UNIVERSIDADE SÃO JUDAS TADEUS
CURSO DE DIREITO
CAMPUS MOOCA

AILTON VICTOR AVANZO

A IMPRESCINDIBILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS NO CENÁRIO CORPORATIVO

São Paulo
2023

A IMPRESCINDIBILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS NO CENÁRIO CORPORATIVO

The Imprescindibility Of The General Data Protection Law In The Corporate Scenario

Ailton Victor Avanzo[1]

Resumo

Os dados pessoais se tornaram um ponto de atenção de grande relevância atualmente, considerando o advento da tecnologia e as infinitas possibilidades de risco a integridade destas informações. O uso e a coleta de dados exigem um nível de atenção especial devido ao seu alto valor moral e tudo o que representa para seus respectivos donos. Os avanços tecnológicos trazem significativa importância ao tema, e isso tem sido um impulso significativo para as mudanças no contexto jurídico relacionado a esta temática e toda a mobilização entorno do que está representa para a sociedade. O projeto em questão aborda a importância e a natureza jurídica da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) em um contexto histórico e corporativo. A LGPD estabelece diretrizes e regras para o tratamento de dados por parte das empresas, visando garantir transparência, segurança e controle sobre as informações pessoais dos indivíduos. O objetivo principal deste projeto é analisar e entender os avanços tecnológicos e suas especificidades, o grande impacto que a LGPD traz para as empresas e para todo o cenário corporativo e os limites da responsabilidade civil dos agentes de tratamento de dados. Serão explorados os principais aspectos da legislação, incluindo os direitos dos titulares dos dados, as responsabilidades das empresas, as medidas de segurança necessárias e as penalidades para o não cumprimento das normas estabelecidas. Além disso, o projeto busca compreender os desafios enfrentados pelas organizações na adequação à LGPD, tais como a necessidade de revisão de processos internos, adoção de medidas de segurança, treinamento dos colaboradores e a criação de uma cultura de proteção e dados em seus ambientes internos e externos.

Palavras-chave: Lei Geral de Proteção de Dados. Responsabilidade Civil. Lei nº 13.709/2018.

[1] Acadêmico do curso Direito na Universidade São Judas Tadeu, rede Ânima Educação. E-mail: victoravanzo@gmail.com. Artigo apresentado como requisito parcial para a conclusão do curso de Graduação em Direito da Universidade São Judas Tadeu. 2023. Orientador: Profº Drº Luis Fernando de Paiva Baracho Cardoso.

Abstract

Personal data has become a very important point of attention today, considering the advent of technology and the infinite possibilities of risk to the integrity of this information. The use and collection of data requires a special level of attention due to its high moral value and everything it represents for its respective owners. Technological advances bring significant importance to the topic, and this has been a significant impetus for changes in the legal context related to this topic and the entire mobilization surrounding what it represents for society. The project in question addresses the importance and legal nature of the General Data Protection Law (Law nº 13,709/2018) in a historical and corporate context. The LGPD establishes guidelines and rules for data processing by companies, aiming to ensure transparency, security and control over individuals' personal information. The main objective of this project is to analyze and understand technological advances and their specificities, the great impact that LGPD brings to companies and the entire corporate scenario and the limits of civil liability of data processing agents. The main aspects of the legislation will be explored, including the rights of data subjects, the responsibilities of companies, the necessary security measures and the penalties for non-compliance with established standards. Furthermore, the project seeks to understand the challenges faced by organizations in adapting to the LGPD, such as the need to review internal processes, adopt security measures, train employes and create a culture of protection and data in their internal environments. and external.

Keywords: General Data Protection Law. Civil Responsibility. Law No. 13.709/2018.

1. Introdução

Na era digital, onde a informação é um ativo valioso, a gestão responsável e segura dos dados torna-se uma prioridade incontestável para as organizações. Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) surge como um marco regulatório crucial no cenário corporativo, estabelecendo diretrizes fundamentais para a coleta, armazenamento, processamento e compartilhamento de informações pessoais. Este trabalho explora a importância da LGPD no contexto empresarial, trazendo o seu contexto e quais os impactos que a tornam tão imprescindível, não só para o cenário corporativo, mas também para os titulares de dados.

Ao abordar as empresas e a necessidade de conformidade com a legislação, busca-se destacar como elas podem não apenas atender às exigências legais, mas também aprimorar a confiança do consumidor, fortalecer a segurança da informação e, por conseguinte, promover uma cultura corporativa centrada na proteção dos dados.

2. A Proteção de Dados e Seu Contexto

Não há como falarmos de proteção de dados sem antes explicitar todo o seu contexto e sua evolução no âmbito jurídico e social, além de todo o seu processo de criação e o que a inspirou.

A tecnologia e suas nuances obtiveram notada ascensão na sociedade desde a sua criação, e este bombardeio de novas informações e digitalização possuem impacto direto em diversas esferas da sociedade contemporânea, sejam nos âmbitos jurídico, social, político e econômico, sendo definida então por (Barreto; Salles Leite, 2017, p. 410) como *a sociedade de Informação:*

> *"A sociedade da informação transformou, em grande medida, a conduta mundial, possibilitando o acesso a conteúdo jamais imaginado antes da supressão de barreiras físicas que separavam as pessoas, hoje usuárias individuais. A comunicação em rede interligou, também, culturas, povos e grupos de diferentes e múltiplas origens e características através do uso da grande rede mundial de computadores, a world wide web; tanto para o bem quanto para o mal."*

As inovações tecnológicas atingiram grande potencial de movimentação de dados na sociedade, uma vez que possibilita que uma alta escala de dados sejam processadas de forma quase que instantânea, sendo importante para o desenvolvimento social e da produção de

riqueza. Indo inclusive além das relações sociais e abarcando grande valor comercial. Barreto Júnior (2015), entende que:

> *"O advento do Informacionalismo é, indubitavelmente, a principal marca econômica da sociedade em rede. Reorganiza a produção de riqueza no sistema econômico, no qual há uma gradativa valoração da informação como mercadoria e fator de geração de valor econômico, o que torna a National Association of Securities Dealers Automated Quotations (Nasdaq), bolsa de valores das empresas tecnológicas, tão estratégica, em termos de organização econômica, quanto a tradicional New York Stock Exchange, denominada bolsa de Wall Street. As megacorporações informativas (Google, Facebook e Yahoo, entre outras) acumulam vestígios de informações sobre os usuários da Internet, tais como seus padrões de navegação, compras realizadas online, preferências culturais, religiosas e ideológicas, websites de interesse, verbetes e expressões pesquisadas nos websites de busca, entre outras, "impressões digitais eletrônicas" que servem para estabelecer uma categorização minuciosa de cada usuário na rede. [...] Circunscreve-se no fato de que há inúmeros usos para esses perfis eletrônicos, tal como direcionamento de publicidade on-line, oferta de mercadorias relacionadas ao perfil do consumidor, além de montar cadastros de valor incomensurável sobre os cidadãos da sociedade em rede."* (BARRETO JUNIOR, 2015, p. 410).

Este cenário desperta algumas incertezas sobre o rápido avanço tecnológico o qual estamos vivendo e os seus efeitos frente aos princípios legais e os direitos humanos.

Essa evolução traz junto consigo um alto índice de armazenamento de dados por parte das empresas, que utilizam ferramentas de alta-performance capazes de armazenar diversas informações pessoais de seus clientes, criando assim um enorme banco de dados, definido como *"uma coleção de dados inter-relacionados, representando informações sobre um domínio específico"* (KORTH; SILBERSCHATZ, 1994).

Ainda nesta seara, a LGPD – Lei Geral de Proteção de Dados – traz em sua ótica o conceito de banco de dados, em seu Art. 5°, inciso IV, como o *"conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico"* (BRASIL, 2018).

Portanto, resta evidente que os bancos de dados são os responsáveis por instrumentalizar a comercialização de dados, modificando e adequando o comportamento humano as necessidades do mercado. (ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, v. 30, n. 1, p. 75-89, 2015.)

A instituição deste fenômeno corrobora com a narrativa denominada *Capitalismo de Vigilância.* Este evento consiste na captação de dados pessoais que são transformados em ativos e comercializados dentro de um mercado pessoal de informações privadas.

O *Capitalismo de Vigilância* mapeia todos os vestígios deixados durante a navegação online, como um grande observador que capta cada passo dado pelo usuário, entendendo seus

costumes, desejos e principalmente seus comportamentos. A partir disso, essa leva de dados são transformados e vendidos à diversas empresas que possuem interesse nestas informações (ZUBOFF, 2020).

No mesmo sentido, Bioni (2020, p. 11) entende que, este movimento vai muito além dos dados em si, pois, para que estes estejam de acordo com o propósito da comercialização, é necessário que sejam convertidos em conhecimento acerca dos hábitos humanos. Esta nova estrutura econômica recente busca empregar esses dados, os quais são baseados em registros de vivências humanas, e transformados em insumos para objetivos comerciais, criando estratégias para campanhas direcionadas a perfis particulares de clientes e desenvolvendo produtos cada vez mais individualizados, influenciando assim o modo de pensar e as decisões dos consumidores (BIONI, 2020).

No entanto, à medida que estes dados se tornam mais acessíveis a um enorme grupo de empresas, gera-se uma certa insegurança para com eles e prejuízos inimagináveis para seus respectivos titulares, pela ocorrência de ações desprovidas de ética, como a sua utilização para tomada de decisões unilaterais, e, dependendo da qualidade dos dados, para práticas discriminatórias.

A cessão de dados pessoais nestas relações possui certo teor ficcional, considerando que há duas vertentes que formam barreiras entre os titulares e sua relação com o livre consentimento de seus próprios dados. Este cenário condiciona a incapacidade cognitiva do titular na avaliação correta da coleta e uso de seus dados. Além de situações em que há notável prevalência de relações comerciais onde a liberdade de escolha do titular é reduzida caso opte pela não cessão de seus dados, impedindo então que os titulares detenham total controle e autonomia sobre seus próprios dados.

A fim de combater essa disparidade de superioridade nas relações entre os percurssores deste movimento desenfreado exploração e os titulares de dados, viu-se a necessidade de instituir uma nova regulamentação diferente a que resguarda a nossa constituição.

Laura Schertel Mendes, neste sentido:

> *"A disciplina da proteção de dados pessoais emerge no âmbito da sociedade de informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados per se, mas a pessoa que é titular desses dados."*
> (MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. Editora Saraiva, 2014. P. 27)

Diante disso, torna-se imprescindível a promoção de uma regulação especifica que promova não somente a autonomia e integridade dos titulares de dados, mas também a importância do aspecto preventivo. E é ai que a LGPD – Lei Geral de Proteção de Dados - (Lei n° 13.709/2018) ganha vasão e robustez, tendo o *"importante papel de reforçar a autonomia dos titulares dos dados e o necessário e devido controle que estes precisam exercer sobre os seus dados"* (FRAZÃO, 2019, p. 31).

Tendo como base a própria RGPD – Regulamento Geral Sobre Proteção de Dados – criada pela União Europeia a fim de promover maior segurança para os cidadãos Europeus, o qual entrou em vigor em maio de 2018.

3. Direito à Privacidade e a Proteção De Dados Pessoais

Notadamente, há uma grande preocupação em relação a proteção de dados na esfera da sociedade contemporânea, visto a constante evolução tecnológica a qual estamos presenciando, sociedade essa a qual se caracteriza por Castells (2018, p. 55), pela alta gama de processamento e transmissão da informação.

O direito à proteção de dados possui vasta correlação com o direito à privacidade, ainda que o direito à privacidade se caracterize, no entanto, pela dicotomia entre as esferas públicas e privada (BIONI, 2020, p.91). Por outro lado, o direito a proteção de dados destina-se a uma escala maior de proteção e segurança da integridade das informações.

Entende Hannah Arendt (2010, p. 77-85) o direito à privacidade como pressuposto democrático, visto que a partir da fuga da "pressão social", os indivíduos podem vivenciar e experimentar suas subjetividades no espaço privado.

Desta forma, deve haver uma seleção criteriosa quanto ao compartilhamento de determinadas informações, da autonomia de escolha entre tornar público ou manter privado, a quem deseja compartilhar informações ou o nível de interação com essas pessoas, de modo que se defina não como uma simples preferência, mas sim uma prerrogativa, afastando assim um interesse externo. Esta conjuntura perpetua a promoção da garantia de não violação ou invasão ao determinarem a vida privada como inviolável (BIONI, 2020, p. 92-93).

Acerca disto, expressa o Artigo 21 do código civil que *"a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma."*

Ainda que o ordenamento jurídico brasileiro não contemple diretamente na constituição federal a proteção de dados pessoais, entende-se que este direito pode ser extraído acerca dos direitos fundamentais expresso no artigo 5°, inciso X da Constituição Federal:

> *Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*
> *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.*

Nesse sentido, a privacidade pode ser encarada como um direito guiado pela liberdade negativa de seu titular, que decide sobre quais aspectos de sua vida estão contidos em sua esfera privada e que, portanto, são tutelados por esse direito (RODOTÀ, 2012, p. 320).

Com base no exposto, o conceito de direito à privacidade se mostra desconexo com a realidade atual, uma vez que a definição de privacidade possui um perfil abstrato e possivelmente inconclusivo acerca do que realmente busca o objetivo do referido direito.

Acerca disto, Stefano Rodotà preceitua:

> *"Se este é o quadro global a ser observado, não é mais possível considerar os problemas da privacidade somente por meio de um pêndulo entre "recolhimento" e "divulgação"; entre o homem prisioneiro de seus segredos e o homem que nada tem a esconder; entre a "casa-fortaleza", que glorifica a privacidade e favorece o egocentrismo, e a "casa-vitrine", que privilegia as trocas sociais; e assim por diante. Essas tendem a ser alternativas cada vez mais abstratas, visto que nelas se reflete uma forma de encarar a privacidade que negligencia justamente a necessidade de dilatar esse conceito para além de sua dimensão estritamente individualista, no âmbito da qual sempre esteve confinada pelas circunstâncias de sua origem."* (RODOTÀ, 2008, p. 25).

Essa evolução do conceito de direito à privacidade objetiva promover não só capacidade de eliminação ou intervenções alheias, mas também a autodeterminação do titular quanto ao controle sobre suas informações pessoais.

O tratamento de dados tem se tornado cada vez mais expansivo e impacta cada vez mais pessoas e realidades sociais. Nesse contexto, portanto, a proteção de dados pessoais ergue-se como a tutela da "própria dimensão relacional da pessoa humana", pois existe um leque vasto de liberdades individuais relacionadas com a proteção de dados pessoais, que extrapolam os limites de tutela do direito à privacidade, pois este é atrelado a uma divisão das esferas pública e privada de seus titulares (BIONI, 2018, p. 99).

4. Agentes de Tratamento de Dados Pessoais

Podendo ser pessoa física ou jurídica, de direito público ou privado, o controlador de dados é a figura responsável pela tomada de decisões em relação aos dados pessoais. É responsável por administrar as diretrizes de tratamento e os meios os quais os dados serão tratados. O controlador de dados possui grande responsabilidade em face da LGPD – Lei Geral de Proteção de Dados, uma vez que é a figura máxima no que tange a tomada de decisões e manuseio de informações.

O Art. 5° da LGPD define o controlador da seguinte forma: *"Para os fins desta Lei, considera-se: VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".*

O operador de dados, podendo ser pessoa física ou jurídica, de direito público ou privado, é responsável por realizar o tratamento de dados pessoais em nome do controlador, como preceitua o Art. 5° da LGPD. O operador não possui autonomia para tomar qualquer decisão relacionada aos dados que estejam sendo tratados, apenas seguir as diretrizes de atuação definidas previamente pelo controlador. Por ele, passarão todos os dados dos usuários, sendo uma figura de extrema importância, por ter que receber, armazenar, dar a devida destinação e eliminar de maneira correta esses dados quando não forem mais necessários. (TEPEDINO, 2020).

Por último, o encarregado de dados ou DPO (Data Protection Officer) é o responsável por ser o elo de comunicação entre o controlador de dados, os titulares e a ANPD – Autoridade Nacional de Proteção de Dados. O DPO possui também a responsabilidade em garantir a segurança das informações tratadas, zelando pela proteção das mesmas contra quaisquer adversidades que possam comprometer a sua integridade.

De forma feral, a Lei 13.719/186 traz em seu artigo 41 que:

> *§ 2º As atividades do encarregado consistem em:*
> *I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;*
> *II - receber comunicações da autoridade nacional e adotar providências;*
> *III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e*
> *IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.*

O DPO (data protection officer) possui fundamental nas decisões estratégicas relacionadas ao tratamento de dados. O DPO deve ter autonomia sobre as atividades que envolvem o controle de dados e deve manter contato direto com a direção da empresa para tomar decisões que garantam a conformidade com as leis de proteção de dados.

Gilberto M. Castro discorre sobre o assunto:

> *"Devido a essas atividades, o DPO terá papel fundamental nas decisões estratégicas das organizações, e deverá ter autonomia sobre as atividades que envolvem qualquer tipo de tratamento de dados e contato direto com a direção da empresa para poder tomar decisões que possam deixa-la em conformidade com a lei. É recomendado que a empresa já nomeie seu DPO, antes mesmo do início efetivo do vigor da lei, dessa forma ele pode ajudar na adaptação da LGPD, condução das etapas dessa projeto analisando a atualização da empresa em relação ao tema, desenvolvendo o relatório de impacto à proteção de dados pessoais, no qual deve conter as características dos tratamentos de dados realizados, o risco para os titulares, conscientizar todos os níveis de organização sobre o tema e avaliar os impactos sobre a proteção de dados. Mesmo que ainda não tenha sido avaliado na prática no Brasil como vai funcionar a figura do DPO, já é possível concluir que será uma peça chave para a adequação da empresa à legislação e para as atividades relacionadas ao tratamento de dados pessoais de seus clientes, funcionários e fornecedores."*

Existe ainda as obrigações destinadas ao agentes de tratamento, como a adoção de "medidas de segurança, técnicas e administrativas" com intuito de 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". (Art. 46 – LGPD), além da obrigação de garantir a segurança da informação em relação aos dados pessoais, mesmo depois do seu término (Art. 47 – LGPD). Estando de acordo com o princípio da responsabilização e prestação de contas, o qual discorre sobre a adoção de medidas capazes e eficazes de poder comprovar que foram observadas e cumpridas, com eficácia, as normas de proteção de dados pessoais pelos agentes de tratamento. (Art. 6 – LGPD, Inciso X).

5. Tratamento de Dados Pessoais

A princípio, os dados pessoais referem-se a informações relacionadas a uma pessoa identificada ou identificável, acerca de todo e qualquer indivíduo, de forma que seja possível identificá-lo e obter informações com base em dados primários, como nome, documentos pessoais, endereços, o qualquer outro dado.

Aos ensinamentos de (MACIEL 2019, p.19):

> *"Dado pessoal é toda informação que pode identificar um indivíduo ainda que não diretamente. Portanto, incluem-se na referida definição, por exemplo, os números de Internet*

> *Protocol – IP, número de identificação de funcionário dentro de uma empresa, e até mesmo características físicas. Isso em razão da presença do léxico "identificável", que amplia a definição de dados pessoais." (MACIEL, Rafael Fernandes. Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18). 1. ed. Goiânia: RM Digital Education, 2019. Pág. 19. Acesso em 12 de nov 2022. p.19).*

No entanto, o tratamento destes dados caracteriza-se por toda forma de operação realizada para com os referidos dados, desde a coleta até o seu arquivamento ou eliminação permanente. Denota, basicamente, toda a operação adquirir, manter ou transmitir dados pessoais.

Acerca do exposto, a lei preceitua:

> *"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." (BRASIL, 2018).*

Segundo Peck (2018, p.44-43): "o tratamento de dados pessoais deve seguir um propósito certo e funcional, mas que não supere a liberdade de informação e expressão, a soberania, segurança e a defesa do Estado". Nesse sentido, o tratamento de dados deve buscar consigo uma maior segurança em temas relevantes da sociedade.

Acerca do tratamento de dados, a LGPD – Lei Geral de Proteção de Dados preconiza em seu Artigo 7°:

> *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.*

Maciel (2019, p.20) discorre que dados sensíveis estão relacionados aos seguintes dados: *"origem racial ou ética, 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"*.

O princípio basilar para a realização do tratamento de dados é o consentimento dos titulares. Através do consentimento o titular expressa que concorda com as ações de tratamento que serão realizadas com seus dados, garantindo assim o respeito ao direito e a liberdade de escolha (RIBEIRO, 2016).

Cabe ressaltar que o titular é apto a revogar seu consentimento a qualquer momento junto ao DPO (*data protection officer).* É necessário apenas que o titular entre em contato por meio dos canais disponibilizados e expresse o seu desejo de revogação.

6. Dados Pessoais Sensíveis

Por outro lado, a luz da LGPD – Lei Geral de Proteção de Dados, em seu Art. 5°, defini os dados sensíveis como aqueles *"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"*.

Assim, entende-se que dados pessoais sensíveis são informações que, se utilizadas de maneira indireta, podem resultar em discriminação ou causar danos potencialmente prejudiciais aos titulares destas informações.

Além de sua diferença na classificação, os dados pessoais sensíveis se fazem valer de uma forma de tratamento distinta dos dados pessoais. Dessa forma, a LGPD expressa:

> *Art. 11° O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:*
> *I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;*
> *II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:*
> *a) cumprimento de obrigação legal ou regulatória pelo controlador;*
> *b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;*
> *c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;*
> *d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;*
> *e) proteção da vida ou da incolumidade física do titular ou de terceiro;*

> *f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou*
> *g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.*

É com fundamento na possibilidade de utilização discriminatória, tanto por parte do mercado, quanto do Estado, que os dados sensíveis se associam a conjunturas em que podem estar presentes potenciais violações de direitos fundamentais, em razão da sua natureza (MULHOLLAND, 2018)

Seu caráter extremamente sensível alerta para o redobramento nas atenções para os responsáveis pelo tratamento destes dados, uma vez que essas informações podem resultar em discriminações para com os seus titulares.

7. Adequação da LGPD ao Cenário Corporativo

A Lei Geral de Proteção de Dados objetiva resguardar a integridade dos dados pessoais, regulando assim o seu uso, compartilhamento, armazenamento e o seu controle.

Acerca disto, (PEIXOTO, 2020) entende que as empresas assumam toda a responsabilidade no tratamento, bem como coleta e o armazenamento de dados apresentando como os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade, conhecida com tríade CIA, sendo focado na proteção e privacidade on-line, assim como a liberdade de se expressar e a segurança da informação de pessoas naturais.

Para caso de não cumprimento das medidas previstas na LGPD, cabe multa simples de 2% (dois por cento) do faturamento, limitando-se a cinquenta milhões de reais ou multas diárias, observando-se o limite máximo de cinquenta milhões (BRASIL, 2018)

Portanto, é de suma importância que as corporações estejam atentas as diretrizes estabelecidas pela LGPD e assim promova a segurança e assegure a integridade dos dados tratados internamente evitando vazamentos e possíveis transgressões. Sendo assim, se faz necessária a 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. (FEDERAL, 2021)

Medidas como essas levam a empresa para um rol de confiabilidade, considerando que o fato de estar adequado as normas da LGPD traz maior credibilidade e eleva o patamar da corporação em diversos aspectos.

Neste sentido Victor Lucca preceitua:

> *"Fica claro que as empresas que se adequarem à LGPD, o quanto antes sairão ganhando, podendo, inclusive, usar dessa premissa como uma forma de marketing para sua empresa, uma vez que a busca do usuário é a efetiva proteção de seus dados"* (LUCCA, Victor Spera de. Análise da Lei Geral de Proteção de Dados Acerca das Relações trabalhistas. Intertem@S, Presidente Prudente, v. 40, n. 40, p. 1-51, 24 nov. 2020.)

Ainda que não estejam explícitas quais as ferramentas são necessárias para garantir o cumprimento integral da lei, fica subentendido que seja necessária uma estrutura de recursos, ainda que mínimos, como softwares, hardwares, além do capital humano responsável pela execução da estratégia e manuseamento dos itens de programação.

Neste sentido, (LYRA, 2017) expõe:

> *"Para que a instituição desempenhe as atribuições da segurança da informação é necessário que esteja adequadamente estruturada. Essa organização interna tem como finalidade o estabelecimento de uma estrutura mínima para realizar o gerenciamento para implantação e operação dentro da organização."*

Além da implantação da estrutura de segurança, é fundamental que a organização conte com mapeamento de segurança, estratégia de segurança, planejamento de segurança, implementação de segurança, administração de segurança e segurança na cadeia produtiva (LYRA, 2017).

8. Meios para Adequação à LGPD

Para que seja implantando a LGPD dentro de uma empresa, é importante que seja de feito de forma sustentável a fim de promover maior segurança com os dados armazenados e garantir que o negócio se torne perene e atrativo comercialmente por sua boa reputação.

Para (DONDA,2020): *"A melhor maneira de ficar em conformidade com a LGPD é criando um comitê para análise e tomada e decisão; designar um DPO (data protection officer); mapear e entender o ciclo de vida dos dados; adotar regulamentações e padrões de segurança da informação; auditar e monitorar o ambiente; Criar um relatório de impacto; Criar um plano de ação para situações de emergência."* (DONDA,2020).

Sendo assim, o DPO ficará responsável pela liderança do comitê instituído, auxiliando no desenvolvimento de estratégias de análise de dados pessoais e sensíveis. Além disso, o DPO será responsável pelo desenvolvimento e aplicação de treinamentos a todos os colaboradores para que todos estejam alinhados e engajados no que tange ao tratamento de dados dentro da

empresa. Ainda neste sentido, o DPO desempenhará a função de elaborar relatórios acerca da legislação (DONDA,2020)

De forma ilustrada, Donda, 2020 estabelece uma metodologia de ação com as seguintes atribuições:

> *"Identificar o fluxo de tratamento de dados (ciclo de vida de dados);*
> *Avaliar se é realmente necessário o armazenamento desses dados;*
> *Identificar e controlar acessos;*
> *Mapear os controles de segurança aplicados na proteção dessas informações;*
> *Analisar o risco, identificar possíveis vulnerabilidades, determinar a probabilidade de uma ameaça e explorar uma vulnerabilidade existente;*
> *Monitorar o tratamento de dados, quem está acessando e de onde, quais ações estão acontecendo, a fim de detectar atividades suspeitas ou acessos não autorizados;*
> *Manter o ambiente em conformidade."*

Assim, entende-se que, classificar e documentar o ciclo de vida das informações faz parte de uma estratégia sustentável, pois permite a rastreabilidade do dado desde o seu armazenamento até o processo de exclusão.

Ainda nesta seara, (Donda, 2020) estabelece um plano de risco objetivando a segurança dos dados pessoais. Sendo ele:

> **A)** Criptografia: criptografar o disco rígido é um controle de segurança importante, pois o usuário pode armazenar dados pessoais no disco e em caso de perda, furto ou roubo, tudo que estiver no disco estará protegido. (DONDA, 2020)
>
> **B)** Softwares de antivírus: É importante manter o antivírus ativo e atualizado. (DONDA, 2020).
>
> **C)** VPN: usuários remotos merecem uma atenção especial e devem ser treinados para entender que certas redes podem ser perigosas e que eles somente devem se conectar a redes seguras. (DONDA, 2020).
>
> **D)** Política de senhas: é muito importante definir uma política de senhas dentro da empresa. Essa política pode ser complexa, porém isso não significa que uma política de senhas efetiva seja segura, pois é possível que alguns usuários acabem escrevendo suas senhas em algum lugar. (DONDA, 2020)
>
> **E)** Autenticação multifator e Passwordless: uma das melhores formas de ajudar a proteger os acessos é habilitando multifatores de autenticação, como senha, biometria, token, entre outros. (DONDA, 2020).

F) Controle de acesso: os dados pessoais e os dados pessoais sensíveis podem estar armazenados em diversos locais, por isso é importante conceder o acesso de maneira a garantir que não haja mais acessos que o necessário. (DONDA, 2020)

G) Auditoria: É fundamental para garantir a segurança da informação. Daniel Donda acredita que a auditoria funcione muito bem como controle de segurança dissuasivo, pois usuários mal-intencionados não irão se arriscar a executar ações em ambientes que sabem que estão sendo monitorados. É importante a implantação de um software de auditoria que facilite o processo e ajude a criar filtros listando determinadas ações de maneira eficiente e eficaz. (DONDA, 2020)

9. Considerações Finais

É evidente que a proteção de dados se tornou uma questão crucial no contexto da sociedade da informação, impulsionada pelo avanço tecnológico e pela transformação do mundo em uma rede interconectada. A ascensão do informacionalismo e a consequente comercialização de dados pessoais pelo Capitalismo de Vigilância levantam preocupações éticas e jurídicas sobre o controle e a autonomia dos indivíduos em relação às suas informações.

A crescente coleta e manipulação de dados pessoais pelas corporações levantam questões sobre privacidade, discriminação e o impacto nas decisões individuais dos titulares de dados. O rápido avanço tecnológico, embora beneficie o desenvolvimento social e econômico, também gera inseguranças e prejuízos para os titulares de dados, que muitas vezes enfrentam situações em que a liberdade de escolha é limitada devido à grande manipulação das informações compartilhadas pelos usuários muitas vezes sem o seu próprio consentimento.

Desta forma, a adequação à Lei Geral de Proteção de Dados (LGPD) exige uma abordagem estratégica e sustentável por parte das empresas. A implementação efetiva da LGPD não apenas reforça a segurança dos dados armazenados, mas também contribui para a construção de uma confiança sólida e atrativa no mercado.

Assim, a implementação da LGPD não é apenas uma obrigação legal, mas uma oportunidade para as empresas fortalecerem sua postura de segurança, ganharem a confiança dos clientes e se destacarem como entidades comprometidas com a proteção efetiva dos dados pessoais.

Estar de acordo com as normas consolida a capacidade de proteção da LGPD e promove a autonomia dos dados pessoais, permitindo assim que os titulares de dados exerçam seu direito à privacidade e tenham controle sobre suas informações, preservando a dignidade e os direitos fundamentais dos indivíduos na era da Sociedade da Informação, sendo crucial para equilibrar o avanço tecnológico com a salvaguarda dos valores éticos, jurídicos e humanos em meio ao constante fluxo de informações digitais.

REFERÊNCIAS BIBLIOGRÁFICAS

ARENDT, Hannah. **A condição humana**. Tradução de Roberto Raposo. Rio de Janeiro: Forense Universitária, 2010.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno Ricardo; DIAS, Daniel**. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor.** Civilistica.com, Rio de Janeiro, ano 9, n. 3, p.1-23, 2020.

DONDA, Daniel. **Guia prático de implementação da LGPD**: conheça as estratégias e soluções para adequar sua empresa em conformidade com a lei. São Paulo: Labrador, 2020. 144p.Disponível:https://plataforma.bvirtual.com.br/Leitor/Publicacao/185745/pdf/0?code=o0NdsHhAoxVXoLVPglbqe/mAz7DzWZvDkvBc2jqiGUXuRiIOqtiFGsoJ5cGhoLPjs3xkR4WT+XWe7Krtuq+xGg==. Acesso em: 25/10/2023.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019.

EUROPEAN UNION. **General data protection regulation EU (2016/679).** Disponível em: Acesso em: 20/10/2023.

FRAZÃO, Ana. **Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados**. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p. 23-52.

LUCCA, Victor Spera de. **Análise da Lei Geral de Proteção de Dados Acerca das Relações trabalhistas**. Intertem@S, Presidente Prudente, v. 40, n. 40, p. 1-51, 24 nov. 2020. Disponível

em: http://intertemas.toledoprudente.edu.br/index.php/Direito/article/view/8892. Acesso em: 25/10/2023

LYRA, M. R. **Segurança e Auditoria em Sistemas de informação. 2ª edição**. [S.l.]: Brasil: CienciaModerna, 2017.Nenhumacitaçãonotexto.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18).** 1. ed. Goiânia: RM Digital Education, 2019.

MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova lei geral de proteção de dados. Revista de direito do consumidor**, Brasília, v. 120, p. 469-483, nov./dez. 2018.

MULHOLLAND, Caitlin Sampaio. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados** (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018.

RODOTÀ, Stefano. **Il diritto di avere. Roma-Bari**: Laterza, 2012.

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

TEPEDINO, Gustavo. FRAZÃO, ANA. OLIVA, Milena Donato**. Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro**. Revista dos Tribunais, 2ªed. São Paulo – SP, 2020.

ZUBOFF, Shoshana**. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação.** In: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta et al., (orgs). **Tecnopolíticas da vigilância**: perspectivas da margem. São Paulo: Boi Tempo, 2019. p. 17- 68.