

ANÁLISE DA LEI 13.709, LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) DIANTE DO ATUAL DIREITO DIGITAL BRASILEIRO

ANALYSIS OF LAW NO. 13.709, THE GENERAL DATA PROTECTION LAW
(LGPD), IN LIGHT OF CURRENT BRAZILIAN DIGITAL LAW

Ciências Sociais Aplicadas • 06/10/2026

REGISTRO DOI: [10.70773/revistatopicos/791167343](https://doi.org/10.70773/revistatopicos/791167343)

Wandercairo Elias Junior¹

Leandro Manuel Pereira Sanches²

Felipe Martins de Almeida³

João Lucas Tavares Silva⁴

RESUMO

O presente trabalho tem como objetivo fazer uma análise da lei geral de proteção de dados, mais especificamente em relação a forma como esses dados serão tratados nessa nova era do direito digital, e como os direitos de seus titulares serão garantidos. Desta forma será analisada os pontos mais importantes e relevantes dessa lei. Com a finalidade de demonstrar como a proteção de dados é um meio de garantias de alguns direitos fundamentais, como, liberdade, privacidade, segurança e do livre desenvolvimento da personalidade. Como meio de atingir os resultados esperados pela presente pesquisa, usaremos o método dedutivo de pesquisa, com base nas leis vigentes, doutrinas e entendimentos acerca do tema. A pesquisa bibliográfica é o método usado sobre o tema exposto. Além disso, sendo usado sites e informações com o objetivo de demonstrar a relevância e importância da nova lei geral de proteção de dados.

Palavras-chave: Proteção de Dados; Direitos Fundamentais; Privacidade; Direito Digital.

ABSTRACT

This present scientific article aims to analyze the general data protection law, more specifically regarding how that data will be handled in this new era of digital law, and how the rights of their holders will be guaranteed. In this way, the most important and relevant points of this law will be analyzed. Demonstrate how data protection is a means of guaranteeing some fundamental rights, such as freedom, privacy, security and the free development of personality. As a way to achieve the results expected from this research, we will use the deductive research method, based on current laws, doctrines and understandings on the topic. Bibliographic research is the method used in the exposed theme. In addition, websites and information are used to demonstrate the

relevance and importance of the general data protection law.

Keywords: Data protection; Fundamental rights; Privacy; Digital Law.

1. INTRODUÇÃO

A tecnologia tem propiciado uma infinidade de possibilidades, facilitando o cotidiano geral. Apesar desses avanços, também surgem desafios relevantes, sobretudo relacionados à segurança no ambiente digital.

Diante dessa realidade, foram criadas e continuam sendo aperfeiçoadas normas nacionais e internacionais destinadas a regulamentar a proteção de dados na internet. Entretanto, as características próprias do ambiente virtual, como o anonimato e a dificuldade de identificação dos usuários, tornam cada vez mais complexas a apuração e a punição de atos maliciosos na rede.

Embora o governo brasileiro tenha demonstrado interesse em proteger os usuários, uma vez que diversas leis vieram nos últimos anos, é praticamente impossível garantir um ambiente totalmente seguro a todos os usuários.

Dessa forma, é de suma importância que as leis a respeito do direito digital sejam capazes de suprir essa necessidade de garantir proteção e segurança aos usuários, a fim de que não sejam reféns de criminosos, além disso é fundamental que as pessoas estejam cientes do quanto dados pessoais podem gerar problemas, se pessoas mal-intencionadas tiverem acesso.

Assim, a elaboração de leis que realmente sejam capazes de identificar e punir, bem como maior divulgação para as pessoas em geral acerca dos riscos da divulgação excessiva de dados tende a

tornar a internet mais segura para todos, coibindo a atuação de criminosos.

O Direito Digital e a tecnologia vêm se inovando de uma forma impressionante em nossos dias atuais, acompanhando o crescimento do número de pessoas inseridas no meio virtual. Por sua vez, os dados pessoais vêm obtendo cada vez mais notabilidade no mundo tecnológico, pois estão presentes e são fundamentais nas relações estabelecidas entre os usuários e as empresas públicas e privadas.

Ao utilizar serviços digitais, as pessoas se conectam diretamente com empresas públicas ou privadas, que oferecem determinados tipos de serviços. Essas empresas, recebem dados pessoais, desta forma, tendo total conhecimento sobre informações que podem comprometer a privacidade e a segurança de quem utiliza destes meios.

Diante desse cenário, é fundamental garantir segurança a todos os usuários, que são crescentes a cada dia, sendo essencial que o Estado invista em mecanismos capazes de prover dignidade no ambiente digital.

Em resposta a essa necessidade, foi promulgada em 14 de agosto de 2018, a Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD) que tem a responsabilidade de tratar das questões relacionadas a dados, dando maior enfoque aos dados pessoais. Trazendo assim, melhores condições e regulando o que deve ser feito através desse envolvimento entre as pessoas e o mundo cibernético.

Este artigo foi redigido com o intuito de analisar a LGPD, além disso, como a lei irá contribuir e ajudar na melhoria da segurança e da privacidade de todos.

Desta forma, no primeiro capítulo, foi feito uma breve análise da evolução da internet, trazendo como as mudanças sociais e a forma de se comunicar e consumir sofreram grandes revoluções com a popularização da internet. Além disso, demonstrando a insegurança e a vulnerabilidade dos usuários.

No segundo capítulo foi abordado um conceito mais amplo sobre a LGPD, e nos seus subtópicos abordando as formas e requisitos mais técnicos acerca de sua aplicabilidade. E por fim, no terceiro capítulo se analisou sobre como as empresas públicas e privadas estão se adaptaram no período de vacatio legis.

2. BREVE ANÁLISE HISTÓRICA DA INTERNET E A INSEGURANÇA NO MUNDO DIGITAL

As origens da internet estão relacionadas ao contexto da Guerra Fria e aos investimentos realizados pelos Estados Unidos em pesquisa militar e desenvolvimento científico, diante da necessidade de aprimorar os sistemas de comunicação e permitir o compartilhamento de informações entre instituições localizadas em diferentes regiões (Leiner et al., 1997; Zambom; Sétimo, 2013).

Em específico, em 1961, começaram a ser publicados estudos sobre a comutação de pacotes, técnica que permitia transmitir informações de forma mais eficiente do que os sistemas tradicionais baseados em circuitos. No ano seguinte, surgiu a ideia de uma rede de computadores interligados globalmente, por meio da qual seria possível acessar dados e programas a partir de diferentes

localidades. Já 1964, os estudos sobre a comutação de pacotes foram aprofundados e em 1965, foi realizada uma das primeiras experiências de comunicação entre computadores situados a longa distância, conectando equipamentos localizados em diferentes estados norte-americanos (Leiner et al., 1997)

O referido experimento demonstrou a possibilidade de compartilhamento remoto de dados e programas, mas também revelou as limitações do sistema telefônico convencional, reforçando a necessidade de adoção da comutação de pacotes no desenvolvimento das redes de computadores (Leiner et al., 1997)

Posteriormente, a Agência de Projetos de Pesquisa Avançada - ARPA, vinculada ao Departamento de Defesa dos Estados Unidos, financiou o desenvolvimento da ARPANET, que entrou em funcionamento em 1969, considerada a primeira rede de computadores com comutação de pacotes do mundo, inicialmente conectando universidades e centros de pesquisa. (Leiner et al., 1997; Robetns; 1986).

Na mesma época, também foram realizados estudos sobre sistemas de comunicação distribuídos, capazes de continuar funcionando mesmo diante da interrupção ou destruição de parte de sua estrutura, especialmente diante das preocupações existentes, naquele período, com possíveis ataques nucleares (Baran, 1964; Leiner et al., 1997).

Assim, o desenvolvimento da internet decorreu da combinação entre interesses militares, pesquisas acadêmicas e a necessidade de compartilhamento de informações e recursos tecnológicos.

Com o passar dos anos, as redes de computadores, inicialmente restritas aos meios militar e acadêmico, expandiram-se gradualmente para outras instituições e países. Durante a década de 1980, a criação da NSFNET ampliou a conexão entre universidades e centros de pesquisa, contribuindo para a formação de uma infraestrutura de comunicação de maior alcance (Leiner et al., 1997; U.S. National Science Foundation, 2024).

No final daquela década e no início dos anos 1990, o crescimento internacional das redes e sua progressiva abertura ao uso comercial favoreceram a interligação de sistemas acadêmicos, governamentais e privados. Consolidou-se, assim, a internet como uma rede mundial formada pela conexão entre diversas redes independentes, e não propriamente como uma única rede centralizada (Leiner et al., 1997; U.S. National Science Foundation, 2024).

Zambom e Sétimo (2013) relatam que a internet nos anos 90 foi ganhando bastante proporção como meio de comunicação, e os e-mails e as salas de bate papo permitiam que houvesse comunicação em tempo real, se tornando uma grande inovação na época, por isso, atraindo usuários de todo o mundo.

A expansão da internet, especialmente a partir do final do século XX, promoveu profundas transformações na sociedade ao estabelecer um ambiente virtual capaz de conectar milhões de computadores em escala global. Esse avanço tecnológico modificou significativamente a dinâmica cotidiana das pessoas, repercutindo nas relações sociais, econômicas, políticas e jurídicas (Fortes, 2016 apud Viana, 2018).

As mudanças sociais que a popularização da internet trouxe ao mundo foram imensas, as pessoas começaram a ter muito mais facilidade de comunicação e interação.

O desenvolvimento tecnológico e a expansão do ciberespaço modificaram significativamente as formas de interação entre indivíduos, empresas, organizações e o próprio Estado. Com a consolidação do ambiente digital, tornou-se igualmente natural o surgimento de conflitos decorrentes dessas novas relações estabelecidas por meio da internet (Araújo, 2018 apud Viana, 2018).

Inferre-se, portanto, a evolução da internet, bem como a sua popularização acarretou pontos positivos e negativos. Nesse sentido, o avanço da internet trouxe melhorias tanto no convívio social quanto no empresarial. Todavia, não foram só melhorias; mas também problemas, por exemplo, o convívio social passou-se a ser virtual, nos quais os hábitos mudaram, não só apenas entre as pessoas, mas também no ramo empresarial.

Sobre o impacto do ciberespaço na sociedade, Bezerra (2019, p. 11) destaca que:

Podemos citar a Internet como a maior revolução da comunicação e conectividade da história humana que, devido a sua relativa recente popularidade e disseminação, ainda há de ter seus efeitos sobre o indivíduo totalmente compreendido, entretanto, já é notável. Anteriormente éramos moldado por uma comunidade fechada, a reconstrução de um indivíduo criado em uma sociedade com limites físicos, obsoletos com a criação de um ciberespaço com acessos livre de ideias e personalidades? Supõem-se que a introdução da Internet transforme a identidade e o conceito de identidade além da consciência a medida que o global substitui o local e o virtual substitui o físico (Bezerra, 2019, p. 11).

Diante disso, alguns pontos positivos são relacionados a praticidade que a internet trouxe para a vida em sociedade, por exemplo, com os avanços tecnológicos possibilitou com que as pessoas pudessem trabalhar usando apenas um aparelho que tenha conexão com a internet, bem como trabalhar em sua própria residência “*home office*”.

Nessa mesma linha de raciocínio, Oliveira (2014) aponta que a internet reconfigurou profundamente a rotina cotidiana em múltiplos âmbitos, abrangendo desde o trabalho e o lazer até as formas de socialização e consumo. O mesmo autor destaca que essas transformações afetaram também a transmissão do conhecimento e a maneira como o indivíduo pensa, age e compreende a realidade.

Os pontos negativos baseiam-se na vulnerabilidade e insegurança das pessoas físicas e jurídicas na era digital, pois elas podem sofrer ataques cibernéticos, tendo em vista que todos são passíveis de crimes digitais.

Neste aspecto, o abordar a diversidade de vulnerabilidades no ambiente virtual, o CERT.br (2012) sistematiza os riscos cibernéticos em dimensões que englobam a segurança patrimonial, a proteção de dados, a privacidade e o bem-estar sociocultural do indivíduo.

No âmbito da segurança e do direito, o CERT.br (2012) destaca a ação de agentes mal-intencionados que utilizam a ilusão de anonimato para aplicar golpes, cometer estelionato, roubar identidades e perpetrar crimes graves.

Essa fragilidade é ampliada pela constante ameaça de softwares maliciosos que provocam a perda ou o roubo de dados em dispositivos conectados, bem como pelas conversas confidenciais que trafegam sem as devidas barreiras de proteção. Além disso, a prática de plágio e a distribuição não autorizada de materiais protegidos por direitos autorais figuram como condutas de alto risco, capazes de acarretar severas sanções jurídicas e prejuízos financeiros aos envolvidos (CERT.br, 2012).

No que tange à circulação de informações e à privacidade, a navegação expõe o usuário ao contato fortuito com conteúdos nocivos como pornografia, apologia ao ódio e manifestações racistas, além de favorecer a disseminação acelerada de boatos e informações falsas com potencial de gerar pânico coletivo (CERT.br, 2012).

A garantia da privacidade é tensionada tanto pelas alterações unilaterais de termos de uso promovidas por plataformas digitais quanto pela permanência prolongada dos registros na rede, tornando a exclusão definitiva de dados ou opiniões impensadas uma tarefa praticamente inviável (CERT.br, 2012).

Por fim, os impactos da conectividade estendem-se à esfera psicossocial e comportamental. O CERT.br (2012) ressalta que a ausência de pistas não verbais, como expressões faciais e tom de voz, em interações exclusivamente textuais gera frequentes ruídos de comunicação e interpretações dúbias. De forma complementar, a utilização desmedida da internet é apontada como um fator direto de degradação da saúde física, queda de produtividade acadêmica e profissional, e enfraquecimento dos laços de sociabilidade no mundo presencial.

Todos os exemplos citados acima acontecem diariamente com muitos usuários, muitos por não saberem os riscos que correm e outros por serem atacados por hackers e ter suas informações comprometidas.

Diante disso, a Lei Geral de Proteção de Dados vem com o enfoque de tentar amenizar estas situações ocorridas no cotidiano e fornecer mais segurança e facilidade no tratamento de dados, onde o próprio usuário tem muito mais autonomia sobre os seus dados fornecidos, e por consequência ter a ciência de como os seus dados pessoais estão sendo tratados.

3. LEI GERAL DE PROTEÇÃO DE DADOS

A privacidade e a segurança dos cidadãos são direitos fundamentais, além de ser um dever do Estado garanti-los, e está tipificada na

Constituição Federal de 1988, que menciona:

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 (Brasil, 1988, Art. 5º).

Segundo Panek (2019, p. 18): “cabe ao direito oferecer mais ferramentas de controle e estabelecer limites éticos, tanto no setor público quanto privado, para colocar de fato o indivíduo sob o controle da forma que as suas informações pessoais são processadas, em prol do direito à privacidade e de seus atributos derivados, adequados à era digital.”

No entanto, no Brasil não existia uma legislação específica em prol do tratamento de dados, e por isso os representantes brasileiros perceberam a necessidade de uma lei que garantisse maior segurança e benefícios aos seus usuários e ainda garantir alguns de seus direitos fundamentais mais importantes elencados na Constituição Federal.

Conforme a grande maioria dos outros países já tinham a sua própria legislação, e o Brasil ainda não tinha uma legislação concernente e específica a proteção de dados, decidiu usar como modelo a lei que regulamenta a proteção de dados na União

Europeia, a *General Data Protection Regulation* (GDPR). Nesse mesmo contexto, a influência e o rigor dessa normativa estrangeira refletiram-se diretamente no cenário interno:

Para o contexto nacional, a GDPR impulsionou a criação de uma legislação nacional que tratasse de proteção dos dados pessoais com uma maior abrangência do que aquela apresentada pelo Marco Civil da Internet, aprofundando a questão e criando parâmetros mais alinhados com os padrões internacionais, além do fato de que a GDPR expressamente veta empresas europeias que tratam de dados de alguma forma de fazer negócios com empresas de países que não possuíssem uma legislação específica para o tratamento de dados (Bezerra, 2019, p.31)

Além do mais, houve diversos escândalos no mundo relacionados à coleta e ao processamento de dados. Um dos casos mais notórios, conforme aponta Leme (2019), ocorreu em 2018 e envolveu a empresa Cambridge Analytica. Na ocasião, jornais como o *The New York Times* e o *The Observer* acusaram a referida companhia de utilizar informações extraídas de redes sociais para manipular campanhas eleitorais, o que teria influenciado diretamente a eleição de Donald Trump à presidência dos Estados Unidos.

Desta forma, tanto o Brasil como toda a comunidade internacional, passaram-se a se sentir compelidos a terem suas próprias normas regulamentadoras de dados pessoais.

Em resposta a este movimento, foi sancionada em 14 de agosto de 2018, a Lei Federal nº 13.709/2018, conhecida como Lei Geral de

Proteção de Dados (LGPD) que tem a responsabilidade de tratar das questões relacionadas aos dados pessoais de pessoas físicas ou jurídicas no Brasil, não só no âmbito digital, mas também em meios físicos, como arquivos e pastas. Assim, dando uma maior proteção do que as demais legislações já vigentes no país, como o marco civil, que apenas garantia a proteção em ambiente online (Brasil, 2018).

Em seu Art. 1º a LGPD relata que: “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” (Brasil, 2018, art. 1º).

Neste mesmo sentido, Pinheiro (2026) destaca que a Lei nº 13.709/2018 representa um marco normativo de profundo impacto tanto para instituições públicas quanto privadas. Para o referido autor, a LGPD regula a proteção das informações dos indivíduos em qualquer tipo de relação que envolva o tratamento de dados pessoais, independentemente do meio utilizado ou se o agente da operação é pessoa natural ou jurídica. Assim, a norma estabelece princípios, direitos e deveres voltados ao uso dessas bases de dados, consideradas atualmente como um dos ativos digitais de maior valor.

A LGPD é de interesse público nacional, das grandes e pequenas empresas e também a pessoas físicas desde que tratem dados pessoais, mas vale ressaltar que a lei protege somente os dados pessoais de pessoas físicas, (pessoas naturais), ela não protege dados de pessoas jurídicas, apenas se aplica aos dois, ou seja, tanto a pessoa física quanto a jurídica que chegam a usar dados de forma

incorreta, sem o consentimento do usuário, a lei será aplicada com as suas devidas sanções.

Pinheiro (2026, p. 35), ainda relata que: “a necessidade de uma lei específica sobre proteção dos dados pessoais decorre da forma como está sustentado o modelo atual de negócios da sociedade digital, na qual a informação passou a ser a principal moeda de troca utilizada pelos usuários para ter acesso a determinados bens, serviços ou conveniências”.

Desta forma, o legislador teve que especificar como serão os procedimentos e funções que irão ser utilizadas para que esses direitos e regras sejam garantidos, e devidamente seguidos, trazendo na legislação especificações de como as empresas jurídicas de direito público ou privado e as próprias pessoas físicas devem se comportar ao tratar dados pessoais, fazendo com que o acesso e a informação a determinados bens ou serviços seja feita de forma mais segura e transparente.

Antes da Lei Geral de Proteção de Dados não havia muita transparência de como os dados pessoais seriam tratados e utilizados, principalmente por parte das empresas, nossos dados estavam sendo usados de forma indiscriminada, ou seja, circulavam por diversas plataformas digitais sem o nosso consentimento.

A LGPD traz em seu artigo 2º fundamentos que devem ser respeitados e observados na aplicação dos artigos de toda esta lei, de forma a ser usados como norteadores.

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;

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018, art. 2º).

Essas definições servem de base para resguardar os nossos direitos fundamentais elencados na Constituição Federal.

No artigo 3º da LGPD nós temos questões relacionadas a territorialidade da lei, no qual todos os legitimados descritos abaixo, estão sujeitos a aplicabilidade da LGPD, desde que preencha estes requisitos a seguir.

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 (Redação dada pela Lei nº 13.853, de 2019) Vigência

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 (Brasil, 2018, art. 3º).

Em decorrência disso, Pinheiro (2026, p. 34) nos diz assim:

(...) a LGPD apresenta alcance extraterritorial e efeitos internacionais, visto que se aplica também aos dados tratados fora do Brasil, desde que a coleta tenha ocorrido em território nacional, ou por oferta de produto ou serviço para indivíduos no território nacional ou que estejam no Brasil. Consequentemente, a título de exemplo, temos que o dado pessoal tratado por uma empresa de serviço de cloud computing que armazena o dado pessoal fora do país é obrigada a cumprir as exigências da LGPD.

Diante disso, entendemos que a LGPD não se limita apenas aos dados tratados em território brasileiro, mas também pode abranger as empresas que não tenham qualquer estabelecimento em nosso país, porém a coleta tem que ter ocorrido em território nacional.

A própria Lei 13.709/2018 nos traz em seu artigo 5º alguns conceitos e definições legais de dados pessoais, além disso quem são os seus titulares, controladores, operadores e os demais responsáveis pelo tratamento desses dados.

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;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

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

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 15.352, de 2026)

IX - agentes de tratamento: o controlador e o operador;

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;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

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;

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;

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019)

XIX - autoridade nacional: entidade da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 15.352, de 2026) (Brasil, 2018, art. 5º).

Conforme citado, temos diversas especificações relacionadas ao tratamento de dados, pois a LGPD nos trouxe de forma mais específica e detalhada como serão o tratamento, desde o consentimento do usuário até mesmo a exclusão.

Ainda conforme citado acima, o tratamento de dados engloba várias definições, como por exemplo, a coleta, classificação, exclusão e transferência dos dados. Desta forma, deixando bem claro todo o procedimento a ser feito com os dados fornecidos pelo usuário. Os

dados pessoais também têm a sua própria definição, podendo ser entendido como tudo que deixe uma pessoa natural identificada ou a torne identificável.

Lima, Alcassa e Pappert (2022) nos explicam que a LGPD adota um conceito amplo de dado pessoal, abrangendo não apenas as informações que identificam diretamente uma pessoa natural, mas também aquelas que, quando analisadas isoladamente ou em conjunto com outros elementos, possam permitir a sua identificação. Dessa forma, a proteção conferida pela legislação alcança tanto os dados que possuem ligação imediata com determinado indivíduo quanto aqueles capazes de torná-lo identificável de maneira indireta.

Para as referidas autoras, esse conceito pode abranger uma grande variedade de informações. O CPF, por exemplo, constitui dado pessoal por estar diretamente associado ao seu titular e permitir sua identificação em diferentes situações, inclusive para finalidades administrativas, cadastrais ou de análise de crédito. Da mesma forma, um número de matrícula criado pela por uma empresa para identificar internamente determinado empregado também pode ser considerado dado pessoal, ainda que sua utilização esteja restrita ao ambiente organizacional, uma vez que possibilita associar aquela informação a uma pessoa natural específica (Lima, Alcassa, Pappert, 2022).

Além disso, a LGPD em seu inciso II do artigo 5º também traz o conceito de dados pessoais sensíveis. Os dados sensíveis precisam ter tanto cuidado e prevenção quanto os demais dados pessoais. Pois aqui também pode ser atingida a dignidade da pessoa humana de uma forma muito impactante, no qual um dos seus principais

dados sensíveis são relacionados a dados pessoais raciais ou étnicos, convicções políticas e religiosas e até mesmo dados genéticos.

Lima, Alcassa e Pappert (2022) nos relata que o conceito de dados sensíveis remete a uma categoria de dados pessoais que exige um rigor mais acentuado em seu tratamento, pois tratam-se de informações que podem gerar discriminações sobre a pessoa a quem se refere, incluindo também os dados genéticos ou biométricos.

Diante dessas características, verifica-se que a utilização indiscriminada ou indevida de dados pessoais sensíveis pode favorecer práticas discriminatórias em diferentes contextos. Informações relacionadas, por exemplo, às convicções políticas ou religiosas de uma pessoa podem influenciar decisões que deveriam ser pautadas por critérios objetivos. No âmbito empresarial, um empregador poderia deixar de contratar determinado candidato em razão de posicionamentos políticos ou religiosos divergentes dos seus, utilizando essas informações como fator de exclusão. Situações dessa natureza demonstram a necessidade de proteção reforçada dos dados sensíveis, justamente para evitar tratamentos discriminatórios e resguardar direitos fundamentais, especialmente a dignidade da pessoa humana.

No entanto, apesar de serem dados sensíveis, há possibilidades de encontrarem-se sobre o domínio de pessoas naturais e pessoas jurídicas, inclusive o próprio governo.

Sobre isto, conforme Pinheiro (2026), a proteção diferenciada conferida aos dados sensíveis decorre dos riscos que a utilização inadequada dessas informações pode representar aos direitos

fundamentais. Embora seu tratamento possa ser necessário em determinadas circunstâncias, deve ocorrer de forma cuidadosa, segura e limitada às finalidades legítimas, evitando situações capazes de gerar discriminação ou outras violações à liberdade, à privacidade e à dignidade da pessoa.

Essas diferentes características dos dados são realmente para poderem identificá-los de uma forma mais eficiente em cada caso e para definir a clareza do tema tratado as pessoas em geral, pois muitos não fazem ideia de como os dados pessoais podem impactar na sua vida.

A Lei Geral de Proteção de Dados em seu artigo 5º inciso III também nos traz o conceito de dado anonimizado. Podemos considerar esse tipo de dado um pouco diferente, pois ele não permite a identificação do seu titular, no qual era um dado pessoal que passou por um determinado processo não previsto pela LGPD para retirar as características que o identificam e o definem (Brasil, 2018). Desta forma esses dados deixam de ser pessoais e por conseguinte deixam de serem protegidos e regulados pela LGPD.

Ainda em relação aos dados anonimizados a LGPD traz o seguinte:

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.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais. (Brasil, 2018, art. 12).

Sobre isto, Pinheiro (2026) destaca que a técnica adotada para a anonimização deve ser capaz de demonstrar, de forma segura, que os dados não podem ser revertidos ou novamente associados ao seu titular por quem os recebe. Essa cautela é relevante para reduzir riscos de responsabilização futura, especialmente em demandas judiciais de natureza consumerista, nas quais nem sempre é possível realizar uma perícia técnica compatível com a complexidade do tema. Nesse cenário, a utilização de soluções de anonimização certificadas tende a se tornar cada vez mais necessária, justamente

para proporcionar maior segurança jurídica e diminuir controvérsias quanto à efetividade do procedimento adotado.

Assim, um dado só é considerado efetivamente anonimizado se não permitir que, via meios técnicos possíveis e disponíveis, reverta-se a identificação à seu titular. Por sua vez, conforme

Por outro lado, a LGPD caracteriza pseudonimizado o dado que deixa de permitir sua vinculação direta ou indireta a determinada pessoa, mas pode ser revertido quando utilizado em conjunto com informações adicionais, que devem ser mantidas separadamente pelo controlador, em ambiente seguro e controlado (Brasil, 2018).

Frisa-se que LGPD não apresenta, em seu art. 5º, uma conceituação específica para o dado pseudonimizado. Contudo, o dado pseudonimizado pode por meios técnicos ser reconstruído e ter o titular do dado identificado novamente e por isso entende-se que este continua sendo um dado pessoal e obtendo a regulação da LGPD.

Diante de todos esses conceitos e definições sobre os dados, não poderíamos deixar de comentar sobre os controladores e operadores. Este é quem realiza o tratamento de dados pessoais em nome do controlador, e aquele é quem tem a competência para tomar as decisões referente ao tratamento dos dados pessoais. Tanto o controlador, quanto o operador podem ser pessoas naturais ou jurídicas, tanto de direito público, quanto de direito privado.

Neste entendimento Lima, Alcassa e Pappert (2022) nos informam que: na concepção da LGPD, o controlador é aquele com a responsabilidade central pela tomada de decisões sobre o tratamento de dados nas instituições, sejam elas de direito público

ou privado. Nesse papel, cabe a ele cumprir diversas exigências legais, a exemplo da implementação de programas de governança em privacidade.

Os mencionados autores destacam ainda que é dever do controlador elaborar o relatório de impacto quando solicitado pela Autoridade Nacional de Proteção de Dados (ANPD), assegurar os direitos dos titulares e, que poder atuar cumulativamente como operador em certos casos. Contudo, como o controlador detém o poder de decisão e a responsabilidade principal, a lei exige que ele seja facilmente identificado. É essa identificação que garante ao titular saber exatamente a quem procurar para exigir informações sobre seus dados.

Assim, o controlador é o responsável por tomar decisões relacionados aos dados pessoais, definindo como deve ser feita a coleta desses dados, estabelecendo quais dados serão tratados e as suas devidas finalidades, além do tempo que estes dados serão mantidos no banco de dados, principalmente os referentes as pessoas jurídicas de direito público ou privado, conforme mencionado anteriormente.

Os artigos 37 e 38 da LGPD Nos esclarece o seguinte:

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados (Brasil, 2018, arts. 37 e 38).

Por sua vez, art. 39 da LGPD apresenta o seguinte: “o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.” (Brasil, 2018, art. 39).

Assim, o operador é aquele que segue as ordens do controlador, no qual são estabelecidas as ordens e funções que deverão serem seguidas. Os dois tem uma relação muito próxima, pois um necessariamente precisa do outro para quem possam elaborar os devidos registros das operações.

Ademais, também temos o denominado encarregado, que se trata de pessoa indicada pelos controladores e operadores para ser o meio de comunicação entre os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

A LGPD nos traz as especificações concernentes ao encarregado, relatando que:

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 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 (Brasil, 2018, art. 41).

Diante disso, podemos afirmar que o encarregado é um meio de ligação entre os controladores, operadores, titulares de dados e a Agência Nacional De Proteção De Dados (ANPD).

Outrossim, a legislação nos trouxe um conceito bem mais transparente sobre o consentimento do titular de dados, abordando

que o titular tem o direito de consentir a utilização de seus dados para uma determinada finalidade. Sendo considerado um dos temas mais importantes da LGPD. A lei geral de proteção de dados, em seu Art.8º nos diz assim:

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 (Brasil, 2018, art. 8º).

Com base no artigo 8º da LGPD, Pinheiro (2026) destaca que o consentimento do titular é um elemento de extrema relevância. A autora explica que, devido ao avanço tecnológico, as informações pessoais tornaram-se mais sensíveis e vulneráveis, especialmente no ambiente digital, o que elevou a importância da autorização prévia para a coleta de dados. Portanto, para assegurar a liberdade e a privacidade dos indivíduos, é indispensável garantir que eles tenham plena consciência de que estão consentindo, além de compreenderem a exata finalidade do uso de seus dados e terem garantido o acesso a esse conteúdo a qualquer momento.

Neste sentido, a LGPD traz o conceito que o tratamento de dados só poderá ser realizado mediante o fornecimento de consentimento do titular dos dados. Além do mais, os titulares têm o total direito de saber o que vão fazer com os seus dados, ou seja, a finalidade proposta para o uso daqueles dados. Isso é muito relevante, pois desta forma as empresas terão que comunicar e pedirem a autorização do titular novamente, caso queiram usar os dados para finalidade diversa da original, proposta anteriormente.

Essa exigência de vinculação estrita à finalidade torna-se ainda mais rigorosa quando envolve informações de maior grau de proteção. Corroborando essa premissa, o SERPRO (2020) esclarece que, em especial no trato de dados sensíveis, tanto as empresas quanto o governo só podem realizar o acesso mediante um consentimento explícito do titular e com um fim previamente determinado.

Para Pinheiro (2026), no tratamento de dados pessoais sensíveis, o consentimento do titular possui especial relevância, embora a própria LGPD preveja situações em que esse requisito poderá ser dispensado.

Portanto, com a LGPD, fica claro que quem é o verdadeiro dono do dado não é aquele que o utiliza, nem aquele que o salvaguarda em bancos de dados. Nada disso, o dado pessoal é estritamente da pessoa a quem ele diz respeito. Na teoria isso parece algo óbvio, mas na prática não é bem assim. E tem muito dado particular sendo usado para fins que seu dono ou dona real sequer sabem. Usos, inclusive, que podem até mesmo prejudicá-los.

Desta forma, o consentimento é o termo mais importante da legislação, pois sem ele, toda o processamento e tratamento de dados seria feita de forma inequívoca e arbitrária.

3.1. Formas e Requisitos para a Garantia dos Direitos dos Titulares de Dados

O titular de dados é a figura principal da LGPD, que lhe conferiu vários direitos e informações em diversos artigos da lei. Na proteção de dados, podemos falar que a pessoa natural tem garantida a titularidade dos seus dados, além das garantias de seus direitos fundamentais.

A LGPD em seu artigo 17 relata que “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, art. 17).

Tung Panek (2019) enfatiza o significativo empoderamento garantido ao titular dos dados pela legislação. Segundo a obra, o indivíduo passa a ter o direito de exigir do controlador, a qualquer momento, o acesso às suas informações e a exclusão de dados que ultrapassem os limites legais. Além disso, o titular ganha a prerrogativa de ser informado sobre o compartilhamento de seus

dados com entidades públicas ou privadas, podendo, inclusive, revogar o consentimento dado anteriormente e interromper definitivamente o tratamento de suas informações por aquele agente.

A Lei geral de proteção de dados em alguns de seus artigos nos relatam as formas e requisitos previstos para o titular de dados, fazendo com que haja muito mais transparência e informação em prol dos usuários.

Em seu artigo 8º a LGPD já nos destaca os meios de manifestação de vontade do titular para o devido tratamento desses dados, além de detalhar que o consentimento do mesmo, pode ser uma forma de autorização e uma forma de revogação a qualquer momento da utilização de seus dados no banco de dados de alguma empresa. Do mesmo modo, o artigo 9º da LGPD nos relata sobre as informações concernentes aos titulares de dados.

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.

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. (Brasil, 2018, arts. 8º e 9º)

Portanto, o texto legal nos informa que é necessário que o titular de dados tenha as devidas informações relacionadas a finalidade e identificação dos responsáveis por estes dados.

3.2. Segurança e Sigilo de Dados

É fato que a segurança e o sigilo de dados são de suma importância para que o direito fundamental a proteção de dados seja devidamente garantida.

O vazamento de dados advindos de ataques hackers é um problema frequente em nossa atual sociedade moderna, além disso as próprias empresas são falhas e não adotam as devidas providencias necessárias ao tratamento correto dos dados.

No contexto das vulnerabilidades, a exposição indevida não se limita a ataques cibernéticos. Conforme as diretrizes da ABNT (2022), a segurança física e do ambiente constitui um pilar fundamental para a proteção da informação. A norma evidencia que o furto ou roubo de equipamentos, a exemplo de servidores e computadores, representa uma ameaça direta à privacidade e aos direitos dos titulares.

Nesses cenários, a subtração física do hardware em si torna-se um problema secundário quando comparada ao impacto crítico do vazamento ou da perda definitiva dos dados pessoais ali armazenados, o que configura uma grave violação à LGPD.

Assim, estamos muito expostos a sofrer com o tratamento de forma inexata. Além de que os dados têm um descarte das informações de forma errônea por partes desses, e isso pode ocasionar severos danos aos titulares de dados.

O texto da lei em seus artigos. 46, 47 e 48 nos relatam os procedimentos a serem seguidos pelos responsáveis pelo tratamento para a devida segurança e sigilo dos dados:

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 (Brasil, 2018, art. 46)

Desta forma, a LGPD define com transparência como deve ser todo o processo de medidas de segurança na proteção dos dados. O Art. 47 diz 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, art. 47).

Ou seja, mesmo após o término do uso de dados pessoais, o agente responsável ou qualquer outra pessoa tem que garantir as devidas seguranças a esses dados, pois ao fim do tratamento também tem que ter o procedimento correto para a exclusão do banco de dados.

E por último o artigo 48 da LGPD define:

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 (Brasil, 2018, art. 48).

Nesse sentido, ao traçar um comparativo com a legislação europeia que fundamentou a LGPD, Pinheiro (2026) ressalta a forma como o GDPR aborda a comunicação de incidentes de segurança. A autora explica que o regulamento europeu, em seu artigo 33, determina que a notificação sobre eventuais vazamentos ou falhas deve ser

realizada sem atrasos injustificados, estipulando um prazo ideal de até 72 horas após a ciência do ocorrido.

Portanto, destacando que é imprescindível a relação entre os controladores, titulares de dados e autoridade nacional de proteção de dados (ANPD) fornecendo-lhes todas as ocorrências de incidente que possam vir a acontecer, e com tempo determinado para efetuar a devida comunicação dos incidentes.

4. CONCLUSÃO

Conforme se pode identificar, a vulnerabilidade dos titulares de dados, tanto no ambiente digital, como no físico, é muito grande, se englobando nesse contexto, todas as pessoas que fornecem seus dados, e por isso sempre foi necessário ter uma legislação própria para tratar os dados pessoais de forma transparente e com a devida organização para que os direitos e garantias dos usuários sejam realmente garantidos.

Antes da LGPD, tínhamos algumas legislações que se referiam a proteção de dados, mas nada muito taxativo e conceitual, que obrigassem as pessoas e as empresas a mudarem a sua forma de pensar e se organizar em prol dos dados pessoais.

A LGPD trouxe conceitualmente os requisitos e especificou as formas de como as pessoas jurídicas de direito público ou privado, e até mesmo as pessoas naturais devem agir ao fazer o tratamento de dados de qualquer pessoa. Além disso, ressaltou diversas vezes sobre os limites impostos, no qual todos devem acatá-los, pois podem ser multados em caso de descumprimento.

Um dos motivos pela qual foi criada a LGPD, advém de muitos debates e problemas de segurança de dados em todo o mundo, no qual a própria União Europeia e os outros países internacionais fizeram imposições sobre os países no qual mantinham relação comerciais, uma legislação própria para que pudessem manter essa relação e conseqüentemente obterem mais confiança e segurança ao tratar dados e troca de informações. Ou seja, a nova lei trouxe confiabilidade e respeito dos outros países perante o Brasil.

Também é muito relevante ter a compreensão que a Lei Geral de Proteção de Dados é de suma importância para resguardar o direito fundamental a proteção de dados, já que a grande maioria das pessoas são vulneráveis e tem os seus dados espalhados de forma indiscriminada pela rede.

Diante disso, a atuação da Autoridade Nacional de Proteção de Dados (ANPD) aliada à aplicação efetiva da LGPD demonstra o amadurecimento de uma legislação capaz de proteger a dignidade do titular em todas as esferas, sejam elas físicas ou digitais.

Perante o exposto, conclui-se que a lei já atua como um escudo protetivo indispensável aos cidadãos, o que materializou a proteção de dados como um verdadeiro direito autônomo dentro do ordenamento jurídico nacional.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002:2022: Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

BARAN, Paul. **On distributed communications: I. Introduction to distributed communications networks.** Santa Monica: RAND Corporation, 1964.

BARRETO JÚNIOR, Irineu Francisco. NASCIMENTO, Arianne Azevedo. FULLER, Greice Patrícia. Lei Geral de Proteção de Dados Pessoais: Efetividade Jurídica do Consentimento do Titular para Tratamento dos Registros. **Revista de Constitucionalização do Direito Brasileiro.** v. 3, n. 2. Jul./Dez. 2020. Disponível em: <https://doi.org/10.33636/reconto.v3n2.e037>. Acesso em: 13 ago. 2026.

BEZERRA, André Luís Martins. **A lei 13.709/18 e os novos desafios da proteção de dados pessoais e identidade.** 2019. 42 p. Monografia (Bacharelado em Direito) – Universidade Federal de Pernambuco, Recife, 2019. Disponível em: <https://repositorio.ufpe.br/bitstream/123456789/36323/1/TCC%20-%20A%20lei%2013.70918%20e%20os%20Novos%20Desafios%20da%20Prote%C3%A7%C3%A3o%20de%20Dados%20Pessoais%20e%20Identidade%20-%20ver1.0-con2.pdf>. Acesso em: 13 ago. 2026.

BRASIL. Constituição Federal, de 05 de outubro de 1988. Disponível em <http://www.planalto.gov.br/ccivil03/Constituição.htm>. Acesso em: 13 ago. 2026.

BRASIL. Lei 13.709, de 14 agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 13 ago. 2026.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Cartilha de segurança para**

internet. Versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, 2012.

LEINER, Barry M.; CERF, Vinton G.; CLARK, David D.; KAHN, Robert E.; KLEINROCK, Leonard; LYNCH, Daniel C.; POSTEL, Jon; ROBERTS, Larry G.; WOLFF, Stephen. A brief history of the Internet. **Internet Society**, 1997. Disponível em: <https://www.internetsociety.org/internet/history-internet/brief-history-internet/>. Acesso em: 5 ago. 2026.

LEME, Carolina Silva. Proteção e Tratamento de Dados Sob o Prisma da Legislação Vigente. **Fronteira Internacional do Direito**. Ano 1, v. 01, 2019. Disponível em: http://www.veirano.com.br/upload/content_attachments/920/591112_FID_01_Protecao_tratamento_dados_original.pdf. Acesso em: 13 ago. 2026.

LGPD BRASIL. **O que muda com a nova Lei de Dados Pessoais**. Disponível em: <https://www.lgpdbrasil.com.br/o-que-muda-com-a-lei/>. Acesso em: 13 ago. 2026.

LIMA, Adrienne; ALCASSA, Flávia; PAPPERT, Milena. **LGPD no Direito do Trabalho**. Rio de Janeiro: Expressa, 2022. E-book. p.69. ISBN 9786553621954

OLIVEIRA, Ricardo. **Mudanças causadas pela internet em nosso cotidiano**. Disponível em: <https://administradores.com.br/artigos/mudancas-causadas-pela-internet-em-nosso-cotidiano>. Acesso em: 13 ago. 2026.

OLIVEIRA, Ana Paula et al. A lei geral de proteção de dados brasileira na prática empresarial. **Revista Jurídica da Escola Superior de**

Advocacia da OAB-PR. Ano 4. Número 1 Maio de 2019. Disponível em: <http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2019/05/revista-esa-cap-08.pdf>. Acesso em: 13 ago. 2026.

PINHEIRO, Patricia P. **Proteção de Dados Pessoais: Comentários À Lei N. 13.709/2018 (lgpd).** 5. ed. Rio de Janeiro: SRV, 2026. E-book. p. 240. ISBN 9788553623617.

REANI, Valéria. **Impactos da Lei Geral de Proteção de Dados para os negócios e as pessoas.** Disponível em: <https://www.conjur.com.br/2018-out-25/valeria-reani-impactos-lei-protecao-dados-negocios>. Acesso em: 13 ago. 2026.

ROBERTS, Larry. The ARPANET and computer networks. In: ACM CONFERENCE ON THE HISTORY OF PERSONAL WORKSTATIONS, 1986, Palo Alto. **Proceedings of the ACM Conference on the History of Personal Workstations.** New York: Association for Computing Machinery, 1986. p. 51-58. DOI: <https://doi.org/10.1145/12178.12182>. Disponível em: <https://doi.org/10.1145/12178.12182>. Acesso em: 5 ago. 2026.

SERPRO. **Nos casos em que a base legal utilizada seja o consentimento, é você cidadão que define se e como seus dados pessoais podem ser tratados por terceiros.** Disponível em: <https://www.serpro.gov.br/lgpd/cidadao/seu-consentimento-e-lei>. Acesso em: 5 ago. 2026.

TUNG PANEEK, Lin Cristina. **Lei Geral de Proteção de Dados nº 13.709/2018: uma análise dos principais aspectos e do conceito de privacidade na sociedade informacional.** 2019. 35 f. Monografia

(Bacharelado em Direito) – Universidade Federal do Paraná, Curitiba, 2019.

U.S. National Science Foundation. **Birth of the commercial Internet**. 2024. Disponível em: <https://www.nsf.gov/impacts/internet>. Acesso em: 5 ago. 2026.

VIANA, Igor Bonfim. **A proteção de dados pessoais na internet à luz do direito pátrio**. 2018. 59 f. Monografia (Bacharelado em Direito) – Universidade Federal de Roraima, Boa Vista, 2018.

ZAMBOM, Élton Visa; SÉTIMO, Pricilla Chaves. **A Evolução da Internet e sua Influência na Comunicação Mundial e na Escrita Formal**. 2013. 76 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Faculdade do Espírito Santo, Cachoeiro de Itapemirim, 2013. Disponível em: <https://multivix.edu.br/wp-content/uploads/2018/08/a-evolucao-da-internet-e-sua-influencia-na-comunicacao-mundial-e-na-escrita-formal.pdf>. Acesso em: 5 ago. 2026.

¹ Professor da Faculdade de Direito, *Campus* Rio Verde, Universidade de Rio Verde. E-mail: [acesse o artigo original para visualizar o e-mail](#)

² Professor da Faculdade de Engenharia de Software, *Campus* Rio Verde, Universidade de Rio Verde. E-mail: [acesse o artigo original para visualizar o e-mail](#)

³ Discente da Faculdade de Engenharia de Software, *Campus* Rio Verde, Universidade de Rio Verde. E-mail: [acesse o artigo original para visualizar o e-mail](#)

⁴ Discente da Faculdade de Engenharia de Software, *Campus* Rio Verde, Universidade de Rio Verde. E-mail: [acesse o artigo original para visualizar o e-mail](#)