digitais, por sua vez, são disponibilizados na internet pelo usuário ou coletados através de aplicativos desenvolvidos para isso, e são direcionados a um banco de dados que possui um “sistema de gerenciamento de

banco de dados", responsável organizar e estruturar os dados recebidos, facilitando a consulta e utilização deles. Logo após, esse mesmo sistema faz a leitura e armazenamento desses dados em discos físicos do "storage array", que é um dispositivo de armazenamento de dados a longo prazo. O conjunto desses dispositivos e servidores, responsáveis pela coleta e armazenamento de dados, de uma empresa é conhecido como "Data Center".

Devido a esse novo contexto de armazenamento de dados em dispositivos eletrônicos e sistemas digitais, surgem novos desafios para que esses métodos se mostrem eficazes no longo prazo, por exemplo, o crescimento exponencial das informações na internet e a vida útil dos dados e informações coletados.

A vida útil dessas informações, também é chamada de "ciclo de vida da informação". Quando os dados são criados ou coletados, em um primeiro momento aquela informação é muito útil e valiosa, mas à medida que o tempo passa essas informações perdem o valor, visto que ficam desatualizadas e menos úteis. Entender como funciona esse ciclo de vida da informação é muito importante e pode ajudar as empresas na implementação de sistemas de coleta e armazenamento eficazes e condizentes com a finalidade prevista.

G Somasundaram e Alok Shrivastava, aduzem que:

> As empresas modernas precisam que seus dados estejam protegidos e disponíveis em tempo integral. Os data centers podem conseguir isso com o uso otimizado e apropriado da infraestrutura de armazenamento. Uma política eficaz de gerenciamento de informações é necessária para dar suporte a esta infraestrutura e potencializar seus benefícios.
> O gerenciamento do ciclo de vida da informação (ILM, Information Lifecycle Management) é uma estratégia pró-ativa que permite a uma organização de TI gerenciar de modo eficaz os dados por todo o seu ciclo de vida, baseada em políticas de negócio preestabelecidas (2011, p.34).

O sistema de ILM está totalmente interligado com a proposta da LGPD em exclusão de dados que já atingiram sua finalidade, dado que, visando a máxima eficiência e utilidade, o gerenciamento do ciclo de vida da informação propõe que ao ser coletado o dado, será feita uma análise e extraída as informações úteis para o agente de tratamento. Feito isso, para não ocupar espaço nos dispositivos de armazenamento de um data center, aquele dado deverá ser excluído do sistema quando não tiver mais finalidade, como disposto no artigo 15 da Lei Geral de Proteção de Dados.

A exclusão dos dados ocorre como uma medida de segurança para evitar o acesso ilegal de qualquer um à essas informações. A LGPD, em seu capítulo VII, tratou da segurança e das boas práticas de governança, com o intuito de tornar o tratamento de dados mais seguro e confiável.

O artigo 46 da lei, dispõe que:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Em complemento ao artigo 46, o artigo 47 informa que “Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.” (Brasil, 2018). Dessa forma, os agente de tratamento ou qualquer outra pessoa que tenha participado em algum momento do tratamento dos dados, ficam responsabilizados por protege-los desde o início do tratamento até depois do término da operação, devendo seguir as normas e padrões de segurança impostos pela Autoridade Nacional.

Em caso de algum incidente de segurança que afete os titulares dos dados, os agentes de tratamento devem comunicar o titular e a Autoridade Nacional, conforme o artigo 48 da LGPD, segundo o qual:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
> I - a descrição da natureza dos dados pessoais afetados;
> II - as informações sobre os titulares envolvidos;
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV - os riscos relacionados ao incidente;

> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
> I - ampla divulgação do fato em meios de comunicação; e
> II - medidas para reverter ou mitigar os efeitos do incidente.
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Para evitar que tais incidentes ocorram, o artigo 49 da LGPD exige que “ Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.” (Brasil, 2018).

A Lei Geral de Proteção de Dados, além de tratar da segurança e do sigilo dos dados, abordou também a questão sobre Boas Práticas e Governança, na Seção II, Capítulo VII, atuando em uma relação simbiótica com a seção I do mesmo capítulo. Essa relação que ocorre entre a seção I e II é extremamente benéfica para o titular dos dados, pois obriga os agentes de tratamento a buscarem um padrão de qualidade alto tanto no tratamento de dados, quanto no ambiente corporativo da empresa que o realizará.

O artigo 50 da Lei Geral de Proteção de Dados dispõe que:

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

É nítida a relação que o artigo possui com a prática do *Compliance*, sendo um conjunto de medidas adotadas pela empresa a fim de evitar fraudes e ilegalidades no ambiente corporativo, além de auxiliar na organização e no cumprimento de leis e normas exigidas para realização de determinada atividade.

Dessa forma o artigo 50 permite que os agentes de tratamento formulem regras de boas práticas, organização, funcionamento e procedimentos que atendam as solicitações dos titulares, as normas de segurança, e outras medidas, visando sempre a segurança dos dados pessoais, de seus titulares e do ambiente digital como um todo. Possibilitando a criação e proliferação de novos paradigmas que contribuem para o desenvolvimento da proteção jurídica digital.

O §1º orienta os agentes de tratamento durante a criação dessas novas regras, de modo que: “ Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.” (Brasil, 2018). Garantindo assim a qualidade e seriedade necessárias para a criação de regras eficazes e gerem resultados positivos no curto e longo prazo. Esse objetivo também é visado pelo §2º do artigo 50 da LGPD, o qual discorre que:

> § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
> I - implementar programa de governança em privacidade que, no mínimo:
> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
> g) conte com planos de resposta a incidentes e remediação; e
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
> II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

Todas essas exigências fazem com que as empresas e agentes de tratamento adotem uma postura integra e ética para com os titulares, evitando a

criação de programas ineficazes e sem utilidade, que não geram resultados no plano fático, onde a mudança necessita ocorrer.

Por fim, o artigo 51 da LGPD, brevemente relata que a Autoridade Nacional de Proteção de Dados deverá estimular a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais, garantindo mais uma vez o direito à autodeterminação no tratamento de dados, previsto pelo artigo 2º e artigo 18 da lei.

Superada a análise das limitações impostas pela Lei Geral de Proteção de dados, incluindo o estudo dos tipos e formas de coletas dos dados, bem como os direitos conferidos aos titulares através dessa legislação, cabe agora realizar um exame acerca das responsabilidade impostas pela lei em decorrência do descumprimento da LGPD.

5 RESPONSABILIZAÇÃO E PENALIDADES IMPOSTAS PELO MAU USO E ARMAZENAMENTO DOS DADOS PESSOAIS

Como mencionado anteriormente, a Autoridade Nacional de Proteção de Dados (ANPD) ficará responsável pela aplicação das sanções previstas na Lei Geral de Proteção de Dados, conforme artigo 55-K da lei.

Nesse sentido, as violações praticadas pelos agentes de tratamento, quais sejam o operador e o controlador de dados, dispostos entre os artigos 42 a 45 na Seção III, Capítulo VI da Lei, serão investigados e punidos pela ANPD. Portanto é

de extrema importância que se faça um estudo sobre os crimes passíveis de responsabilidade existente nesse diploma de lei.

Iniciando a análise dos crimes, o artigo 42 da LGPD esclarece de maneira objetiva que:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

É importante destacar, além da obrigação de reparação dos dados causados pelos agentes de tratamento ao titular, que o operador responderá solidariamente pelo dano quando descumprir obrigação imposta pela lei ou quando não acatar as instruções lícitas impostas pelo controlador, equiparando-se a ele. Da mesma forma, caso o controlador esteja diretamente envolvido no tratamento de dado que ocasionou dano ao titular, este responderá solidariamente junto ao operador.

Facilmente pode-se vislumbrar a correlação com o instituto da responsabilidade civil nestas hipóteses. Discorrendo brevemente sobre as modalidades de responsabilidade civil, pode-se dizer que a responsabilidade civil subjetiva é aquela quando há a necessidade de comprovação do dano e a existência do nexo causal entre a conduta e a lesão, além da culpa do agente que causou o dano. De outro modo, a responsabilidade objetiva, adotada pelo Código de Defesa

do Consumidor, é aquela onde não é preciso que se prove a culpa do agente, sendo necessário a comprovação apenas do dano e do nexo causal.

A LGPD não abordou de forma clara qual regime de responsabilidade adotado. Entretanto, a doutrina vislumbra ambas as hipóteses de responsabilidade, tanto a objetiva quando se tratar de relações de consumo, tendo forte influência do Código de Defesa do Consumidor, quanto a subjetiva quando se trata de relações civis, tendo forte influência do Código Civil

Outro aspecto importante, mencionado no artigo 42, §2º, diz respeito a inversão do ônus da prova. Isso ocorre porque os agentes de tratamento possuem uma vantagem probatória perante os titulares que são considerados como hipossuficientes nessa relação, já que os agentes de tratamento controlam seus dados e, portanto, detém eventuais provas de danos em sob sua guarda.

Em adição, a LGPD admite a possibilidade de dano coletivo, como mencionado no §3º do artigo 42. Dano coletivo se traduz em uma lesão a moral e aos valores essenciais de uma sociedade, como, por exemplo, veiculação de propagandas abusivas. Nas palavras de acordo com Rui Stoco:

> O dano moral coletivo é a injusta lesão da esfera moral de uma dada comunidade, ou seja, é a violação antijurídica de um determinado círculo de valores coletivos. Quando se fala em dano moral coletivo, está-se fazendo menção ao fato de que o patrimônio valorativo de uma certa comunidade (maior ou menor), idealmente considerado, foi agredido de maneira absolutamente injustificável do ponto de vista jurídico; quer isso dizer, em última instância, que se feriu a própria cultura, em seu aspecto imaterial.

A LGPD permite que a reparação dos danos coletivos seja feita por meio judicial com uma única demanda que satisfaça o interesse da coletividade. Essa demanda pode ser proposta por Associações, Defensoria Pública e Ministério Público, sendo aplicáveis as normas de ação coletiva, como o Código de Defesa do Consumidor, em seu artigo 81, e a Lei de Ação Civil Pública, em seu artigo 1º inciso IV.

Em contra partida, existem casos em que os agentes de tratamento não serão responsabilizados por danos ao titular em virtude do tratamento. Esses casos estão presentes no artigo 43 da lei, segundo o qual:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Essas possibilidades de exclusão de responsabilidade ocorrem devido à quebra do nexo causal entre a conduta dos agentes de tratamento e o dano suportado pelo titular.

O inciso I é simplista e óbvio, ao mesmo tempo que é necessário, pois, ao isentar o agente de tratamento da responsabilidade do dano sofrido pelo titular em virtude de tratamento não realizado por ele, impediu que o agente de tratamento carregasse um fardo excessivo e injusto no desempenho de sua função, protegendo-o acerca de eventuais conflitos sem fundamentos entre o titular, ANPD e os agentes de tratamento, visto que não existiria qualquer nexo causal entre a conduta do agente e o dano sofrido pelo titular.

O inciso II, assim como o I, evitou que o agente sofresse uma responsabilização exacerbada, vez em que, o controlador ou operador agiu conforme disposto em lei, seguindo todos os protocolos e exigências, não existindo motivo então para que fosse responsabilizado por eventual dano ao titular. Entretanto, se os agentes de tratamento e o titular dos dados não são responsáveis pelo dano causado. Quem responderia pelo dano ? Nesse caso, incumbiria a Autoridade Nacional de Proteção de dados a tarefa de examinar a situação e aplicar a sanção devida ao responsável pelo dano, conforme estipula o artigo 55-J, inciso IV da Lei Geral de Proteção de Dados.

O inciso III destaca que somente não haverá responsabilidade do agente no caso de culpa exclusiva do titular ou de terceiros, ou seja, em casos de culpa concorrente, o agente de tratamento responsável não terá o benefício da exclusão de responsabilidade, devendo responder pelos danos causados de maneira proporcional a sua parcela de responsabilidade. Dessa forma, o que ocorre é apenas uma atenuação da culpa do agente responsável e do valor a ser pago como indenização ao titular, como dispõe o artigo 945 do Código Civil. No caso da culpa exclusiva do titular, esta pode ocorrer por ato ou omissão do mesmo, por exemplo, quando deixa sua conta pessoal de redes sociais logadas em computadores de acesso público, por negligência.

No caso de culpa exclusiva de terceiros, esse terceiro deve ser pessoa física ou jurídica estranha a relação entre controlador, operador e titular, não podendo ser representante ou preposto do agente de tratamento pois, em analogia com o Código de Defesa do Consumidor, em seu artigo 34, o fornecedor de serviço (que no caso seria o agente de tratamento) responde solidariamente pelos atos de seu preposto ou representante autônomo.

Por sua vez, o artigo 44 da Lei nº 13.709/2018 definiu quando seria considerado irregular o tratamento de dados e, por consequência, haveria a responsabilização dos agentes de tratamento e de terceiros que contribuíram para a ocorrência do dano moral ou patrimonial ao titular. Nas letras do artigo supra citado:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Dessa forma, a exclusão de responsabilidade prevista no artigo 43 não incidiria em casos de tratamento irregular, pois, ao deixar de observar o todos os requisitos e exigências dispostos na lei, os agentes de tratamento facilitam a invasão dos sistemas de segurança e permitem que os dados sejam violados.

Após o entendimento das hipóteses de responsabilização dos agentes de tratamento, do titular, e até mesmo de terceiros. É pertinente que seja realizado um estudo acerca das penalidades impostas pelo meu uso e armazenamento dos dados.

5.2 Sanções Impostas Pelo Mau Uso e Armazenamento de Dados

As sanções para aqueles que estão em desacordo com a Lei nº 13.709/2018 passaram a vigorar a partir do dia 01 de agosto de 2021. Tais medidas serão aplicadas pela Autoridade Nacional de Proteção de Dados, como já exposto no artigo 55-J, inciso IV.

O Capítulo VIII, Seção I da Lei Geral de Proteção de Dados, dispõe sobre as sanções administrativas e, cabe dizer que, independente do seguimento ou do tamanho da empresa, está deverá se adequar as exigências da Lei. Nesse sentido, o artigo 52 da LGPD explica que:

> 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; (Incluído pela Lei nº 13.853, de 2019)
> 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; (Incluído pela Lei nº 13.853, de 2019)
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Interessante notar que as sanções aplicáveis vão desde penalidades leves, como uma advertência, até penalidades mais pesadas que envolvem multas e proibição do tratamento de dados, podendo gerar grandes prejuízos para as empresas.

Além disso, é possível que a ANPD torne pública a infração cometida pelos agentes de tratamento, o que retoma o princípio da autodeterminação informativa do titular e do direito à informação e transparência no tratamento de dados, possibilitando que o titular tenha conhecimento das práticas que determinada empresa realiza e do quão seguro seus dados estão sob tratamento daquela empresa, facultando-lhe a decisão de deixar que seja realizado o tratamento de seus dados por ela. Isso implica em um efeito indireto, pois, escândalos relacionados ao tratamento de dados de uma empresa influenciam de maneira totalmente negativa sobre sua imagem, que é muito importante para a captação de clientes e, visando

evitar que qualquer infração possa “manchar a reputação da empresa”, ela mesmo se autofiscaliza para evitar maiores problemas.

Outro ponto muito importante, diz respeito ao bloqueio do tratamento de dados referente a infração cometida, o que assegura aos titulares uma política de redução de danos, ao passo que, assim que a ANPD for notificada sobre a irregularidade no tratamento, essa poderá bloquear, e até mesmo eliminar os dados pessoais a que se refere a infração antes que o titular possa a vir sofrer algum dano.

Dando continuidade, o §1º do artigo 52 da LGPD informa sobre as aplicações das sanções administrativas, no qual:

> § 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.

Compreende-se a partir da leitura do §1º que o legislador optou por permitir que a ANPD fizesse um juízo de proporcionalidade entre a gravidade da falta e a sanção posta sobre o fato cometido pelos agentes de tratamento. Responsabilizando-os não apenas de maneira objetiva, mas analisando os aspectos subjetivos da violação cometida por eles, como a boa-fé do infrator e a sua cooperação para reverter os danos.

Dessa forma, em casos de reincidência, em que o infrator comete ilícitos para auferir vantagem indevida, em benefício próprio ou de terceiros, juntamente com a falta de adoção de medidas de segurança e de boas práticas de governança e outros critérios a serem avaliados pela ANPD, a sanção a ser aplicada ao agente infrator pode ser mais severa do que quando o agente de tratamento prática o inverso, recebendo assim uma penalidade mais branda.

A intenção em penalizar os agentes de tratamento e as empresas conforme os itens listados no caput do artigo 52, encontra fundamento no §6º do artigo 52, o qual menciona:

> § 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.

Sendo assim, as penalidades mais graves serão aplicadas quando já tiver sido aplicada alguma outra sanção, como as dos incisos II, III, IV, V e VI, ou quando os agentes de tratamento estiverem submetidos a outros órgãos que tem competência para julgar as infrações cometidas por eles.

Os parágrafos 2º e 3º do artigo 52, por sua vez, abordam a questão de aplicação de penalidades dispostas em outros diplomas de lei. Segundo o qual:

> § 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.
> § 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.

Por tanto, admite-se a possibilidade da utilização de outros diplomas de lei na aplicação de sanções administrativas, civis e penais pelos crimes cometidos previstos na Lei Geral de Proteção de Dados, reforçando a ideia de que a LGPD apresenta um microssistema jurídico que abarca diversas áreas do saber na sua composição, como menciona Cíntia Rosa Pereira de Lima:

> Ademais, a coleta e o tratamento de dados pessoais passaram a ser atividades do cotidiano, sem que a comunidade brasileira fosse alertada dos seus perigos e potenciais riscos. Neste sentido, a LGPD inaugura um microssistema jurídico destinado à proteção de dados, que é um direito humano já assegurado na Carta de Direitos Humanos da União Europeia, e que, em breve, será um direito e garantia fundamental como preconiza a PEC 17/2019.

Em adição, o §4º aduz que:

> § 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.

Sendo assim, nos casos em que não for possível para a ANPD definir o valor exato do faturamento de uma empresa, seja por desconhecimento sobre o ramo em que a apresa atua ou por valores apresentados pela empresa de forma errônea, a ANPD poderá fixar um valor estimado para aplicação da multa estipulada no inciso II do artigo 52.

O §5º refere-se à destinação dos valores coletados através das sanções aplicadas. Segundo ele: “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.” (Brasil, 2018).

De acordo com o Ministério da Justiça e Segurança Pública, o Fundo de Defesa de Direitos Difusos tem a seguinte função:

> O Fundo de Defesa de Direitos Difusos - FDD, criado pela Lei nº 7.347, de 24 de julho de 1985, tem por finalidade a reparação dos danos causados ao meio ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico, paisagístico, por infração à ordem econômica e a outros interesses difusos e coletivos.

Visando, portanto, o bem comum e a reparação de danos sofridos pela sociedade de maneira coletiva.

O §7º aborda uma hipótese importante para resolução de conflitos entre os agentes de tratamento e titulares dos dados sem que seja necessário o envolvimento de ANPD ou outro órgão que regule essa relação. Nele está exposto:

> § 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.

Em casos particulares que envolvam vazamento de dados individuais ou acessos não autorizados, é facultado ao titular a conciliação direta com os agentes de tratamento, tornando a solução do conflito mais rápida, fácil e menos

custosa, como acontece em litígios civis, onde o Código de Processo Civil permite que as partes façam acordos particulares para resolução do conflito.

O artigo 53 menciona os procedimentos para definir sobre as sanções administrativas a infração da LGPD. Nele está transcrito o seguinte:

> Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.
> § 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.
> § 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Sendo assim, a ANPD fica encarregada de definir as sanções que serão aplicadas em caso de descumprimento da Lei. Além disso, deverá preceder uma consulta pública, conferindo a participação da população no processo de elaboração das metodologias e penalidades, que deverão ser apresentadas para os agentes de tratamento, informando-lhes sobre todos os elementos contidos no regulamento de maneira clara e objetiva.

Por fim, o artigo 54 da Lei trata sobre a aplicação da multa diária, no qual:

> Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.
> Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.

Confirmando mais uma vez a tese de que os agentes de tratamento serão responsabilizados de acordo com a parcela de dano que causarem.

5 CONCLUSÃO

Ante as premissas extraídas ao longo da investigação científica, fica evidente a necessidade e a importância de uma legislação específica para a

proteção de dados não só no Brasil, mas nos países do mundo inteiro. Isso porque as inovações tecnológicas e as mudanças de estilo de vida dos seres humanos, apontam para o aumento da utilização da internet e dos dispositivos eletrônicos na sociedade, o que consequentemente exige que esse meio seja regido por leis e seja fiscalizado constantemente para que não haja um retrocesso dos direitos e garantias conquistados com tanto esforço e empenho ao longo dos anos e que se aplicam na vida cotidiana, devendo ser transportados para esse meio digital evitando conflitos de quaisquer natureza.

Nesse sentido, a LGPD foi uma novidade legislativa que se mostrou bastante satisfatória até o momento. Devido a influência que sofreu de diversos diplomas de leis espalhados pelo mundo e que se mostraram eficazes ao longo do tempo, a Lei 13.709/2018 torna-se o reflexo de legislações nacionais como a Lei de Acesso à Informação, o Marco Civil da Internet, o Código de Defesa do Consumidor e o Código Civil, bem como de legislações internacionais, como o Ator de Proteção de Dados de Hesse, a Diretiva 95/46/CE da União Europeia e o General Data Protection Regulation (GDPR), entre outros. Devido as diversas influências internas e externas que a LGPD recebeu, sua formatação final se mostrou bastante adequada para os padrões de qualidade de proteção de dados nacionais e internacionais, resultando em uma conquista legislativa importante e um avanço na proteção de dados no Brasil.

Devido a sua complexidade, inerente ao próprio tema de dados pessoais e tecnologia, a Lei Geral de Proteção de Dados tomou certo cuidado ao tratar do tema, tentando ser explicativa e didática. No estudo dessa legislação, foi possível elencar a existência de três tipos principais de dados, sendo eles os dados pessoais propriamente ditos, os dados pessoais sensíveis e os dados pessoais anonimizados. Esses três tipos principais se subdividem respectivamente em dados públicos, dados pessoais de crianças e adolescentes e dados pseudominizados.

Destacando a importância dos dados pessoais sensíveis e os dados pessoais de crianças e adolescentes, que recebem tratamento diferenciado em virtude de suas características, uma vez que, os dados pessoais sensíveis podem ser motivo de discriminação para seu titular e, por isso, possuem requisitos extras para ter seu acesso permitido. O mesmo ocorre com os dados pessoais de crianças e adolescentes pois, como o titular desses dados é menor de idade, ele apresenta

vulnerabilidades que podem colocar suas garantias fundamentais em risco. Dessa forma, esse grupo recebe uma maior proteção da LGPD.

Outro ponto importante abordado é a maneira como os dados são coletados. Existem inúmeras maneiras de coletar dados atualmente, podendo essa coleta ser realizada de maneira offline, ou seja, sem internet, o que implica em uma dificuldade um pouco maior para realização dessa coleta, ou de maneira online na qual a variedade de maneiras e técnicas para coleta de dados é surpreendente. Cabe ressaltar que, como a internet e os meios tecnológicos estão em constante desenvolvimento, é impossível esgotar todos os meios de coleta de dados, até porque novos modos de coleta de dados serão desenvolvidos com o passar dos anos.

Em adição, o estudo do armazenamento de dados e das medidas de segurança utilizadas para sua proteção se mostrou muito interessante. Foi possível perceber a evolução dos meios de armazenamento de dados, que passaram de fichas e anotações em papeis para armazenamento em dispositivos físicos como CDs, pendrives e, posteriormente, para meios digitais como armazenamento em nuvem, o que confere uma velocidade superior e mais segurança na guarda dos dados, em comparação aos meios utilizados no passado.

Ademais, não se pode ignorar a notoriedade do principal enfoque da Lei Geral de Proteção de Dados, o titular. O titular dos dados é aquele que recebe a proteção e garantias dessa lei devido a presunção de sua hipossuficiência em relação aos agentes de tratamento. Nota-se nesse ponto diversas semelhanças com o Código de Defesa do Consumidor, que o trata como hipossuficiente em relação ao fornecedor de produtos e serviços.

De um lado, o titular de dados é protegido pela LGPD, de outro, a LGPD exige dos agentes de tratamento uma série de requisitos e deveres para que eles possam exercer sua função. Garantindo sempre a proteção dos interesses dos titulares e de seus dados.

Entretanto, existem casos em que a lei isenta os agentes de tratamento da responsabilização pelos danos, por exemplo quando eles não realizaram o tratamento de dados pessoais, quando não houve violação da LGPD durante o tratamento ou quando a culpa pelo dano é exclusiva de titular ou terceiro. Doutro modo, as empresas e agentes de tratamento que não estiverem em conformidade com a lei ou violarem o disposto nela, serão responsabilizados na medida da

violação e do dano causado ao titular, recebendo penalidades mais brandas como advertência para adoção de medidas corretivas, ou penalidades mais graves como a suspensão do exercício da atividade de tratamento de dados. destacando nessas hipóteses a importância da Autoridade Nacional de Proteção de Dados, que fica encarregada da fiscalização e aplicação das penalidades previstas no código ao agentes e empresas.

Por todo exposto, fica evidente que a LGPD é uma legislação que, apesar de ser muito bem redigida e atender a maioria das necessidades atuais do Brasil e ao padrão de qualidade esperado por outros países, ela passará por inúmeras mudanças, o que exige dos legisladores, doutrinadores, estudiosos e até mesmo dos cidadãos, estudo e entendimento básico sobre o tema para que possam realizar as alterações necessárias da maneira mais assertiva o possível e exigir dos agentes de tratamento e dos órgãos fiscalizadores o cumprimento da lei e proteção dos direitos e interesses da sociedade. um grau de atenção maior para as alterações que virão a seguir.

REFERÊNCIAS

ACADEMIA NOTARIAL BRASILEIRA. “A LGPD inaugura um microssistema jurídico destinado à proteção de dados”. **Academia Notarial Brasileira**, s.p, 20 jan. 2020. Disponível em: https://academianotarial.org.br/noticias/lgpd-inaugura-um-microssistema-juridico-destinado-protecao-de-dados. Acesso em: 3 nov. 2021.

ALEMANHA. **Hessisches Datenschutzgesetz (HDSG)**. Disponível em: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/HDSG.pdf. Acesso em: 01 nov. 2021.

ASSIS E MENDES ADVOGADOS. **HISTÓRICO das leis de proteção de dados e da privacidade na internet**. 15 jun. 2020. Disponível em: https://assisemendes.com.br/historico-protecao-de-dados/. Acesso em: 1 nov. 2021.

BABO, Gustavo Schainberg S. **Discriminação Algorítmica:** Origens, Conceitos e Perspectivas Regulatórias. 15 jun. 2020. Disponível em: https://www.dtibr.com/post/discrimina%C3%A7%C3%A3o-algor%C3%ADtmica-origens-conceitos-e-perspectivas-regulat%C3%B3rias-parte-1. Acesso em: 3 nov. 2021.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. **Comentários à Constituição do Brasil.** vol. 2, São Paulo: Saraiva, 1989.

BATISTA, Adonis. **Você sabe o que são cookies na internet? Conheça os 3 tipos**. 21 jan. 2019. Disponível em: https://blog.hariken.co/voce-sabe-o-que-sao-cookies-na-internet-conheca-os-3-tipos/. Acesso em: 3 nov. 2021.

BITTAR FILHO, Carlos Alberto. **Do dano moral coletivo no atual contexto jurídico brasileiro**. Jus. 2005. Disponível em: https://jus.com.br/artigos/6183/do-dano-moral-coletivo-no-atual-contexto-juridico-brasileiro. Acesso em: 3 nov. 2021.

BMA Advogados. **A PORTABILIDADE DE DADOS PESSOAIS NA LGPD E SUAS IMPLICAÇÕES**. 30 mar. 2020. Disponível em: https://www.bmalaw.com.br/conteudo/protecao-de-dados-tecnologia-e-negocios-digitais/a-portabilidade-de-dados-pessoais-na-lgpd-e-suas-implicacoes. Acesso em: 3 nov. 2021.

BRASIL. Decreto nº 10.474, de 26 de agosto de 2020. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. **DECRETO Nº 10.474, DE 26 DE AGOSTO DE 2020**: seção 1, Brasília, DF: Diário Oficial da União, 27 ago. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226. Acesso em: 26 mai. 2021.

BRASIL. **Decreto-Lei 2.848, de 07 de dezembro de 1940**. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940.

BRASIL. Lei 8.069, de 13 de julho de 1990. Dispõe sobre o **Estatuto da Criança e do Adolescente** e dá outras providências. Diário Oficial da União, Brasília, 16 jul. 1990.

BRASIL. **Lei Geral de Proteção de Dados**. Disponível em: https://www.tjsp.jus.br/LGPD/LGPD/ALGPD#:~:text=No%20%C3%A2mbito%20da%20LGPD%2C%20o,ao%20tratamento%20de%20dados%20pessoais.. Acesso em: 28 mai. 2021.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações. **Lei de Acesso à Informação**, Brasília, DF, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 28 out. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.**: seção 1, Brasília, DF: Diário Oficial da União, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 mai. 2021.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Código de Defesa do Consumidor**, Brasília, DF, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 28 out. 2021.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. 24 abr. 2014.

ESTADOS UNIDOS. **Data Protection Authority**. Disponível em: https://iapp.org/resources/article/data-protection-authority/. Acesso em: 28 mai. 2021.

FALKVINGE, Rick. Brasil Desperdiça Chance de Exercer Influência Geopolítica; Mata o Projeto de Lei do Marco Civil da Internet em Fiasco Político. **Falkvinge On Liberty**, 21 nov. 2012. Disponível em: https://falkvinge.net/2012/11/21/brasil-desperdica-chance-de-exercer-influencia-geopolitica-mata-o-projeto-de-lei-do-marco-civil-da-internet-em-fiasco-politico/. Acesso em: 27 out. 2021.

INTELIGOV. **LGPD e Lei de Acesso à Informação**. 1 dez. 2020. Disponível em: https://blog.inteligov.com.br/lgpd-e-lai/. Acesso em: 28 out. 2021.

KHOURI, Paulo R. Roque A. O problema do consentimento informado na Lei Geral de Proteção de Dados Pessoais. **Revista Consultor Jurídico**. 31 mar. 2021.

Disponível em: https://www.conjur.com.br/2021-mar-31/garantias-consumo-problema-consentimento-informado-lgpd. Acesso em: 1 jun. 2021.

KOETSIER, Jhon. **Top 10 Apps By Downloads And Revenue Q2 2021:** Report. Forbes, 15 jul. 2021. Disponível em: https://www.forbes.com/sites/johnkoetsier/2021/07/15/top-10-apps-by-downloads-and-revenue-q2-2021-report/?utm_campaign=forbes&utm_source=twitter&utm_medium=social&utm_term=Carrie&sh=34527cd93295. Acesso em: 4 nov. 2021.

Lima, Cíntia Rosa Pereira D. **Comentários à Lei Geral de Proteção de Dados**. Grupo Almedina (Portugal), 2020. 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 03 Nov 2021.

LOBO, Hewdy. **O que é vício de consentimento?**. Jus. 15 out. 2015. Disponível em: https://jus.com.br/artigos/43994/o-que-e-vicio-de-consentimento. Acesso em: 3 nov. 2021.

Lotame. **What Are the Methods of Data Collection?**. 13 maio 2019. Disponível em: https://www.lotame.com/what-are-the-methods-of-data-collection/. Acesso em: 3 nov. 2021.

LOURENÇO, Patrícia Ribeiro. LGPD e Direito do Consumidor: impactos e influências. **Microservice**. [2020]. Disponível em: https://www.microserviceit.com.br/lgpd-e-direito-do-consumidor/. Acesso em: 27 out. 2021.

MATOS, Thiago Farina. Comércio de dados pessoais, privacidade e Internet. **Revista de Doutrina da 4ª Região**. n. 7, s.p, 18 jul. 2005. Disponível em: https://core.ac.uk/download/pdf/16049789.pdf. Acesso em: 3 nov. 2021.

MEDEIROS, Erick Felipe. **Responsabilidade Civil segundo a LGPD**. Migalhas, 6 jul. 2021. Disponível em: https://www.migalhas.com.br/depeso/348113/responsabilidade-civil-segundo-a-lgpd. Acesso em: 3 nov. 2021.

MINISTÉRIO DA EDUCAÇÃO. **Sobre a Lei de Acesso à Informação**. Disponível em: https://www.gov.br/capes/pt-br/acesso-a-informacao/servico-de-informacao-ao-cidadao/sobre-a-lei-de-acesso-a-informacao. Acesso em: 27/10/2021.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Fundo de Defesa de Direitos Difusos**. [entre 2000 e 2021]3. Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/perguntas-frequentes/consumidor/fundo-de-defesa-de-direitos-difusos. Acesso em: 3 nov. 2021.

MINISTÉRIO DAS COMUNICAÇÕES. **Pesquisa mostra que 82,7% dos domicílios brasileiros têm acesso à internet**: Dados são referentes a 2019 e representam um crescimento de 3,6 pontos percentuais em relação a 2018. Portal do Governo Brasileiro, 14 abr. 2021. Disponível em: https://www.gov.br/mcom/pt-

br/noticias/2021/abril/pesquisa-mostra-que-82-7-dos-domicilios-brasileiros-tem-acesso-a-internet. Acesso em: 4 nov. 2021.

OLIVEIRA, José Eduardo da Silva. **RESPONSABILIDADE CIVIL DOS AGENTES DE PROTEÇÃO DE DADOS NO BRASIL**. Orientador: Adriano Marteleto Godinho. 2019. 50 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade Federal da Paraíba. 2019. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/16584/1/JESO04102019.pdf. Acesso em: 3 nov. 2021.

PECK, P. **Proteção de dados pessoais**. São Paulo: Editora Saraiva, 2020. 9788553613625. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553613625/. Acesso em: 26 mai. 2021.

REINALDO FILHO, D. **A Diretiva Europeia sobre proteção de dados pessoais**: uma análise de seus aspectos gerais, fev. 2013. Disponível em: https://jus.com.br/artigos/23669/a-diretiva-europeia-sobre-protecao-de-dados-pessoais. Acesso em: 05 nov. 2021.

SANTANA, Lucas. **Algoritmo racista:** Twitter detalha como sua IA privilegia brancos em fotos. Out, 20 maio 2021. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/05/20/twitter-detalha-como-seu-algoritmo-privilegia-pessoas-brancas-em-fotos.htm. Acesso em: 3 nov. 2021.

SBCOACHING. **Big Data:** O que é, Para que serve e Exemplos práticos. [2020]. Disponível em: https://www.sbcoaching.com.br/big-data/. Acesso em: 11 ago. 2021.

SERPRO. **O que são dados pessoais, segundo a LGPD**. [2020]. Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-pessoais-lgpd. Acesso em: 3 nov. 2021.

SOARES, Fernando. **O Big Data e o seu uso na saúde**. 15 nov. 2016. Disponível em: https://blog.cmtecnologia.com.br/big-data-saude/. Acesso em: 1 nov. 2021.

SOMASUNDARAM, G.; SHRIVASTAVA, A.; SERVICES, E.E. **Armazenamento e Gerenciamento de Informações**. Grupo A, 2011. 9788577807642. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788577807642/. Acesso em: 03 Nov 2021.

TEIXEIRA, Ilderlândio. **LGPD e LAI**: uma análise sobre a relação entre elas. Portal do Governo Brasileiro. 30 mar. 2020. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/lei-acesso-informacao-lai-lei-geral-protecao-dados-pessoais-lgpd. Acesso em: 28 out. 2021.

UNIÃO EUROPEIA. **Diretiva 95/46/CE**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046. Acesso em 28 out. 2021.

UNIÃO EUROPEIA. **Diretivas da União Europeia**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al14527. Acesso em 28 out. 2021.

UNIÃO EUROPEIA. **General Data Protection Regulation**. Disponível em: https://gdpr-info.eu/. Acesso em 28 out. 2021.

WALTERS, Robert. **A importância dos dados e cybersecurity na atualidade**. [2020]. Disponível em: https://www.robertwalters.com.br/recrutamento/hiring-advice/importancia-dados-e-cybersecurity.html. Acesso em: 1 nov. 2021.

WARREN, Samuel D.; BRANDEIS, Louis D. Right to Privacy. **Harvard Law Review**. v. 4, ed. 5, 15 dez. 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 28 out. 2021.

ZANINI, Leonardo Estevam de Assis. **O surgimento e o desenvolvimento do right to privacy nos Estados Unidos**. Jus. 15 jul. 2017. Disponível em: https://jus.com.br/artigos/57228/o-surgimento-e-o-desenvolvimento-do-right-to-privacy-nos-estados-unidos/3. Acesso em: 27 out. 2021.