**UNIVERSIDADE DE TAUBATÉ**
**HEMILI OLIVEIRA FERNANDES DA SILVA**

# LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE DA EVOLUÇÃO DO DIREITO FRENTE AO DESENVOLVIMENTO DA SOCIEDADE

**TAUBATÉ**
**2022**

**HEMILI OLIVEIRA FERNANDES DA SILVA**

# LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE DA EVOLUÇÃO DO DIREITO FRENTE AO DESENVOLVIMENTO DA SOCIEDADE

Trabalho de Graduação apresentado ao Departamento de Ciências Jurídicas da Universidade de Taubaté, para obtenção do título de Bacharel em Direito.

Orientador: Luiz Guilherme Paiva Vianna

**TAUBATÉ**

**2022**

**Grupo Especial de Tratamento da Informação - GETI**
**Sistema Integrado de Bibliotecas - SIBi**
**Universidade de Taubaté - UNITAU**

S586l Silva, Hemili Oliveira Fernandes da
Lei geral de proteção de dados : uma análise da evolução do direito frente ao desenvolvimento da sociedade / Hemili Oliveira Fernandes da Silva. -- 2022.
80f.

Monografia (graduação) - Universidade de Taubaté, Departamento de Ciências Jurídicas, 2022.
Orientação: Prof. Me. Luiz Guilherme Paiva Vianna, Departamento de Ciências Jurídicas.

1. Proteção de dados - Legislação - Brasil. 2. Tecnologia da informação. 3. Direito à privacidade. 4. Internet. 5. Lei geral de proteção de dados. I. Universidade de Taubaté. Departamento de Ciências Jurídicas. Curso de Direito. II. Título.

CDU - 343.232:004.738.5(81)

Ficha catalográfica elaborada pela Bibliotecária Regina Márcia Cuba – CRB 8ª/7416

**HEMILI OLIVEIRA FERNANDES DA SILVA**

# LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE DA EVOLUÇÃO DO DIREITO FRENTE AO DESENVOLVIMENTO DA SOCIEDADE

Trabalho de Graduação apresentado ao Departamento de Ciências Jurídicas da Universidade de Taubaté, para obtenção do título de Bacharel em Direito.

Orientador: Luiz Guilherme Paiva Vianna

Data: _____

Resultado: _____

COMISSÃO JULGADORA

Prof. _____ Universidade de Taubaté

Assinatura _____

Prof. _____ Universidade de Taubaté

Assinatura _____

À minha avó Maria de Nazaré, que sempre zelou pela minha educação.

## AGRADECIMENTOS

À Deus, inteligência suprema, por ter me capacitado a realizar este trabalho.

Ao meu orientador Professor Luiz Guilherme Paiva Vianna, pela paciência, orientação, apoio e atenção que me ajudaram a concluir este trabalho.

À Universidade de Taubaté, pelas inúmeras oportunidades concedidas, sem as quais eu não chegaria até aqui.

Aos demais professores, pela amizade, inspiração e conhecimentos compartilhados.

Aos meus amigos de sempre, pelo alívio cômico nesse ano difícil.

“Toda pessoa tem o direito de estar só e de excluir, do conhecimento de terceiros, aquilo que só a ela se refere e que diz respeito ao seu modo de ser no âmbito da vida privada” (BORGES, 2018).

## RESUMO

A presente pesquisa tem como escopo uma análise da evolução do direito frente ao desenvolvimento da sociedade, com atenção ao advento da Lei Geral de Proteção de Dados (LGPD). Acerca do tema, cabem as seguintes indagações: Quais motivos ensejaram a criação da LGPD? Seria a LGPD uma forma residual de responsabilidade, considerando o Marco Civil da internet no que concerne a este ponto? As empresas estão preparadas para se adequarem à LGPD? Entre outras perquirições. O objetivo geral da pesquisa é, por conseguinte, analisar a LGPD, seus aspectos e impacto no ordenamento jurídico, considerando sua notabilidade e atualidade. A criação da LGPD ratificou a proteção de dados pessoais entre os direitos e garantias fundamentais, e estabeleceu a competência privativa da União para legislar sobre a proteção e o tratamento de dados pessoais, isso para garantir que não haja risco de estados e municípios legislarem acerca do tema ou interferirem na aplicação da LGPD. A LGPD também trouxe maior proteção ao direito consumerista, acompanhando as necessidades do consumidor na sociedade moderna. Em resumo, com a LGPD, o país está imerso em uma estrutura nova de proteção de dados, estrutura essa que transcende o âmbito setorial, incluindo todo tratamento e coleta de dados dentro do território nacional, em consonância com a União Europeia, a quem a LGPD tomou como modelo, o RGPD (Regulamento Geral de Proteção de Dados) ou, sem traduzir, GDPR (*General Data Protection Regulation*). A LGPD é um retrato da evolução legal, vez que cuida da segurança e proteção do direito ao sigilo dos dados e informações no âmbito digital, todavia, ainda merece aprimoramento, principalmente no sentido da clareza e da aplicabilidade de suas disposições.



**Palavras-chave:** LGPD. Tecnologia da Informação. Direito. Privacidade. Internet.

***ABSTRACT***

The present research has as its scope an analysis of the evolution of Law in the face of society's development, with emphasis on General Data Protection Act (LGPD). Regarding the subject matter, the following questions are relevant: What reasons led to the creation of the LGPD? Would the LGPD be a residual form of responsibility, considering the Marco Civil da Internet in this regard? Are companies prepared to adapt themselves to the LGPD? Among other inquiries. The general objective of the research is, therefore, to analyze the LGPD, its aspects and impact on the legal system, considering its notability and relevance. The creation of the LGPD ratified the protection of personal data among fundamental rights and guarantees, and established the exclusive competence of the Union to legislate on the protection and processing of personal data, to ensure that there is no risk of states and municipalities legislating or interfering in the application of the GDPR. The LGPD also brought greater protection to consumer law, following consumer needs in modern society. In summary, with the LGPD, the country is immersed in a new data protection structure, that transcends the sectorial scope, including all data processing and collection within the national territory, in line with the European Union, to which the LGPD took as a model, the RGPD (General Data Protection Regulation). The LGPD is a portrait of legal evolution, as it takes care of the security and protection of the right to data confidentiality and information in the digital sphere, however, it still deserves improvement, mainly in the sense of clarity and applicability of its provisions.

***Keywords***: LGPD. Information Technology. Law. Privacy. Internet.

## LISTA DE QUADROS

## LISTA DE SIGLAS

| | |
|---|---|
| Art. | Artigo |
| IP | *Internet Protocol* |
| LGPD | Lei Geral de Proteção de Dados Pessoais |
| RGPD | Regulamento Geral de Proteção de Dados |

**SUMÁRIO**

# 1 INTRODUÇÃO

A tecnologia vem crescendo cada dia mais, e gradativamente surgem diversas inovações, notadamente no que concerne à tecnologia da informação. A utilização de recursos informáticos vem crescendo em grande escala, seja para pesquisas de grande importância, como também para condutas danosas, possibilitando que indivíduos possam cometer diferentes delitos pelas redes da internet, ou ainda que as empresas obtenham, indevidamente, os dados de indivíduos que não sejam seus usuários.

Tem-se a ideia errônea de que aquele que faz mal uso dos dados pessoais de terceiros, ou comete algum crime cibernético, tem certo anonimato, podendo praticá-los em qualquer lugar e por qualquer meio. Isso se deve ao fato de haver poucos profissionais plenamente capacitados para investigar esses tipos de delitos, o que torna os autores ainda mais aguerridos. Apesar disso, os atos cometidos por trás das telas têm tanto peso quanto os crimes cometidos fora da rede.

Nesse diapasão, a proteção de dados pessoais se converte na própria proteção da pessoa humana, sobretudo com relação ao amparo do livre desenvolvimento de sua personalidade e, especificamente, quanto a garantia da sua autodeterminação informacional (LIMA, 2020).

Para tal garantia foi criada a Lei Geral de Proteção de Dados (LGPD) publicada em 14 de agosto de 2018, de alcance nacional e interesse geral. Nesse interim, a LGPD trouxe regulamentação acerca do tratamento de dados com base em princípios, direitos e obrigações, o que foi de suma importância, considerando que dados pessoais são um dos ativos de maior valor na conjuntura atual.

A LGPD prevê a necessidade de consentimento livre e informado para o tratamento dos dados, porém, para que isso ocorra, é necessário se falar em reflexão e amadurecimento dos titulares dos dados para garantia da efetividade da previsão legal e o devido reconhecimento da dignidade da pessoa humana.

Acerca do instituto da dignidade da pessoa humana, a Carta Magna estabelece que todos são iguais perante a lei, sem distinção de qualquer natureza; prevê a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de eventual violação (BRASIL, 1988).

Destarte, a LGPD, em perfeita consonância com a Carta Magna, tem como

escopo primário a proteção dos direitos fundamentais contidos no art. 5º da Lei Maior. Contudo, há de se falar que a Lei Geral de Proteção de Dados veio para regulamentar a proteção dos dados e não para coibir.

Dessa forma, a LGPD resguarda a dignidade da pessoa humana e a livre iniciativa, claro que, de toda forma, protegendo mais o instituto jurídico de maior valor, qual seja, a dignidade da pessoa humana.

Acerca do tema, cabem as seguintes indagações, dentre outras futuras: Quais motivos ensejaram a criação da LGPD? Seria a LGPD uma forma residual de responsabilidade, considerando o Marco Civil da internet no que concerne a este ponto? As empresas estão preparadas para se adequarem à LGPD?

Aventou-se a hipótese de que o Marco Civil da Internet, Lei nº 12.965/2014, tentou garantir a limitação e o uso do consentimento para acessos a dados pessoais, como se vê no art. 7º em seus incisos de VII à X.

Defendeu-se, também, a hipótese de que muito tem se discutido acerca da competência para processamento, julgamento e responsabilidade desses crimes, pois o atual Código Penal adotou a Teoria da Ubiquidade e neste caso a competência seria do Brasil, mas também teria a hipótese do vazamento ou furto de dados atingir vários locais, e daí seria a competência do local do resultado, foi levantada até mesmo a hipótese da competência parcial, para os casos em que o crime começa no exterior mas os resultados são gerados no Brasil.

O objetivo geral da pesquisa é, por conseguinte, analisar a LGPD considerando os aspectos que a cercam, sua notabilidade e atualidade. Pretende-se, para tanto, expor de forma clara os fundamentos principiológicos trazidos pela LGPD; considerar de maneira sistemática as etapas da implementação da LGPD no ordenamento, tratando, inclusive, das profissões criadas para atender ao disposto nesta; demonstrar de forma clara a importância da implementação do tratamento adequado de dados pessoais; tratar das possíveis penalidades em caso de tratamento inadequado de dados pessoais, e, ainda, em caso de vazamento; e apresentar respostas às questões propostas nesta introdução, assim como também responder às questões que vierem a surgir no curso do desenvolvimento da pesquisa.

A relevância da pesquisa possui dupla dimensão: científica e social. No que concerne à contribuição ao conhecimento científico, qualquer estudo que se preocupe em colocar em relevo novas abordagens sobre a LGPD, ou que ampliem as abordagens já existentes, é pertinente, uma vez que a proteção de dados tem por

objetivo garantir e proteger as liberdades públicas e os direitos fundamentais das pessoas singulares e, em particular, a sua honra e integridade pessoal e familiar.

Em razão das lacunas existentes e em um amplo processo de entendimento, a presente pesquisa objetiva contribuir com o despertar do senso crítico, de forma a popularizar a LGPD para conscientização dos cidadãos brasileiros acerca da importância do tratamento adequado dos dados pessoais.

Como metodologia, foi adotada a pesquisa bibliográfica. Foi realizada ainda a leitura crítica, a redação de resumos e paráfrases das obras pertinentes ao enfrentamento do tema e à comprovação das hipóteses. Além da leitura de livros pertinentes ao objeto de pesquisa, foram consultados apontamentos e jurisprudência disponíveis *online*, devidamente relacionados.

Seguem, por fim, a conclusão e as referências.

## 2 DADOS PESSOAIS E A CULTURA DA INFORMAÇÃO

Os dados pessoais são o objeto jurídico tutelado pela Lei Geral de Proteção de Dados Pessoais (LGPD). No entanto, muitas pessoas ainda não têm certeza no que exatamente “dados pessoais” ou “dados de caráter pessoal” consistem. Não há uma lista definitiva do que são ou não dados pessoais, então tudo se resume a interpretar corretamente a definição da LGPD.

Diniz (2018, p. 233) informa que: “dados pessoais são qualquer tipo de dados que podem ser usados para identificar direta ou indiretamente uma pessoa (titular dos dados)”. Assim, dado pessoal é qualquer tipo de informação relativa a pessoas singulares ou identificáveis, tanto no que diz respeito à sua identidade como às suas profissões e situação pessoal.

Alguns exemplos de dados pessoais são nome, fotografia, número de telefone, endereço físico (que permite a identificação direta), bem como endereço IP (*Internet Protocol*) ou nome de utilizador (que permite a identificação indireta).

A coleta, processamento e armazenamento de dados pessoais são estritamente regulamentados pela LGPD. Portanto, é importante saber exatamente como seu provedor de análise digital coleta, gerencia e armazena dados pessoais. O uso de dados pessoais também deve ser documentado e claramente divulgado aos usuários finais (MOROZOV, 2019).

Por sua vez, Doneda (2020) define os dados pessoais de um indivíduo como qualquer informação relativa a uma pessoa singular identificada ou identificável.

Pessoa singular identificável é aquela que pode ser identificada, direta ou indiretamente, por referência a um identificador, por um identificador online, ou por um ou mais fatores específicos do estado físico, fisiológico, genético, mental, identidade econômica, cultural ou social dessa pessoa singular (RODOTA, 2020).

Do ponto de vista da natureza das informações, os subsídios pessoais incluem tanto informações objetivas, como a presença de determinadas substâncias no sangue, quanto informações subjetivas, como opiniões ou avaliações. Se considerar o formato ou meio em que as informações são encontradas, os dados pessoais podem incluir informações disponíveis em qualquer forma, por exemplo, alfabética, numérica, entre outros (SMALL; VORGAN, 2019).

Por fim, do ponto de vista do conteúdo da informação, o conceito de dados pessoais inclui dados que fornecem qualquer tipo de informação. De acordo com

Gonçalves (2018), essas informações não precisam necessariamente se limitar à vida privada e familiar do indivíduo para que caiam no domínio dos dados pessoais, e é aí que os “identificadores” aparecem.

Identificadores, como o próprio nome sugere, são informações a partir das quais uma pessoa pode ser identificada, uma vez que mantém uma relação privilegiada e próxima com o interessado (OLTRA, 2021).

Explana-se que o novo alcance oferecido ao conceito de “dados pessoais” reafirma um dos principais objetivos da LGPD: proteger os direitos e liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais (GARCIA, 2020).

Nesse sentido, para garantir que qualquer estabelecimento que processe dados pessoais na União, seja como controlador ou processador de dados, cumpra o disposto na LGPD, foram estabelecidas multas mais severas para os infratores (MOROZOV, 2019). Entretanto, essas penalidades serão esclarecidas mais à frente.

Os dados pessoais referem-se basicamente a qualquer informação sobre uma pessoa viva, onde essa pessoa é identificada ou pode ser identificada. Eles podem abranger vários tipos de informações, como nome, data de nascimento, endereço de *e-mail*, número de telefone, endereço, características físicas ou dados de localização, desde que seja claro a quem essa informação se refere, ou se for razoavelmente possível descobrir (GARCIA, 2020).

Segundo Inellas (2019), os dados pessoais não precisam estar em forma escrita, também podem ser informações sobre a aparência ou o som de um titular de dados, por exemplo, fotos ou gravações de áudio ou vídeo, mas a LGPD se aplica apenas quando essas informações são processadas de maneira automatizada (por exemplo, eletronicamente) ou como parte de algum outro tipo de sistema de arquivamento (BRASIL, 2014).

A LGPD rege as situações em que os dados pessoais são “tratados”. Processar basicamente significa usar dados pessoais de qualquer forma, incluindo; coletar, armazenar, recuperar, consultar, divulgar ou compartilhar com outra pessoa, apagar ou destruir dados pessoais. A utilização de dados pessoais não é possível sem o consentimento do titular (BRASIL, 2014).

Insta consignar que a LGPD não se aplica quando isso é feito para atividades puramente pessoais ou domésticas (BRASIL, 2014).

As organizações geralmente coletam muitos tipos diferentes de informações sobre pessoas e, mesmo que uma informação não identifique alguém, ela pode se tornar relevante quando relacionada com outras informações.

Por exemplo, um controlador de dados que solicita informações sobre pessoas que baixam produtos de seu *site* pode solicitar que indiquem sua ocupação (MOROZOV, 2019). Contudo, isso não está incluído no escopo de dados pessoais da LGPD porque, muito provavelmente, um cargo não é exclusivo de uma pessoa.

Da mesma forma, uma organização pode perguntar para qual empresa determinada trabalha, o que, novamente, não pode ser usado para identificar alguém, a menos que seja o único funcionário (RODOTA, 2020).

No entanto, em muitos casos, essas informações podem ser usadas em conjunto para reduzir o número de pessoas físicas vivas a ponto de estabelecer razoavelmente a identidade de alguém.

## 2.1 TIPOS DE DADOS PESSOAIS

A LGPD faz uma distinção entre três tipos de dados pessoais: “dados pessoais gerais ou comuns” (que não necessitam de medidas especiais de proteção); os “dados pessoais de categorias especiais” (também chamados de dados especialmente protegidos ou dados sensíveis); e “dados pessoais de natureza criminosa” (BRASIL, 2014).

Inellas (2019) descreve o primeiro tipo de dados, dados pessoais gerais ou comuns, que são quaisquer dados pessoais que não estejam incluídos nas categorias de dados especiais são considerados dados pessoais gerais ou comuns.

Dados pessoais comuns podem incluir detalhes de identificação pessoal, como nome e endereço, relacionamentos com clientes, finanças pessoais, questões fiscais, dívidas, dias de doença, circunstâncias relacionadas ao trabalho, circunstâncias familiares, residência, automóvel, qualificações, aplicativos, *curriculum vitae*, data de emprego, cargo, área de trabalho, telefone comercial, dados-chave: nome, endereço, data de nascimento, endereço IP ou outras informações não confidenciais semelhantes (NIGRI, 2016).

O segundo tipo, os dados pessoais de categorias especiais, são dados notadamente protegidos, considerando sua sensibilidade. São dados de categorias especiais os que se referem a:

| |
|---|
| **Origem étnica ou cultural**: Este tipo de dado refere-se à raça ou etnia das pessoas. A etnia é a crença subjetiva em uma origem comum. Essa crença pode ser baseada em semelhanças na aparência externa, costumes, idioma, religião ou memória de eventos históricos, como migrações. |
| **Opiniões políticas, religiosas e filosóficas**: Isso inclui todos os dados referentes à religião ou crença de uma pessoa e suas opiniões políticas. |
| **Orientação sexual**: São os dados sobre orientação sexual e gênero. Estes são aspectos importantes da identidade. |
| **Filiação a sindicato**: Os dados sobre filiação a sindicato são dados que indicam se uma determinada pessoa é membro de um sindicato. |
| **Dados genéticos**: São dados pessoais relacionados com as características genéticas herdadas ou adquiridas de uma pessoa singular que fornecem informação única sobre a fisiologia ou saúde dessa pessoa singular e que resultam, nomeadamente, de uma análise de uma amostra biológica da pessoa física em questão. Isso inclui análise cromossômica, de DNA ou RNA, ou qualquer outro tipo de análise que permita obter informações equivalentes. Quando as informações genéticas forem anonimizadas, deixarão de ser consideradas dados pessoais. |
| **Dados biométricos**: Os dados biométricos são dados pessoais resultantes de um tratamento técnico específico relacionado com as características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitem ou confirmam a identificação única dessa pessoa singular, tais como imagens faciais ou dados dactiloscópicos (impressões digitais) ou análise de assinaturas manuscritas. Dados de categoria especial são considerados quando sua finalidade é identificar exclusivamente uma pessoa física (por exemplo, em controles de acesso). |
| **Dados relacionados com a saúde**: Dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde. Podem referir-se ao estado de saúde passado, atual ou futuro. Ele não cobre apenas detalhes específicos de condições médicas, testes ou tratamentos, mas inclui quaisquer dados relacionados que revelem algo sobre o estado de saúde de uma pessoa. Portanto, os dados de saúde podem incluir uma ampla gama de dados pessoais, por exemplo: Qualquer informação sobre lesões, doenças, deficiências ou riscos de doenças, incluindo histórico médico, opiniões médicas, diagnóstico clínico e tratamento; Dados de exames médicos, resultados de testes, dados de dispositivos médicos ou dados de rastreadores *fitness;* e Informações coletadas do indivíduo ao se registrar nos serviços de saúde ou no acesso ao tratamento. |
| **Detalhes de compromissos, lembretes e contas que dizem algo sobre a saúde da pessoa:** Estes se enquadram na "prestação de serviços de saúde", mas devem revelar algo sobre o estado de saúde de uma pessoa. Por exemplo, uma consulta com o médico de família ou o hospital em isolamento não lhe dirá nada sobre a saúde de uma pessoa, pois pode ser uma consulta para acompanhamento ou avaliação. No entanto, se pode razoavelmente inferir dados de saúde do livro de consultas de uma pessoa em uma clínica de osteopata ou de uma conta de uma série de sessões de fisioterapia. |

Quadro 1: Categorias de dados especiais
Fonte: Inellas (2019, p. 331)

Observa-se que são dados protegidos pois revelam informações que podem ter impacto nos direitos e liberdades fundamentais dos indivíduos, expondo-os potencialmente à discriminação e, portanto, devem ser tratados com maior cuidado e maiores medidas de proteção aplicadas.

O último tipo se refere aos Dados pessoais de natureza criminosa. De acordo com Nigri (2016), os dados pessoais sobre queixas criminais, processos ou condenações não são dados de categoria especial. No entanto, regras e salvaguardas semelhantes estão em vigor para processar esse tipo de dados, para lidar com os riscos específicos associados a eles.

Para processar dados pessoais sobre condenações ou infrações criminais, é necessário ter uma base legal e uma autoridade legal ou autoridade oficial para o processamento. Também se pode processar esse tipo de dados se tiver autoridade oficial para fazê-lo porque está processando os dados em uma capacidade oficial. Outrossim, não se pode manter um registro completo de condenações criminais, a menos que o faça em uma capacidade oficial (SMALL; VORGAN, 2019).

No que se refere ao tratamento de dados pessoais, deve ser levado em consideração toda e qualquer etapa de tratamento de tais dados. Isso inclui a coleta, registro, sistematização, armazenamento, pesquisa, uso, divulgação ou exclusão de dados pessoais.

A LGPD exige que se leve em consideração como os dados são usados para tomar decisões sobre pessoas específicas. Nesse interim:

> As informações que não se qualificam como dados pessoais para uma organização podem se tornar dados pessoais se uma organização diferente as possuir com base no impacto que esses dados podem ter no indivíduo (WANDERLEI, 2021, p. 192).

Assim, tudo depende do motivo pelo qual a organização está processando os dados.

Corroborando o acima exposto, exemplifica-se que:

> Em primeiro lugar, uma foto de uma rua nas mãos de um fotógrafo não é um dado pessoal, ao passo que essa mesma foto nas mãos de um investigador que está trabalhando para identificar as pessoas e veículos que estavam presentes naquela rua naquele momento específico consideraria dados pessoais dos interessados. Em segundo lugar, a videovigilância ou imagens de segurança cujo único propósito seja a identificação de indivíduos quando e onde as autoridades considerem adequado devem ser considerados como tratamento de dados sobre indivíduos identificáveis, mesmo que, em alguns

> casos, os indivíduos registados não possam ser identificados (WANDERLEI, 2021, p. 199).

Se uma organização processa dados com o único propósito de identificar alguém, então os dados são, por definição, dados pessoais.

A esse respeito Doneda (2020, p. 200) versa: “Se não tiver certeza se as informações que armazena são dados pessoais ou não, é melhor errar por cautela”. Isso significa garantir que o processamento de dados pessoais seja limitado ao necessário e reter os dados apenas enquanto cumprirem sua finalidade.

Por sua vez, Gonçalves (2018) reforça que também deve considerar seriamente a pseudonimização e/ou criptografia das informações, especialmente se envolver categorias especiais de dados pessoais.

A pseudonimização mascara os dados substituindo as informações de identificação por identificadores artificiais. E muito embora seja essencial proteger os dados e possa ajudar a proteger a privacidade e a segurança dos dados pessoais, a pseudonimização tem seus limites, por isso a LGPD também menciona a criptografia (BRASIL, 2014).

A criptografia também oculta informações substituindo os identificadores por outra coisa. Mas enquanto a pseudonimização permite que qualquer pessoa com acesso aos dados veja parte do conjunto de dados, a criptografia permite que apenas usuários aprovados acessem o conjunto de dados completo (GARCIA, 2020).

Acredita-se que a pseudonimização e a criptografia podem ser usadas simultaneamente ou separadamente, mas a regra geral é que tanto o controlador quanto o processador devem tomar medidas de segurança técnicas e organizacionais apropriadas com base em uma avaliação de risco específica. A avaliação pode implicar que sejam tomadas medidas físicas ou técnicas específicas, como o fechamento das instalações e outras medidas para garantir que pessoas não autorizadas não possam acessar dados confidenciais (MOROZOV, 2019).

Em sua forma mais básica, os dados não pessoais são qualquer conjunto de dados que não contenha informações de identificação pessoal (RODOTA, 2020).

Em essência, isso significa que nenhum indivíduo ou pessoa viva pode ser identificada olhando para esses dados.

Por exemplo, embora os detalhes do pedido coletados por um serviço de entrega de alimentos contenham o nome, idade, sexo e outras informações de contato de uma pessoa, eles se tornarão dados não pessoais sem identificadores como nome e informações de contato.

Os dados não pessoais foram classificados em três categorias principais: dados não pessoais públicos, dados não pessoais da comunidade e dados não pessoais privados:

> Todos os dados coletados pelo governo e suas agências, como censos, dados coletados por empresas municipais sobre o total de receitas tributárias em um determinado período, ou qualquer informação coletada durante a execução de todas as obras financiadas com recursos públicos, foram mantidos sob o guarda-chuva de dados públicos não pessoais.
> Todos os identificadores de dados sobre um conjunto de pessoas que têm a mesma localização geográfica, religião, trabalho ou outros interesses sociais comuns formarão a comunidade de dados não pessoais. Por exemplo, metadados coletados por aplicativos de transporte, empresas de telecomunicações, empresas de distribuição de eletricidade e outros foram incluídos na categoria de dados comunitários não pessoais pelo comitê.
> Dados privados não pessoais podem ser definidos como dados produzidos por indivíduos que podem ser derivados da aplicação de software ou conhecimento proprietário (WANDERLEI, 2021, p. 203).

À risca, nem todos os dados de uma pessoa física são considerados pessoais. Por exemplo, os dados anonimizados não são considerados dados pessoais desde que não seja possível reidentificar a pessoa física a que se referem. Também não são considerados dados pessoais aqueles referentes a pessoas jurídicas, incluindo o nome e forma da pessoa jurídica e seus dados de contato.

No entanto, consideram-se dados pessoais os relativos a empresários individuais e profissionais liberais que possam ser tratados com base em interesse legítimo, desde que não seja feito para estabelecer uma relação com eles fora da referida condição (MOROZOV, 2019).

Em outras palavras, a LGPD deve ser rigorosamente observada quando esses dados forem relacionados a pessoas físicas. Abaixo, quadro expositivo de termos de suma importância relacionados ao tema:

| **DADOS PESSOAIS** |
|---|
| **O que são dados pessoais?**<br>São informações sobre pessoas físicas ou jurídicas. Pode ser qualquer tipo de informação: dados de identidade, endereço, dívidas, etc. |
| **A que dados se refere a lei de dados pessoais?**<br>Aos dados pessoais armazenados em arquivos, registros, bancos de dados públicos ou privados e que são armazenados para fornecer relatórios. |

**A minha imagem nos vídeos do sistema de vigilância também é um dado pessoal?**

Sim.

**Os dados biométricos são dados pessoais?**

Sim. Os dados biométricos são um tipo de dados pessoais obtidos através de um tratamento técnico específico. Eles estão relacionados às características físicas, fisiológicas ou comportamentais de uma pessoa humana que permitem sua identificação única.

**Que direitos esta lei reconhece em relação aos meus dados pessoais?**

A lei reconhece o seu direito a:

- que seus dados pessoais não sejam usados ou registrados sem o seu consentimento;

solicitar e receber informações sobre quais dados pessoais seus estão registrados em bancos de dados públicos ou privados;

- solicitar que seus dados sejam corrigidos ou atualizados;

solicitar a sua eliminação, nos casos em que corresponda;

- solicitar que sejam mantidos em sigilo; e

- iniciar uma ação judicial para conhecer seus dados ou exigir sua retificação, exclusão, confidencialidade ou atualização.

**O meu consentimento é sempre necessário para que uma base de dados inclua os meus dados pessoais?**

Sim. Exceto quando:

- seus dados foram obtidos de fontes publicamente acessíveis;

- os seus dados foram recolhidos para o exercício de funções dos poderes do Estado ou por obrigação legal;

- os seus dados constam de listas que se limitam aos dados do nome, documento de identidade nacional, identificação fiscal ou da segurança social, profissão, data de nascimento e morada;

- os seus dados foram obtidos por uma relação contratual, científica ou profissional e são necessários para o seu desenvolvimento ou cumprimento;

- trata das operações realizadas pelas entidades financeiras e das informações que recebem de seus clientes; e

- um órgão público que obteve seus dados no exercício de suas funções os transfere para outro órgão público para usá-los para uma finalidade que esteja dentro de suas funções.

**CADASTRO DE DADOS PESSOAIS**

**Pode haver registro de dados referentes à origem racial ou étnica, opiniões políticas, convicções religiosas, filosóficas ou morais, filiação sindical ou que estejam relacionadas à saúde ou à vida sexual?**

Não. Esses dados são chamados *de dados confidenciais* e ninguém pode forçá-lo a fornecê-los. Também não podem ser registados, salvo por motivos de interesse geral autorizados por lei.

**Os meus dados biométricos são dados sensíveis?**

Os dados biométricos que identificam uma pessoa são dados sensíveis apenas quando podem revelar outros dados e o uso desses outros dados pode levar à discriminação. Por exemplo, quando os dados biométricos revelam a etnia ou fornecem informações sobre a saúde de uma pessoa.

| |
|---|
| **Se eu pedir para conhecer meus dados pessoais registrados em um banco de dados, eles são obrigados a me fornecer a informação?**<br>Sim. O responsável pela base de dados deve fornecer gratuitamente a informação no prazo de 10 dias corridos a partir do momento em que a solicitou. |
| **Pode haver registro de antecedentes criminais ou de contravenção?**<br>Sim, mas só podem ser detidos pelas autoridades públicas competentes, no âmbito das leis. |
| **Os herdeiros de uma pessoa falecida podem pedir para serem informados dos dados que registaram sobre a pessoa falecida?**<br>Sim. |
| **Por quanto tempo as empresas que fornecem informações sobre conformidade de crédito podem manter meus dados?**<br>Apenas por 5 anos. Se você cancelou sua dívida, esse prazo é reduzido para 2 anos e seu pagamento deve ser registrado. |
| **Que obrigações têm os responsáveis pelos registos de dados pessoais?**<br>Para além de respeitarem os direitos sobre os seus dados pessoais e fornecerem-lhe as informações que solicita, devem expor os direitos reconhecidos por lei sobre os seus dados pessoais em local visível e claro. Ao exibir a informação sobre os seus direitos, devem também informar que a Agência de Acesso à Informação Pública é o órgão onde pode apresentar reclamações e reclamações para proteger os seus dados pessoais. Todas essas informações devem estar disponíveis antes que eles levem seus dados. |
| **ACESSO À INFORMAÇÃO** |
| **Como eles devem me dar a informação?**<br>À sua escolha: por escrito, por meio eletrônico, telefone, imagem ou outro meio. Eles sempre têm que lhe dar as informações de forma clara e em uma linguagem acessível ao conhecimento médio da população |
| **Se os dados cadastrados estiverem errados, desatualizados ou não apropriados para serem cadastrados, o que posso fazer?**<br>Você sempre pode pedir que corrijam o erro ou atualizem as informações. No caso de dados confidenciais, você pode exigir que eles sejam excluídos ou mantidos em segredo. Os responsáveis pelo banco de dados devem corrigir o erro em até 5 dias úteis após o envio da reclamação. O procedimento é gratuito. |
| **O que acontece se me impedirem de conhecer os meus dados pessoais ou se recusarem a corrigi-los?**<br>Em ambos os casos, você pode registrar uma reclamação na Agência de Acesso à Informação Pública. Você também pode iniciar a ação de proteção de dados pessoais. |

| |
|---|
| **Como posso aceder aos meus dados pessoais registados nos sistemas de videovigilância?**<br>Para aceder a estes dados deve: provar sua identidade; indique a data e hora aproximadas em que sua imagem pode ter sido capturada; e fornecer as informações necessárias para que possam identificar sua imagem. |
| **Como o responsável pelo banco de dados deve me fornecer as informações quando eu quiser acessar meus dados registrados em vídeos do sistema de vigilância?** |
| O responsável pela base de dados deve:<br>- fornecer seus dados pessoais de forma clara;<br>- informar a hora e o local onde sua imagem foi gravada;<br>- informar para que finalidade sua imagem foi registrada;<br>- informá-lo sobre o destino dos dados salvos e possíveis atribuições;<br>- dar-lhe arquivo impresso ou digital a imagem que eles capturaram. Esta possibilidade é excecional e só corresponde se explicar os motivos pelos quais pretende ter a imagem nesse formato e pagar o custo do procedimento;<br>- informá-lo claramente que se não ficar satisfeito com a resposta, pode apresentar uma reclamação junto da Direção Nacional de Proteção de Dados Pessoais ou iniciar uma ação de *habeas data*; e<br>- ter em mente que se você solicitar sua imagem impressa ou digital e outra pessoa também aparecer, o responsável pelo banco de dados deve aplicar alguma técnica que permita que as imagens sejam separadas para que apenas a sua possa ser identificada. |
| **PROCESSAMENTO DE DADOS AUTOMATIZADO** |
| **O que posso fazer se uma decisão tomada com base no tratamento automatizado dos meus dados pessoais me prejudicar?**<br>Se o responsável pela base de dados tomar decisões com base exclusivamente no tratamento automatizado dos seus dados e isso o prejudicar, pode pedir-lhe que explique claramente a lógica que aplicou para tomar essa decisão. |
| **ROUBO DE IDENTIDADE** |
| **O que é roubo de identidade?**<br>O roubo de identidade ocorre quando alguém se passa por você usando seu documento de identidade. Por exemplo, se seu documento foi roubado e usado para comprometê-lo fazendo um empréstimo ou obtendo cartões de crédito, celulares, etc. Você pode registrar uma reclamação na Agência de Acesso à Informação Pública. |
| **AUTORIDADE DE EXECUÇÃO** |
| **Quem é a autoridade de aplicação desta lei?**<br>Autoridade Nacional de Proteção de Dados Pessoais (ANPD). Esta Agência deve controlar a proteção integral dos dados pessoais armazenados em arquivos, registros, bancos de dados ou outros meios técnicos de processamento de dados, públicos ou privados, destinados a fornecer relatórios. Deve garantir o direito à honra e privacidade das pessoas e acesso à informação |

Quadro 2: Cumprimento da LGPD
Fonte: Wanderlei (2021, p. 212)

Ante ao exposto, entende-se que os dados pessoais são todas as informações relativas a uma pessoa singular identificada ou identificável. Uma pessoa é considerada identificável quando sua identidade pode ser determinada direta ou indiretamente por meio de qualquer informação.

Existem também dados que se referem a aspetos mais sensíveis, sendo os que se referem à esfera mais íntima do seu titular, ou cuja utilização indevida pode dar origem a discriminação ou implicar um risco grave para o mesmo. De forma enunciativa, mas não limitativa, são considerados sensíveis dados pessoais que possam revelar aspectos como origem racial ou étnica, estado de saúde, informações genéticas, crenças religiosas, filosóficas e morais, opiniões políticas e preferência sexual.

## 2.2 RECONHECIMENTO TORNA HIERARQUICAMENTE SUPERIOR NO ORDENAMENTO JURÍDICO, ACIMA DE OUTRAS LEIS

Recentemente, em 10 de fevereiro de 2022, foi promulgada a Emenda Constitucional 115/2022, que incluiu a proteção de dados pessoais no rol de direitos e garantias fundamentais.

Nigri (2016) relembra que a inviolabilidade da vida privada dos indivíduos já fazia parte no rol dos direitos fundamentais no art. 5º, inciso X, da Constituição Federal, *in verbis*: “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, p. 5).

Além disso, o direito à vida privada é reconhecido também no art. 21 do Código Civil, *in verbis*: “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” (BRASIL, 2002, p. 21).

Entretanto, apenas agora incluiu-se o inciso LXXIX da Carta Magna, *in verbis*:

> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022)
> § 1º As normas definidoras dos direitos e garantias fundamentais têm aplicação imediata.

> § 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte.
> § 3º Os tratados e convenções internacionais sobre direitos humanos que forem aprovados, em cada Casa do Congresso Nacional, em dois turnos, por três quintos dos votos dos respectivos membros, serão equivalentes às emendas constitucionais (Incluído pela Emenda Constitucional nº 45, de 2004) (Vide ADIN 3392) (Vide Atos decorrentes do disposto no § 3º do art. 5º da Constituição)
> § 4º O Brasil se submete à jurisdição de Tribunal Penal Internacional a cuja criação tenha manifestado adesão (Incluído pela Emenda Constitucional nº 45, de 2004) (BRASIL, 1988, p. 5).

De modo que tal inciso foi criado para tratar especificamente do direito à proteção dos dados pessoais, inclusive nos meios digitais.

Igual importância teve o estabelecimento da competência da União de organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei (art. 21, inciso XXVI), *in verbis*: XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei (Incluído pela Emenda Constitucional nº 115, de 2022) (BRASIL, 1988, p. 21).

Bem como da competência privativa da União de legislar sobre proteção e tratamento de dados pessoais (art. 22, inciso XXX). XXX - proteção e tratamento de dados pessoais (Incluído pela Emenda Constitucional nº 115, de 2022) (BRASIL, 1988, p. 22).

Isso, sem dúvida, auxiliará na necessária uniformidade do tratamento do tema em todo o território nacional.

O reconhecimento de um direito como fundamental incide em considerá-lo hierarquicamente superior no ordenamento jurídico, supra outras leis (constitucionais e infraconstitucionais). Destarte, a proteção de dados foi uniformizada com outros direitos fundamentais, o que fortalece as disposições da LGPD.

Os sujeitos responsáveis ou obrigados que devem garantir o direito à proteção de dados pessoais são: Poder Executivo, Prefeituras Municipais, Partidos Políticos, Poder Legislativo, Órgãos Autônomos, Poder Judicial, Universidades e Instituições Públicas de Educação Superior e Fundos Públicos.

Diniz (2018, p. 255) assim versa: “Você é o proprietário dos seus dados pessoais, quem decide sobre o seu tratamento, a quem os entrega, para quê, quando e com que finalidade”.

Por vezes os indivíduos se deparam com a necessidade de fornecer seus dados pessoais para diversos fins, seja para realizar um procedimento, contratar um

serviço ou comprar um item. No entanto, ao coletar e processar seus dados pessoais, tais sujeitos devem obrigatoriamente observar os princípios: qualidade, consentimento, finalidade, legalidade, proporcionalidade, responsabilidade, lealdade e informação.

As instituições públicas devem divulgar os seus “avisos de privacidade”, pelos meios eletrônicos e físicos de que dispõem, nos quais é informado o titular dos dados pessoais, a finalidade, o tratamento, as transferências que podem ser efetuadas, dos mesmos, bem como os meios para exercer o direito de acesso, retificação, cancelamento e oposição dos dados pessoais.

É abissal a recente jornada brasileira da matéria de proteção de dados até presentemente, alcançando cada vez mais legitimidade e relevância na sociedade, agora excelsa a um elemento de política de Estado, celebrada como um direito fundamental. Ao Estado agora cabe zelar pela máxima eficácia e efetividade de tal direito, para que os indivíduos possam usufruir de todos os benefícios descritos acima.

## 2.3 A CULTURA EM RELAÇÃO À PROTEÇÃO DE DADOS PESSOAIS

Parece que hoje vivencia-se um virtual ciberutopismo (fé cega na rede), pois compartilha-se demais na rede (*oversharing*) às vezes ignorando os riscos que podem advir disso (MOROZOV, 2019). Razão pela qual é necessário estabelecer uma cultura em termos de proteção de dados.

Por isso, de acordo com Gonçalves (2018, p. 355): “Em um primeiro momento, os indivíduos devem se questionar: o que se entende por cultura em termos de proteção de dados pessoais?”.

O mesmo autor responde que se trata do conjunto de conhecimentos, opiniões, práticas ou comportamentos que uma pessoa tem sobre o tratamento e proteção da sua informação pessoal (dados pessoais) (GONÇALVES, 2018).

Do exposto, conclui-se que uma cultura de proteção de dados pessoais (informações pessoais), deve atender a uma dupla perspectiva: jurídica (conhecimento) e social (opiniões, práticas ou comportamentos) (RODOTA, 2020).

Em relação à abordagem jurídica, trata-se de ter uma visão sobre um sistema jurídico, seja como um todo ou em relação a setores ou aspectos particulares dele (OLTRA, 2021).

Em termos de proteção de dados, não basta apenas ensinar à população, mesmo aos interessados no assunto, a existência de um marco regulatório, trata-se também de mostrar-lhes os principais componentes e seus conteúdos (GARCIA, 2020).

Em outras palavras, em termos de proteção de dados pessoais, é importante o seu reconhecimento como prerrogativa fundamental, a titularidade dos mesmos, o responsável pelo seu tratamento e a proteção oferecida pelas autoridades na matéria. Portanto, o ensino do direito à proteção de dados pessoais não deve se limitar apenas a isso, mas também abranger seu conteúdo essencial, sua conexão com os princípios e valores contidos nos textos constitucionais, bem como sua relação com outros Direitos.

Assim sendo, a abordagem estudada deve ser projetada na forma como a cultura jurídica em matéria de proteção de dados deve ser compreendida e ensinada, ou seja, seu passado, presente e futuro (MOROZOV, 2019).

Por outro lado, explana Doneda (2020), em relação à abordagem social, esta permitirá não só conhecer o caminho que a proteção de dados pessoais percorreu no campo jurídico, que sem dúvida, se originou como consequência do fenômeno tecnológico, mas também permitirá conhecer essa nova etapa da humanidade, ou seja, a nova vida social influenciada pelo crescente uso e desenvolvimento da tecnologia.

À vista disso, a perspectiva social da cultura em termos de proteção de dados no presente é regida por opiniões, práticas ou condutas:

> O exposto torna-se evidente quando os indivíduos expressam nas redes sociais e na internet o que pensam, sentem e fazem em seu cotidiano, o que, no passado, só era conhecido por si mesmo ou por um grupo muito pequeno de pessoas. No entanto, agora a realidade é outra, isto, em consequência da incessante inovação científica e tecnológica, significa uma mudança que está a afetar não só as vidas, mas também a própria privacidade (WANDERLEI, 2021, p. 214).

Por isso e, em uma perspectiva sociológica do comportamento social e dos efeitos de poder compreender este novo ambiente de comunicação e expressão, é preciso dizer que os indivíduos agem seguindo determinados padrões de comportamento socialmente transmitidos, como está acontecendo com os migrantes digitais (os nativos digitais são todas aquelas pessoas nascidas desde meados da década de 1990. Enquanto isso, os imigrantes digitais são o resto dos mortais que

nasceram antes dos nativos digitais e que tiveram que se adaptar a esse novo ambiente digital (SMALL; VORGAN, 2019).

Neste novo ambiente digital, para ser aceito dentro de um novo grupo social, o indivíduo tem que se adaptar às novas práticas sociais que foram estabelecidas, uma vez que se vive em uma revolução a que se chama “internet social”, pelo fato de ser um meio através do qual se pode não só obter informação, mas também adaptar-se às novas realidades, a sua utilização permite a recolha, tratamento e transmissão de uma grande quantidade de informações, inclusive referentes à própria pessoa, pois, em cada conexão feita, o indivíduo deixa rastros que podem ser captados por inúmeros atores (OLTRA, 2021).

As redes sociais não são exceção, através delas também é possível obter informações valiosas sobre a própria pessoa.

Sem dúvida, a realidade que a comunidade social enfrenta hoje é aquela que tem a ver com o uso e implementação de tecnologia e tecnologia da informação, que está se tornando um estilo de vida que não é mais apenas típico dos Estados e das empresas, mas é até mesmo para pessoas.

Portanto, é necessário que os governos adotem posições favoráveis à proteção dos direitos dos cidadãos, para que possam enfrentar a evolução tecnológica. Em particular, pelos órgãos ou instituições responsáveis pela proteção da proteção de dados pessoais (MOROZOV, 2019).

Assim, uma cultura em termos de proteção de dados deve atender basicamente a situações muito precisas, como promover a educação e a cultura dos cidadãos sobre a importância de proteger sua privacidade na internet e nas redes sociais, bem como o uso e alcance da tecnologia; fornecer informações mais transparentes e adequadas por parte dos prestadores de serviços aos cidadãos; o estabelecimento de medidas de proteção da privacidade e a atribuição de maiores responsabilidades aos prestadores de serviços; bem como o ensino e desenvolvimento de um quadro normativo que esteja de acordo com os tempos.

# 3 DO DIREITO À PRIVACIDADE E A PROTEÇÃO DOS DADOS PESSOAIS

## 3.1 DIREITOS INERENTES À PERSONALIDADE E À PRIVACIDADE

Quando se trata da privacidade, tem-se a necessidade imperiosa de fomentar que é praticamente impossível sua definição exata. Cada país tem seu conceito de privacidade, o modo oriental e o modo ocidental de sociedade são muitas vezes extremos, assim como o conceito de privado e público para estes. E, muitas vezes, este conceito se altera entre países vizinhos, devido a cultura e as relações sociais.

O vocábulo “privacidade”, vem do latim, mais precisamente do verbo *privare*, cuja forma adjetiva é *privatus* e *privacy* (o mesmo que intimidade) (TARTUCE; CASTILHO, 2016).

O termo não se trata apenas da “privacidade” propriamente dita, vai muito além disso, segundo Pereira (2020), quando se fala em privacidade, podem ser lembrados os termos: vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e outros menos utilizados, como privatividade e privaticidade, por exemplo.

Apesar da profunda importância da privacidade e do crescimento de questões jurídicas a ela relacionadas, tentativas de definição desse Direito Fundamental pecam por tentar encontrar um conceito unitário, passível de ser aplicado a quaisquer situações.

A Carta Magna de 1988 incluiu o assunto em seu artigo principal, o art. 5º, inciso X, nas Garantias e Direitos Fundamentais, com a proteção da “intimidade” e da “vida privada”, in verbis: “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, p. 5), além de outros dois termos relacionados, como “honra” e “imagem”, igualmente colocados no Código Civil de 2002.

Martins (2020) versa que os diversos “significados”, tanto no Brasil como no mundo, não distorcem a sua realidade, pelo contrário, alimentam ainda mais o seu objetivo e enobrece o estudo sobre da privacidade.

Quanto a personalidade, Beviláqua (2017, p. 223) afirma que: “A personalidade jurídica é mais do que um processo superior da atividade psíquica, é uma criação social, exigida pela necessidade de pôr em movimento o aparelho jurídico, e que, portanto, é modelada pela ordem jurídica”.

Por sua vez, Limongi (2018, p. 221) retrata como que: “O atributo de personalidade é toda característica, situação ou condição, suscetível de ser assumida pela personalidade, e que seja capaz de ocasionar uma repercussão jurídica”.

Já Gomes (2018, p. 842) discorre que: “A personalidade é um atributo jurídico. Todo homem, atualmente, tem aptidão para desempenhar na sociedade um papel jurídico, como sujeito de direito e obrigações”.

No que lhe toca, Miranda (2012, p. 211) versa que: “A personalidade é a possibilidade de esse encaixar em suportes fáticos, que, pela incidência das regras jurídicas, se tornem fatos jurídicos. Portanto, a possibilidade de ser sujeito de direito”.

Outrossim, o direito à privacidade é um dos Direitos da Personalidade mais importantes para a vida humana. De modo que existem três campos que o incidem, diretamente, de uma relação jurídica: a própria pessoa; a pessoa ampliada na família; e o mundo exterior (BIONI, 2020).

No que tange ao mundo exterior, o direito à privacidade se traduz diretamente aos Direitos Patrimoniais e aos Direitos Familiares (WANDERLEI, 2021).

Neste diapasão, Limongi (2018, p. 293) estabelece, ainda, que: “Os Direitos de Personalidade dizem-se as faculdades jurídicas cujo objeto são os diversos aspectos da própria pessoa do sujeito, bem assim da sua projeção essencial no mundo exterior”.

É nesta ideia basilar de Direitos da Personalidade que o trabalho traz a essência do direito à privacidade, estendendo-o após a morte da pessoa.

Dessa forma, o Direito da Personalidade humana se faz presente em diversos subsistemas do ordenamento jurídico brasileiro, tais como: Direito Civil, Constitucional, Penal, Administrativo, entre outros:

> O Direito da Personalidade está em tudo o que co-envolve a necessidade de indagar qual a tutela da personalidade humana, no conjunto da atual ordem jurídica. Se bem que essa busca é potenciada, face ao que se propôs, em função da ulterior determinação da hermenêutica da tutela geral da personalidade no âmbito das relações civis (CAMPOS, 2017, p. 455).

Haja vista, o Direito da Personalidade emerge de uma comum e abrangente concepção jurídica do homem e das relações humanas, traduzida uma unificante ponderação de interesses, em termos de se poder dizer que é a mesma emanação de poder humano juridicamente reconhecido, que é tutelada nos diferentes ramos da ordenação jurídica.

Ademais, durante muito tempo, os Direitos da Personalidade, com ênfase no direito à privacidade foram considerados apenas no campo do Direito Público, em traços históricos não lineares. Mas com o passar dos tempos a tutela pública começou a ter resultados insuficientes, devido à excessividade das normas de Direito Público inconiventes com os outros direitos das pessoas (PAESANI, 2020).

Por muito tempo, também, teve-se firmado de que os Direitos da Personalidade seriam, tão somente, aqueles abarcados pelo ordenamento. Ou seja, os Direitos Positivados.

Contudo, o Direito Privado, bem como a evolução da sociedade, mostrou que o positivismo não é absoluto:

> Recoloca-se aqui a velha questão de se saber se direito é só aquilo que está na lei, ou se existem faculdades jurídicas que, não previstas embora no ordenamento, se tornam sancionáveis em virtude de sua definição em outra forma de expressão do Direito (BORGES, 2018, p. 304).

Dessa forma, existem Direitos Privados da Personalidade definidos fora das leis que regem a sociedade, reconhecidos pelos costumes e pelo Direito Científico.

Para ser mais claro, Gonçalves (2018) diz que atualmente o Código Civil, enumerados pelos artigos 11 a 21, não se traduzem como os únicos Direitos da Personalidade, ou seja, não são taxativos, e reforça que novos direitos estão surgindo com o escopo da personalidade, como será visto pela LPGD.

A generalidade das especificações dos Direitos da Personalidade é preocupante por ser de difícil menção, mas de fato devem ser agrupados de acordo com os aspectos que cada um abarca (BORGES, 2018).

A esse respeito, Limongi (2018) alude estes aspectos de três formas diferentes: o físico, o intelectual e o moral. Portanto, há a especificação entre o direito à integridade física, o direito à integridade intelectual e o direito à integridade moral.

Estes direitos não são “conservadores” e podem participar de mais de uma forma na sua essencialidade, como o direito à imagem, que pode ser colacionado nos direitos de natureza moral como física, mas podem ser trazidos dentro de classes conforme à sua natureza dominante (TOLEDO, 2017). Assim, a tutela da privacidade teve seus passos até a tutela absoluta.

Sabidamente, o direito tenta amoldar-se a realidade fática da sociedade e relativizar a proteção do sujeito de direitos. Nesse interim, a tutela da privacidade pode

ser conceitualizada como de outra ordem, direcionada, principalmente, à informação e condicionadas pela tecnologia.

No âmbito desse condicionamento tecnológico, a internet não exige apenas novas soluções jurídicas para os novos problemas, ela também afeta a maneira como os problemas e as soluções jurídicas devem ser analisados. Ao romper com os paradigmas jurídicos tradicionais e desafiar os mecanismos convencionais de tutela, a rede *online* representa um dos principais objetos de estudo dos doutrinadores preocupados com essa nova realidade (LEONARDI, 2020).

Assim, atualmente, a principal dificuldade que permeia a tutela da privacidade é o oferecimento de propostas e soluções que sejam eficientes para os novos problemas. Dessa forma, novos mecanismos jurídicos deverão ser criados e um "meio termo" deve ser encontrado, em todas as relações, para que o direito prevaleça de forma a trazer cooperação e ética (BORGES, 2018).

Portanto, o jurista deve se precaver e se preocupar com as mudanças tecnológicas decorrentes da globalização, pois a exposição indesejada é facilmente divulgada pelos meios tecnológicos, como também, intrusão as residências, violação de correspondência, divulgação da imprensa, ou seja, pelos meios mais clássicos de violação da privacidade nos dias atuais. São os novos tempos do direito à privacidade.

## 3.2 BREVE PANORAMA DO DIREITO À PRIVACIDADE

A necessidade de privacidade é uma característica humana, razão pela qual há preocupação direta com o Direito à Privacidade e sua devida tutela.

Diversas vezes, tal preocupação se relaciona e tem como escopo a busca de calmaria e do abrigo. Mas, em outras vezes, a busca da privacidade se molda na tentativa da igualdade e da liberdade, e não tão longínquo apresenta-se elo à personalidade e ao seu desenvolvimento em um emaranhado de relações a serem abarcadas pelo direito (BORGES, 2018).

Enfim, o direito à privacidade protege do conhecimento alheio o modo de ser da pessoa.

Tal paradigma é reflexo de outrora, em que não havia espaço para a tutela jurídica da privacidade, pois exercia-se outros meios de regulação, dada a rigorosa hierarquia social presente à época, ou até na questão da arquitetura dos espaços, tanto públicos, como privados (GARCIA, 2017).

Ademais, pode-se dizer que havia neutralização do ordenamento jurídico por ter cunho patrimonialista ou corporativo. Ou o caso da tutela da privacidade ser apenas um sentimento subjetivo, não digno de uma tutela fundamental (BORGES, 2018).

Na contemporaneidade a cumplicidade entre a proteção da privacidade e a da propriedade teve então início, assumindo diversas conotações, dependendo do momento e do ponto de vista assumido:

> Se é o da exclusão, o da dicotomia entre situações subjetivas patrimoniais e não patrimoniais, do direito subjetivo, da exploração econômica ou da eficiência. Nos países do *commom law*, por exemplo, é fato que a base da elaboração jurisprudencial das regras de proteção da *privacy* baseiam-se na proteção da propriedade privada, em especial nos institutos de *trespass, nuisance* e *conspiracy*. No Brasil, nota-se que a inviolabilidade do domicílio e da correspondência, nas quais se incluem o direito à privacidade, estão presentes em todas as Constituições brasileiras, desde a Constituição do Império de 1824 (BULOS, 2019, p. 222).

Interpreta-se que a tutela da privacidade, na atualidade, não é mais apenas patrimonialista e não abarca apenas isolamento e tranquilidade.

Corroborando o acima exposto, Martins (2020, p. 232) afirma que: “A inserção de um direito à privacidade em ordenamentos de cunho eminentemente patrimonialista fizera dela uma prerrogativa reservada a extratos sociais bem determinados”.

Entretanto, houve o despertar do direito para com a privacidade, na qual a mudança se deu em um momento de alterações da percepção humana pelo ordenamento, e em consequência seguiu-se a juridicização de diversos aspectos do dia-a-dia, mesmo sendo de certa forma individualista (TOLEDO, 2017).

Com o direito à privacidade já, devidamente, estabelecido como um Direito Fundamental nos dias atuais, poucos, mas existentes traços individualistas ainda são notáveis.

Entretanto, de acordo com Gonçalves (2018), não é espantosa essa notabilidade, devido as individualidades na relação vital, e também, pelo direito ter sido originado em aspectos burgueses, ou seja, na segunda metade do século XIX, no auge do liberalismo jurídico clássico.

Em conseguinte, estas mesmas relações foram potencializadas pelo desenvolvimento e aumento dos fluxos de informações, e consequentemente, surgiram importantes passos para a sociedade democrática vislumbrar outras liberdades fundamentais do direito.

Desse modo, o “elitismo” do acolhimento da privacidade ficou marcado nos tribunais até por volta da década de 1960, com as mudanças e desdobramentos da sociedade, a relação entre Estado e cidadão, as reivindicações da classe operária, e o crescimento do fluxo das informações, que é consequência direta do desenvolvimento tecnológico, na qual se teve maior recolhimento e processamento da informação (PAESANI, 2020).

Com o consequente aumento do fluxo de informações, as importâncias destas informações aumentaram, por conseguinte. Ou seja, deixam de conter a privacidade oferecida apenas àquele seleto grupo elitista, passando a ser tida por uma maior parcela da sociedade, em gamas de igualdade (BULOS, 2019).

Pode-se estabelecer, de início, que dois fatores estão entre as justificativas para a utilização de informações pessoais, o controle e a eficiência:

> Inicialmente o Estado percebeu que seria capaz de utilizar em grande escala das informações pessoais. E são motivos considerados cristalinos, pois a simples menção de que a Administração Pública deve ser eficiente, torna este conhecimento acurado, na qual, por exemplo, muito se viu na concretização de pesquisas, e com a consequente “mudança” conforme estas seriam realizadas, para que seja demonstrada a eficiência. Quanto ao controle, este já era tido de várias formas pelo Estado. O controle social apenas foi potencializado, pois aumentou-se o controle sobre a população com o abarcamento dos dados destes, como é visto nos países com regimes considerados totalitários (BULOS, 2019, p. 222).

Observa-se que uma série de interesses se articulam em torno desses dois fatores, seja envolvendo o Estado ou então entes privados, interesses sobre os quais é útil traçar uma síntese preliminar, para maior aprofundamento.

Saindo da esfera estatal, o apreço dos organismos privados na utilização e guarda das informações era bem rara. Tal atividade não era atraente para os privados pelos seus altos custos, tanto para o tratamento dos dados quanto pela própria dificuldade para sua coleta. Custos estes que poderiam parecer mais interessantes ao Estado, seja pelo seu poder econômico, pelos interesses específicos ou por maior escala (DONEDA, 2020).

Entretanto, essa utilização centralizada no âmbito estatal durou até o desenvolvimento de tecnologias que possibilitaram sua coleta e processamento por grandes organismos particulares. Contudo, não se justificou apenas pela redução considerável dos custos, mas sim pela forma diversa da utilização das informações (SZANIAWSKI, 2015).

Assim, a importância da informação acompanhou a tecnologia, tornando-a útil e de baixo custo.

Contudo, tais mudanças quantitativas culminaram em mudanças qualitativas, alterando o equilíbrio na equação poder-informação-pessoa-controle:

> Uma das chaves para compreender esta estrutura, e talvez a mais rica em evidências para as finalidades, é a consciência do papel da técnica e de como utilizá-la para uma eficaz composição jurídica do problema da informação. Deve-se verificar como o desenvolvimento tecnológico age sobre a sociedade e, consequentemente, sobre o ordenamento jurídico. Há de se considerar o seu potencial para imprimir suas próprias características ao meio sobre o qual se projeta, e não somente ressaltar as possibilidades latentes neste meio (CAMPOS, 2017, p. 459).

Haja vista, a vontade da elaboração da técnica se entranhou em diversas instâncias da sociedade, moldando-se a ditames, na qual se buscava vantagens, como: agilidade, maior eficiência ou infalibilidade.

Mas, dada privacidade, com o passar do tempo, foram noticiados alguns mitos sobre seu fim ou sobre a elaboração de *dossiers*. “Outros “mitos” relacionados à privacidade pertencem igualmente à mesma ordem de ideias como, por exemplo, a noção de que grandes bancos de dados centralizados seriam as grandes ameaças à privacidade (BORGES, 2018).

Certamente o processamento distribuído “democratizou” esta arquitetura, fragmentando o tratamento de dados pessoais, porém as questões referentes aos grandes bancos de dados continuam pertinentes e presentes, por exemplo, nas discussões referentes à adoção de um número de identificação único ou de cartas de identidade digitais. Além do que as vantagens em termos de desempenho e custos que proporciona a computação distribuída, *grid computing*, certamente contribuirão para tornar tais raciocínios ainda mais relativos e cinzentos (PAESANI, 2020).

Em um cenário como este, ressurgem ideias e grandes propostas para discussão, como sobre os fenômenos tecnológicos, o que ocasiona diretamente um avanço à vista. Mas, o seu fundamento principal não deixou de existir, pois: “Toda pessoa tem o direito de estar só e de excluir, do conhecimento de terceiros, aquilo que só ela se refere e que diz respeito ao seu modo de ser no âmbito da vida privada” (BORGES, 2018, p. 304).

Dessa forma, com os avanços tecnológicos, a preocupação com os sinais das mudanças e as necessidades jurídicas, fizeram com que se criassem “barreiras virtuais”, que extrapolam os limites geográficos e espaciais.

Pinheiro (2020) diz que parece ter chegado a um momento inicial de maturação da relação entre a técnica e os valores presentes no ordenamento jurídico, no qual deixa de existir uma clara escolha entre o apoio às novas tecnologias ou a sua recusa.

Nota-se que com o desenvolvimento tecnológico há um reforço dos mecanismos existentes e estes procuram propagar o espaço de coexistência as novas tecnologias, mas sempre buscando o máximo respeito aos Direitos Fundamentais.

Cabe ressaltar, com positividade, que não houve uma ruptura entre a privacidade de outras épocas com a privacidade de agora, mas sim uma continuidade histórica da tutela, e com isso, alterações conforme a sociedade civil e a sociedade da informação (TARTUCE; CASTILHO, 2016).

Nas últimas décadas, a privacidade criou um elo entre diversos interesses, o que, consequentemente, ocasionou na mudança da sua substância, ou seja, de seu perfil. E com estas mutações por conta do desenvolvimento e da sociedade informacional, o eixo “pessoa-informação-segredo”, se consagrou no mais novo eixo “pessoa-informação-circulação-controle” (BIONI, 2020).

Assim, a tutela da privacidade abarca, juntamente com outros Direitos da Personalidade, com a ideia de fundamentação, excluindo de vez o posicionamento majoritário do “elitismo” e do egoísmo. Antes era a tranquilidade e o isolamento, agora uma criação de uma esfera privada própria, tendo um elo entre a comunicação própria e no relacionamento dos demais.

Algo que ocorreu paradoxalmente a proteção da privacidade na sociedade da informação é a proteção dos dados pessoais. Essa ampliação das funções dos dados pessoais, é considerada uma característica dos “novos direitos”. Mas tal posição será devidamente debatida mais à frente, em um tópico específico (BORGES, 2018).

Em conseguinte, com os avanços tecnológicos e com sua inclusão no meio eletrônico, houve o fenômeno da convergência, pois antes grande parte do que havia era de vigilância física ou psicológica, passando a tomar a forma de vigilância sobre os dados pessoais.

Corroborando o exposto, Beviláqua (2017, p. 308) versa que: “Antigamente, não existia essa imensa preocupação com a proteção da vida privada do indivíduo, visto que não haviam meios de comunicação de massa”.

Ficava a questão da informação em um plano secundário, o que não ocorre nos dias atuais. Com isso, há mais um marco na força de expansão, e, assim, sua consequente evolução do tratamento do direito da privacidade no ordenamento jurídico. Dessa forma, o que antes era definido e restritivo apenas na tutela penal ou na tutela de um direito subjetivo, toma corpo, se caracteriza e consolida como um Direito Fundamental.

É justamente neste desenvolvimento como um Direito Fundamental que se percebe que a necessidade de funcionalização levou ao seu desdobramento, em consonância com boa parte da experiência doutrinaria, legislativa e jurisprudencial.

Este desdobramento verifica-se, por exemplo, pela forma com que o tema foi tratado na elaboração da recente Carta dos Direitos Fundamentais da União Europeia (hoje também parte integrante do projeto de Tratado Constitucional da União europeia), cujo art. 7º trata do já tradicional direito ao “respeito pela vida familiar e privada”; ao passo que seu art. 8º é dedicado especificamente à “proteção dos dados pessoais (SZANIAWSKI, 2015).

A Carta dos Direitos Fundamentais da União Europeia acaba marcando a complexidade da privacidade em dois grandes pontos: em um primeiro momento na questão da tutela individualista; e em um segundo momento tem como objeto o dinamismo dos dados pessoais e suas várias facetas (SZANIAWSKI, 2015).

Ou seja, com a continuação da preocupação com a privacidade, o que se alterou um pouco foram os meios. Mas, o que não ocasionou a perda ou ruptura de sua fundamentação e o respeito do Princípio da Dignidade do ser humano.

Daí a necessidade de superar a ordem de conceitos pela qual o direito à privacidade era limitado por uma tutela de índole patrimonialista, e de estabelecer novos mecanismos e institutos para possibilitar a efetiva tutela dos interesses da pessoa.

Ademais, a privacidade deve ser debatida também no âmbito coletivo. Neste sentido, a responsabilidade civil não pode ser levada ao esquecimento, pois é a solução para uma gama de problemas, e consideravelmente um avanço na tutela oferecida pelo ordenamento.

No direito brasileiro a proteção da pessoa humana é assegurada com valoração máxima e no caso da privacidade como um Direito Fundamental. No Brasil, o problema privacidade avançou em passos mais curtos por conta do problema estrutural e do desenvolvimento social lento, e consequentemente, a preocupação da sociedade para

com a privacidade, em seguida, principalmente, na questão dos dados pessoais, eram quase esquecidos (TOLEDO, 2017).

Porém, por mais que a sociedade brasileira não dê o devido tratamento aos dados pessoais e a privacidade, não quer dizer que este direito será tratado como de menor importância, pois os Direitos Fundamentais não são de maior ou menor magnitude, e sim compõem uma teia de direitos essenciais e uníssonos:

> A conotação contemporânea da proteção da privacidade, que se manifesta sobretudo (porém não somente) através da proteção de dados pessoais; e que deixa de dar vazão somente a um imperativo de ordem individualista, mas passa a ser a frente de onde irão atuar vários interesses ligados à personalidade e às liberdades fundamentais da pessoa humana, fazendo com que na disciplina da privacidade passe a se definir todo um estatuto que acaba por compreender as relações da própria personalidade com o mundo exterior (CAMPOS, 2017, p. 572).

Quando se fala de privacidade nos dias atuais, não se trata somente de ter sigilo ou caráter confidencial de fatos pessoais, mas sim de informações sobre si próprio que são armazenadas e na maioria das vezes compartilhadas com terceiros, e, não menos importante, da manutenção destas informações para que sejam sempre atualizadas e verdadeiras.

A privacidade adota, assim, um caráter relacional, com o âmago da própria personalidade com o das outras pessoas e, consequentemente, com o mundo exterior, mas pontuando que a pessoa tem os poderes para originar a sua inclusão e exposição.

## 3.3 PROTEÇÃO DE DADOS PESSOAIS COMO NOVO ELEMENTO DE TUTELA PESSOAL

O conceito da privacidade evoluiu de tal forma, que não ficou somente no usual, de imagens e intimidades serem violadas por *paparazzis,* mas avançou nas situações cotidianas e também no mundo tecnológico, com a coleta dos dados pessoais, além de seus processamentos e transferências por órgãos particulares e públicos.

A expressão “dados” é de origem latina e inglesa, e que dizer *data*, e significa “as informações que passaram por tratamento, seja por meio eletrônico ou não” (GOMES, 2018, p. 65).

O avanço tecnológico e a busca pelo tratamento automatizado de informações pessoais mudaram o elo entre as pessoas, as empresas, o Estado e os direitos à privacidade. Assim, houve um aumento de informações pessoais nas mãos de alguns para uso em proveito próprio.

Como exposto, o uso destas informações pessoais repercute diretamente nos seus titulares, consequentemente, afetando os principais Direitos da Personalidade.

Neste diapasão, em vários países, principalmente em países mais desenvolvidos e com uso maior e constante da tecnologia, surgem grandes iniciativas para estabelecer normas a respeito desta utilização, muitas vezes indevidas, das informações pessoais e da privacidade:

> A partir de 1970, esta tendência consolidou-se com o amadurecimento, em diversos países, de normativas que vieram a tratar especificadamente da proteção de dados pessoais; normativas estas que comungavam dos mesmos princípios e técnicas desde a sua gênese e que, a despeito das diversas particularidades regionais a serem levadas em conta, possuem até hoje uma certa uniformidade. A presença de alguns princípios centrais de proteção de dados pessoais é uma tendência que é confirmada, hoje, por uma série de instrumentos normativos transacionais que tratam da matéria (CAMPOS, 2017, p. 600).

Nesta temática, o que se vê no Brasil é uma certa demora para principiar e legislar sobre o assunto, devido ao atraso no desenvolvimento e o uso da tecnologia pela sociedade brasileira (WANDERLEI, 2021).

Em contrapartida, em países desenvolvidos houve uma clara tendência normativa sobre a proteção dos dados pessoais. Entretanto, nos dias atuais, a legislação sobre a proteção dos dados pessoais não se concentra mais em países desenvolvidos, abarcando boa parte dos países do mundo, demonstrando uma autonomia da temática da proteção dos dados pessoais, transformando em uma tendência já enraizada na sociedade da informação.

Com esse desenvolvimento da matéria, a busca da tutela se tornou mais eficaz e também abarcou a matéria aos Direitos Fundamentais, criando-se gerações de leis sobre o assunto.

Gonçalves (2018) menciona que a primeira geração de leis era composta de preceitos que elucubravam o estado da tecnologia e a visão do jurista à época, na qual grandes centros elaboradores de dados concentravam as coletas de dados, e que posteriormente foram para o controle dos órgãos públicos.

Assim, criaram um elo com o Estado que eram seus destinatários principais (ou único) destas normas.

Porém, como a falta de conhecimento do uso indiscriminado em conjuntura com as suas consequências, fez com que surgissem princípios de proteção, com foco primordial na atividade de processamento de dados, mas não interligados diretamente a proteção dos dados pessoais ou do direito da privacidade (TARTUCE; CASTILHO, 2016).

Estas leis de primeira geração rapidamente se tornaram ultrapassadas, conforme o avanço tecnológico que aumentou significativamente a cada ano, avançando, assim, para a segunda geração no final da década de 70 (PAESANI, 2020).

A característica básica que diferencia tais leis das anteriores é que sua estrutura não gira mais em torno do fenômeno computacional em si, mas da consideração da privacidade e da proteção dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão (o que é patente na própria denominação da lei francesa) (PEREIRA, 2020).

Esta evolução é baseada principalmente na insatisfação dos cidadãos, que são a base da proteção dos dados pessoais, pois havia uso de terceiros de seus dados pessoais, e a carência de meios para defenderem seus interesses eram necessários. Além disso, os centros de tratamento de dados pessoais, como já mencionados, sofreram grave fragmentação, resultando em leis inviáveis para a época (DONEDA, 2020).

Assim, o sistema foi elaborado para que o cidadão tivesse meios de identificar o uso indevido de seus dados pessoais.

Certamente, afirma Martins (2020), estas leis tinham seus problemas a serem enfrentados, mas houve uma revolução sistêmica e também da forma do cidadão pensar sobre os dados pessoais, pois o que era considerado exceção se tornou regra, tornando requisito essencial da vida social.

Dessa forma, o Estado, assim como os entes privados, começou a usar o fluxo de informações pessoais como forma de funcionamento de suas engrenagens.

Dando sequência, com a chegada da década de 80, houve a mudança para a terceira geração que procurou cada vez mais a tutela dos dados pessoais, concentrando-se, principalmente, no cidadão e criando meios melhores não

focalizados apenas na liberdade de fornecer ou não os próprios dados pessoais, mas sim na efetivação desta liberdade (LIMA, 2019).

A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e leva em consideração o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes, proporcionando o efetivo exercício da autodeterminação informativa (TARTUCE; CASTILHO, 2016).

O direito à autodeterminação informativa tem seu início com uma base extensiva das liberdades presentes nas leis da geração anterior, na qual era prerrogativa de alguns que definiam afrontar os custos econômicos e sociais do exercício destas prerrogativas (WANDERLEI, 2021).

Como tinha enfoque em “alguns”, esta geração exclusivista deu lugar a quarta geração de leis de proteção de dados, na qual muito se vê nas legislações atuais de diversos países, procurando sempre suprir as desvantagens do caráter individualista que existia até o surgimento desta geração (TARTUCE; CASTILHO, 2016).

Entre as técnicas utilizadas:

> Estas leis procuravam fortalecer a posição da pessoa em relação às entidades que coletam e processam seus dados, reconhecendo um desequilíbrio nesta relação que não era resolvido por medidas que simplesmente reconheciam o direito à autodeterminação informativa. Outra técnica é, paradoxalmente, a própria redução do papel da decisão individual de autodeterminação informativa. Isto ocorre por conta do pressuposto que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, que não pode ser conferida exclusivamente a uma decisão individual pela dificuldade de se tenha uma real noção dos efeitos decorrentes do tratamento de dados, como é o caso para certas modalidades de utilização de dados sensíveis (BORGES, 2018, p. 309).

Assim, o enfoque principal das leis era no problema integral da informação, pois não se pode apenas basear a tutela, de tais leis, na escolha individual, mas sim mecanismos que tornem o molde coletivo de proteção.

Essa busca pelo ordenamento justo e protetivo é observado nos países que legislam sobre o assunto, com princípios em comum, e com a forma positivista de elencar tais tutelas, com a consolidação da proteção da pessoa e com os Direitos Fundamentais (BIONI, 2020).

Pode-se abarcar sete princípios que acompanharam, em sua maioria, as gerações da proteção de dados pessoais, como:

> Princípio da Transparência, na qual um banco de dados deve informar a autoridade competente de sua existência, o que irá abarcar e emitir relatórios periódicos, ou seja, ser de conhecimento público e notório.
> Princípio da Qualidade, como o próprio nome diz, é o meio de coletar e tratar os dados de forma cuidadosa e de correção, com grande qualidade e fiéis a realidade.
> Princípio da Finalidade, este é de uma grandeza necessária, pois este princípio tem a essência da utilização dos dados pessoais, e esta deve ser conforme comunicada ao interessado, na prática tem bastante relevância também, pois fundamenta-se na restrição de transferência de dados a terceiros, e a valorar a razoabilidade da utilização de certos dados para uma finalidade especifica.
> Princípio do Livre Acesso, primordial para o uso e tratamento dos dados pessoais, pois o indivíduo deve ter acesso a base de dados onde seus dados estão armazenados, na qual poderá controla-los, e consequentemente, realizar imperfeições e correções das informações, ou até acrescentar dados.
> Princípio da Segurança Física e Lógica, como o nome diz, deverá ter uma grade segurança, tanto física como de acesso remoto, contra riscos de extravio, destruição, entre outros.
> Princípio da Proporcionalidade, na qual os dados só podem ser tratados se tiver relevância direta com a finalidade para a qual foram coletados, evitando-se certos abusos de seu uso.
> Princípio da Necessidade, muito parecido com o princípio da proporcionalidade, pois os dados deverão serem coletados e tratados, somente os que são necessários para a determinada finalidade, na qual deverão ser descartados todos que se tornarem excessivos (BIONI, 2020, p. 91).

Todos estes princípios, mesmo que adaptados ou divididos, são basilares de variadas leis, tratados, convenções ou acordos entre privados no tocante a proteção dos dados pessoais, formando um núcleo da tutela da proteção dos dados pessoais.

A aplicação de tais princípios, no entanto, é a parte mais aparente de uma tendência à autonomia da proteção de dados pessoais e a sua consideração como um Direito Fundamental em diversos ordenamentos (TARTUCE; CASTILHO, 2016).

Haja vista, é possível considerar a Convenção de Estrasburgo como o principal marco de uma abordagem da matéria pela chave dos Direitos Fundamentais. Em seu preâmbulo, a Convenção clarifica que a proteção de dados pessoais está diretamente ligada à proteção dos Direitos Humanos e das liberdades fundamentais, entendendo-a como pressuposto do estado democrático e trazendo para este campo a disciplina, evidenciando sua deferência ao art. 8º da Convenção Europeia para os Direitos do Homem (GARCIA, 2017).

## 3.4 DA TUTELA DOS DADOS PESSOAIS NO BRASIL

Como já mencionado, o Brasil “engatinhou” a passos curtos no caminho da importância da proteção dos dados pessoais na sociedade da informação. Reconhece-se que ainda há muito o que se fazer, mas grandes nomes da doutrina e e igualmente grandes pesquisadores do assunto trabalham, intensivamente, para trazer uma norma de caráter geral sobre a proteção de dados pessoais.

Durante anos o único mecanismo de proteção dos dados pessoais foi o Código de Defesa do Consumidor, em seus arts 43 e 44, com exceção do *habeas data,* regulada pela Lei n. 9.507, de 12 de novembro de 1997, mas que não obtiveram resultados significativos para a elaboração de uma lei geral sobre ao assunto (TARTUCE; CASTILHO, 2016).

Neste sentido, destacam-se os esforços que visam à consolidação de um marco normativo próprio e autônomo sobre proteção de dados pessoais no ordenamento, com a promulgação de leis que tratam de forma direta, ainda que setorial, da proteção de dados pessoais, como a Lei do Cadastro Positivo (Lei 12.414, de 2011), a Lei de Acesso à Informação (Lei 12.527, de 2011) e o Marco Civil da Internet (Lei 12.965, de 2014) (SZANIAWSKI, 2015).

Todas estas normas trazem, de forma clara, alguns dos princípios de proteção de dados pessoais aqui abordados.

### 3.4.1 PROTEÇÃO DE DADOS PESSOAIS NO CÓDIGO DE DEFESA DO CONSUMIDOR

Nos artigos citados acima, há a regulação breve e geral da manutenção dos bancos de dados e cadastros dos consumidores, garantindo diversos direitos a estes, respeitando em boa parte os princípios norteadores da tutela de proteção de dados.

De acordo com Martins (2020), a transparência é respeitada no intuito do consumidor ser comunicado, antecipadamente, que certa informação a seu respeito está sendo usada, tratada, conforme artigo 43, §2ª, *in verbis*: “§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele” (BRASIL, 1990, p. 43). De modo que, a comunicação nunca deve ser feita depois de processada.

Outros direitos do consumidor elencados no Código de Defesa do Consumidor, no tocante a proteção de dados pessoais é o da retificação, caso em que o consumidor deverá ter acesso a qualquer dado que diz respeito a ele, com opção de retificá-lo e

alterá-lo, tal qual reza o art. 43, *caput* e §3º, *in verbis*: “§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas (BRASIL, 1990, p. 44).

De modo que se trata do direito de acesso, que corresponde diretamente ao Princípio do Livre Acesso.

Assim, nas presunções de negação ao cumprimento destes direitos, o consumidor tem o *habeas data* e procedimentos ordinários na legislação consumerista, no art. 43, §4º, *in verbis*: “§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público (BRASIL, 1990, p. 45).

Em conseguinte, nos §§1º, 5º e 6º do artigo 43, *in verbis*:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> § 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
> .
> [...]
> .
> § 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
> § 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor (Incluído pela Lei nº 13.146, de 2015) (Vigência) (BRASIL, 1990, p. 1).

Tais incisos trazem que a clássica informação negativa não poderá ser armazenada por mais de cinco anos no que restrinja a concessão de crédito.

O Código de Defesa do Consumidor por anos fora usado como mecanismo de proteção de dados pessoais, como também para elaboração de diversas outras leis, mas este somente não sustenta a importância da tutela da proteção dos dados pessoais.

### 3.4.2 PROTEÇÃO DE DADOS PESSOAIS NA LEI DO CADASTRO POSITIVO

Por mais que o enfoque deste trabalho não se prolongue no sentido de adimplemento de obrigações financeiras, salienta-se que a Lei n. 12.414 de 2011 trouxe avanços significativos na proteção de dados pessoais, pois fora promulgada vinte e cinco anos após o Código de Defesa do Consumidor, o que fez com que se conjecturasse no ordenamento, como um exemplo de proteção de dados pessoais.

Um dos avanços significativos desta Lei é que somente com o consentimento do titular dos dados que se pode abrir o cadastro positivo, paradoxalmente ao caso do cadastro negativo (GARCIA, 2017).

A citada lei postou, pela primeira vez, o Princípio da Finalidade no ordenamento brasileiro, tanto em seu art. 2ª, I e V, como no art. 7º e de forma direta no art. 5º, VII, como se vê, *in verbis*: "Art. 5º. São direitos do cadastrado: VII – ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados" (BRASIL, 2011, p. 5).

Trata-se de um passo importante da relação da proteção dos dados pessoais, com a autodeterminação informacional. São também elencados outros princípios nesta lei, como o do livre acesso, que deverão ser gratuitos e incondicionados (art. 5º, II), e da qualidade dos dados (art. 9º, §2º) (BRASIL, 2014).

### 3.4.3 PROTEÇÃO DOS DADOS PESSOAIS NO MARCO CIVIL DA INTERNET

O Marco Civil da Internet, Lei n. 12.965, de 23 de abril 2014, é a norma legal que disciplina o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem faz uso da rede, bem como da determinação de diretrizes para a atuação do Estado.

O Marco Civil da Internet não pode ser classificado como uma norma geral de proteção de dados pessoais, mas é um dos maiores avanços da proteção no ordenamento brasileiro, como se vê já no início da lei, em seu art. 3, *in verbis*:

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

> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (BRASIL, 2014, p. 3).

O citado artigo trata de como a proteção dos dados pessoais e da privacidade são princípios da utilização da internet no Brasil.

A separação dos princípios da privacidade e da proteção dos dados pessoais é proposital, pois uma por mais que abarque a essência da outra, deverá e terá tratamento diverso, com conjecturas próprias e com a finalidade de Direitos Fundamentais (TARTUCE; CASTILHO, 2016).

Beviláqua (2017) compara que a base desta separação remete a Carta de Direitos Fundamentais da União Europeia, na qual usou em artigos distintos cada proteção (arts. 7 e 8).

Registra-se, contudo, que a recém-aprovada legislação veio congregar a referida atenção especial à proteção dos dados pessoais, após os escândalos de espionagem revelados por Edward Snowden, quando alguns dispositivos relacionados a tal matéria foram inseridos em consonância com a demanda internacional colocada a respeito da proteção dos dados pessoais (SZANIAWSKI, 2015).

O artigo do Marco Civil da Internet que se relaciona com os Princípios da Proteção de Dados Pessoais que merece destaque é o art. 7 da lei, na qual concentra de forma direta e preventiva os direitos e garantias do titular dos dados pessoais, como se vê no inciso VIII, *in verbis*:

> VIII – informações claras e completas sobre a coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> Justifiquem sua coleta;
> Não sejam vedadas pela legislação; e
> Estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet (BRASIL, 2014, p. 7).

Claramente, o que se vê neste inciso são dois dos princípios já mencionados da proteção dos dados pessoais, como o da transparência e o da finalidade.

Em resumo, a transparência se coaduna na obrigação das informações serem claras e completas, como se vê também no inciso VI deste mesmo artigo, *in verbis*:

> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade (BRASIL, 2014, p. 7).

E quanto a finalidade, como seu nome já diz, para o que se destina, proibindo desde já o uso para além do consentido pelo usuário.

O consentimento assim dito, pode ser a solução ou problema da proteção dos dados pessoais, como pode ser abordado pela *human computer interaction* e a *privacy by default*, na qual concernem em caminhos para acompanhar o consentimento (PAESANI, 2020).

Outro princípio mencionado na lei é o da segurança, em seus artigos 13 e 15, *in verbis*:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
> § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.
> § 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.
> § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º .
> § 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
> § 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência (BRASIL, 2014, p. 13).

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
> § 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a

> guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §
> § 3º e 4º do art. 13.
> § 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
> § 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência (BRASIL, 2014, p. 15).

Observa-se que esses artigos discernem sobre a retenção obrigatória de dados, e como serão armazenados, em igual passo no art. 3, inciso V, na qual deverá haver medidas técnicas de estabilidade da rede e sua segurança.

### 3.4.4 PROJETO DE LEI N. 5276/2016

A discussão sobre um Projeto de Lei de Proteção de Dados Pessoais se arrastou por anos, mas o que se pode chamar de pontapé inicial foi a consulta pública elaborada pelo Ministério da Justiça, no ano de 2010, sobre a proteção de dados pessoais, nunca sequer realizada por um órgão público (GOMES, 2018).

Porém, este assunto ficou um pouco restrito a instituições e debates no Comitê Gestor da Internet, e este tomou a frente para que tivessem mais debates e, posteriormente, organizando seminários anuais junto ao governo, setor privado, comunidade técnica, sociedade civil e academia, e estes seminários serviram de base para o fomento da tão requisitada Lei Geral de Proteção de Dados (GARCIA, 2017).

Em paralelo, o Marco Civil da Internet foi determinante para que se olhasse diferentemente para a proteção dos dados pessoais, ainda mais com o escândalo envolvendo o caso de Edward Snowden. Assim, em 2015 houve uma mudança e movimentação sobre uma possível Lei de Proteção de Dados (DINIZ, 2018).

Amadureceu, então, uma versão pós-consulta pública com inovações significativas às versões anteriores e que foi recentemente encaminhada, com poucas modificações, ao Congresso Nacional no último dia 12 de maio de 2016, recebida pela Câmara dos Deputados, conjuntamente com um legado digital deixado por Dilma Rousseff, logo antes de ser suspensa do cargo, que inclui o Decreto Regulamentar do

Marco Civil da Internet, a Política de Dados Abertos do Governo Federal e o Programa Brasil Inteligente (LIMA, 2019).

Dessa forma, caminhou-se para a elaboração do Projeto de Lei n. 5.276/2016, em concorrência direta com dois outros, um também em trâmite na Câmara dos Deputados e o outro no Senado Federal. Mas em 2015, o senador Aloysio Nunes unificou todos os projetos similares em trâmites após realização de audiência pública, mostrando um substituto e ganhando corpo de uma LGPD (GARCIA, 2017).

Assim, o Projeto de Lei n. 5.276/2016 teve o regime de tramitação como de urgência constitucional, demonstrando sua real necessidade e “pulando” etapas na tramitação comum.

Desta forma, após seis anos do início da discussão, da sua internalização por ambas as Casas do Congresso Nacional nos últimos quatro anos com iniciativas próprias, da revitalização da discussão com a sociedade brasileira em 2015, do regime de urgência constitucional atribuído a uma das três iniciativas legislativas em questão, e, por fim, das declarações apartidárias de políticos em favor dessa pauta há, sem dúvida, uma conjuntura que demonstra que o Brasil caminhava a uma velocidade nunca vista para ter, finalmente, uma LGPD.

### 3.4.5 A LEI GERAL DE PROTEÇÃO DE DADOS

O Parlamento brasileiro aprovou a regulamentação da LGPD como Lei nº 13.709 em agosto de 2018. Desde então, a lei foi alterada duas vezes e entrou em vigor em 15 de agosto de 2020 (TOLEDO, 2017).

Silva e Lima (2020) relatam que a LGPD não é a primeira lei brasileira de proteção de dados. O Brasil é um país muito ativo em pesquisa acadêmica e legislação sobre proteção de dados. Mesmo antes da assinatura do LGPD, já existiam no país cerca de 40 leis e regulamentos relativos à proteção de dados.

“Proteção de dados” é um termo um tanto confuso, sendo na verdade, uma proteção de indivíduos. O objetivo é proteger a privacidade das pessoas protegendo seus dados (PINHEIRO, 2020, p. 91).

A LGPD fornece (ou exige) tal proteção e impõe deveres e limitações aos agentes de acusação para fazer cumprir a proteção.

O que há de novo no LGPD em comparação com as leis e regulamentações brasileiras anteriores, algumas das quais complementa, é o amplo escopo que possui:

> A LGPD foi modelada após o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, que por sua vez é baseado nas convenções das Nações Unidas. A ideia central do LGPD e do RGPD é que a proteção de dados pessoais é um direito humano. Isso significa que a proteção de dados não se limita a áreas específicas. A legislação anterior de proteção de dados no Brasil era "setorial" (BIONI, 2020, p. 97).

Em outras palavras, aplica-se a áreas pessoais como sistema de saúde, setor financeiro, entre outros.

Contudo, o regulamento da LGPD é um pouco diferente, de acordo com Silva e Lima (2020), a LGPD se aplica em qualquer um dos seguintes cenários: quando o tratamento de dados pessoais ocorrer no Brasil; quando o objetivo do tratamento for a oferta ou prestação de bens ou serviços; ou quando são processados os dados pessoais de pessoas que estavam no Brasil no momento da coleta dessas informações.

Mais notavelmente, e de acordo com a abordagem do RGPD, é que o LGPD define o direito à proteção de dados, independentemente do Estado em que é processado. Se, por exemplo, um banco coleta dados de determinado indivíduo, enquanto ele está visitando São Paulo, a LGPD se aplica ao processamento do banco, independentemente ser for cadastrado ou processar fisicamente os dados em São Paulo, ou em qualquer outro lugar.

Das atividades de processamento:

> Em várias áreas, como defesa nacional, aplicação da lei, jornalismo e estatísticas, são excluídas ou parcialmente excluídas da LGPD. Além disso, os dados processados para fins puramente privados não se enquadram no âmbito da lei. O processamento de dados pessoais é proibido por padrão. Permitido apenas se houver causa legítima. LGPD especifica uma lista de causas legítimas no artigo 7. As causas mais importantes são: o proprietário dos dados deu o seu consentimento para o tratamento dos dados. O consentimento deve ser informado, inequívoco e voluntário; o tratamento é necessário para a aplicação de um contrato que o titular dos dados tenha estabelecido (essencialmente, uma espécie de consentimento indireto); o responsável pelo tratamento tem a obrigação legal de processar os dados; para o exercício da aplicação da lei; para proteger a vida ou a segurança física de uma pessoa; e para questões de proteção de crédito (PEREIRA, 2020, p. 122).

A lista contida na LGPD é completa, ou seja, se o único motivo para o tratamento de dados pessoais for que irá "beneficiar os resultados", não será permitido.

Acerca dos direitos do proprietário dos dados, o proprietário dos dados pode exigir o seguinte do controlador: Confirmação da existência de um tratamento de dados pessoais (sempre do proprietário dos dados, claro); Acesso aos dados pessoais do proprietário dos dados; Correção de dados incompletos, imprecisos ou obsoletos; Anonimização, bloqueio ou exclusão de dados desnecessários ou excessivos, ou dados processados ilegalmente; Portabilidade de dados para outro provedor de serviços ou produtos (por exemplo, portabilidade de dados ao passar de um seguro saúde para outro); Exclusão de dados pessoais processados com o consentimento do proprietário dos dados; Informações sobre qualquer organização com a qual o controlador compartilhou os dados (incluindo processadores); e Informações sobre a possibilidade de negar o consentimento e as consequências dessa recusa (PINHEIRO, 2020).

No nível federal, o Brasil criou uma agência nacional de proteção de dados, a Autoridade Nacional de Proteção de Dados (ANPD*)*. Este órgão pode exigir que as organizações forneçam informações sobre o processamento de dados pessoais, impor sanções e, geralmente, é responsável por garantir o cumprimento da LGPD.

Os agentes encarregados do processamento são obrigados a "adotar medidas técnicas e administrativas de segurança capazes de proteger os dados pessoais de acessos não autorizados e situações acidentais ou ilegais de destruição, perda, alteração, comunicação ou qualquer tipo de processamento impróprio ou ilegal" (art. 46) (BRASIL, 2018, p. 1).

Em outras palavras, eles devem fazer um esforço razoável para proteger os dados pessoais. Os controladores também têm a obrigação de garantir que os processadores estejam cientes dessa responsabilidade.

Se uma organização violar a LGPD, a ANPD tem uma série de medidas disciplinares que pode aplicar à organização infratora. Mais importante ainda, a ANPD pode impor uma multa de até dois por cento da receita total da organização infratora (ou seu grupo) no Brasil, por um máximo de 50 milhões de reais. Se uma empresa sofrer várias violações de segurança, esse valor será cobrado para cada violação (PEREIRA, 2020, p. 122).

Além disso, se um processador de dados violar a lei de proteção de dados e, ao fazê-lo, causar danos aos titulares dos dados ou a qualquer outra pessoa, o processador de dados pode ser responsabilizado pelos danos em tribunal (artigos 42 a 45). (BRASIL, 2018, p. 1).

Ressalta-se que não existe uma tecnologia única que permita às organizações “apertar um botão” para cumprir instantaneamente a LGPD. A implementação de um paradigma fundamental, como a LGPD, é um processo de várias etapas. Exige que as organizações repensem como conduzem suas operações do dia a dia. Só então eles podem decidir como usar as tecnologias para atingir seus objetivos.

A LGPD certamente vai revolucionar a forma como as empresas fazem negócios no Brasil e com os brasileiros. Além disso, como disse Gilberto Gil: “O Brasil foi, é e estará na moda”. Outros países latino-americanos devem adotar legislação semelhante nos próximos anos (PINHEIRO, 2020).

Silva e Lima (2020) relatam que as interações no ambiente *online* demonstraram a necessidade de segurança dos dados pessoais. Redes sociais, aplicativos e sites recebem a cada segundo um exacerbado volume de informações de seus usuários.

O tratamento inadequado pode implicar no vazamento deste tipo de conteúdo, trazendo riscos para as pessoas e perda de credibilidade para as empresas.

Desta forma, as empresas precisam comprovar o comprometimento com a segurança e a integridade dos dados de clientes, funcionários e parceiros. Essas informações podem constar em cadastros, mailings, pesquisas, relatórios, contratos e outros meios.

Reconhecidamente a LGPD é um divisor de águas na esfera organizacional, resvalando-se na atividade de *Compliance*, que visa assegurar a conformidade das organizações com as leis e regulamentações vigentes, destarte, ambos estão estreitamente relacionados.

Nas palavras de Silva e Lima (2020, p. 235): “Estar em *compliance* com a LGPD é devidamente adequar-se à rotina e os processos ao texto da lei e, inserindo a organização em um novo tipo de cultura”.

Essa adaptação assegura maior segurança aos clientes, funcionários e parceiros, beneficiando ainda as empresas.

Haja vista, adequar-se à LGPD ainda se mostra um desafio, por se tratar de uma legislação coeva:

| |
|---|
| **Fazer um mapeamento dos fluxos de dados:** identificar as operações internas que estão relacionadas à captação e ao tratamento de dados pessoais de clientes, funcionários e parceiros. |
| **Organizar os dados que foram levantados:** após mapear as operações que envolvem dados pessoais, é preciso analisar esse material e classificá-lo de acordo com a relevância e a finalidade. Aproveitar para eliminar informações duplicadas, inválidas ou que não são usadas pela empresa. |
| **Ter políticas de proteção:** para estar de acordo com a LGPD, também é imprescindível que a empresa estabeleça políticas de proteção de dados pessoais para manter as informações seguras. Essas diretrizes devem ser informadas tanto para o público interno (funcionários) quanto para o externo (clientes e parceiros). |
| **Revisar os termos e políticas:** caso a empresa tenha elaborado termos de uso, políticas de privacidade e contratos antes da LGPD, será necessário revisar esse material para adaptá-lo às novas regras. |
| **Envolver a equipe:** é preciso que todos os funcionários sigam as diretrizes criadas. Divulgar as informações sobre a LGPD e as ações da empresa para se adequar à lei nos canais de comunicação interno e realize treinamentos que permitam fixar essas regras e engajar os profissionais. |
| **Escolher as ferramentas corretas:** verificar se as ferramentas que a empresa dispõe para o tratamento de dados pessoais estão em conformidade com a LGPD. Há muitas soluções tecnológicas disponíveis que podem ajudar nessa adaptação. Uma recomendação é a implantação de um canal de denúncias, mecanismo que contribui para identificar, investigar e combater possíveis irregularidades. |
| **Fazer monitoramentos periódicos:** o trabalho do *compliance* é contínuo, feito no dia a dia da empresa. Por isso, é fundamental acompanhar o andamento das ações que foram implantadas. Isso, inclusive, é uma exigência da LGPD. |
| **Lembrar-se de comprovar as boas práticas:** adotar ferramentas que possibilitem o registro das ações internas que foram criadas, do repasse das informações aos funcionários e do trabalho de avaliação periódica. |



Figura 1: Como se adaptar a LGPD
Fonte: Pereira (2020, p. 123)

Em resumo, é necessário adequar a rotina e os processos à LGPD, o que garante muitos benefícios para a empresa. O primeiro deles é a segurança jurídica de estar em conformidade com a lei. Outro aspecto positivo é evitar sanções e o prejuízo financeiro. A multa pelo descumprimento da legislação pode chegar a R$ 50 milhões (PINHEIRO, 2020).

Outra vantagem é o fortalecimento da credibilidade no mercado, uma vez que estar de acordo com a lei oferece maior segurança para clientes, funcionários e parceiros. Os casos de vazamentos de dados pessoais são responsáveis por danos à imagem e à reputação de empresas.

Todas as empresas, independente do porte ou do setor de atuação, devem estar em conformidade com a LGPD. Em caso de dúvidas, é necessário buscar auxílio de profissionais que possam orientar sobre a adequação prática aos termos da lei.

# 4 FURTO DE DADOS E O PROJETO DE LEI N. 4554/2020

Em 21 de junho de 2021 um Projeto de Lei que endurece as penas para crimes eletrônicos de furto de dados foi aprovado pela Câmara dos Deputados. O Projeto de Lei n. 4554/2020 foi elaborado pelo senador Izalci Lucas (BIONI, 2020).

Segundo Silva e Lima (2020, p. 44), “o volume de fraudes já começa a afetar a economia do país, gerando perda de poder aquisitivo e também perdas emocionais por parte das vítimas”.

O Projeto de Lei não distingue crimes praticados por dispositivos conectados ou não à internet e altera trecho do Código de Processo Penal, que trata da competência para processar e julgar algumas modalidades do crime de fraude.

O que muda com o novo Projeto de Lei:

| |
|---|
| **Invasão de dispositivo de computador:** a pena mínima é de 3 meses a 1 ano, e a pena máxima é de 1 a 4 anos. Em caso de perda econômica, a pena pode ser aumentada de 1 2/3. Atualmente, aumenta de um 1/6 a 1/3. A pena mínima no caso de acesso a conteúdos provenientes de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações confidenciais ou telecomando não autorizado do dispositivo invadido passa de 6 meses para 2 anos e a máxima de 2 a 5 anos. |
| **Furto eletrônico:** a proposta prevê pena mínima de 4 e máximo de 8 anos de reclusão se o furto for praticado por meio de dispositivo eletrônico ou de computador, conectado ou não à rede de computadores, com ou sem violação de um mecanismo de segurança, a utilização de programa malicioso, ou por qualquer outro meio fraudulento semelhante, o que não está previsto na legislação em vigor. Se o crime for cometido através da utilização de servidor fora do território nacional, a pena passa de 1 para 2/3. E se praticado contra idosos ou vulneráveis, 1/3 para 2/6. |
| **Fraude eletrônica:** a proposta altera o Código de Processo Penal no caso de fraude, acrescentando a expressão “fraude eletrônica”. A pena estipulada é de 4 a 8 anos se a fraude for cometida com a utilização de informação prestada pela vítima ou por terceiro induzido por erro através de redes sociais, contatos telefônicos ou envio de e-*mail* fraudulento, ou por qualquer outro meio fraudulento analógico. Como no caso do furto eletrônico, se o crime for praticado com a utilização de servidor mantido fora do território nacional, a pena passa de 1 para 2/3. E se for cometido contra vulneráveis e idosos, pode ser aumentado em um 1/3 para 2/6. |
| **Jurisdição:** quando o crime for cometido pela internet ou por meio eletrônico, a jurisdição será determinada pelo local de residência ou residência da vítima. |

Quadro 3: O que mudou com o Projeto de Lei
Fonte: Pereira (2020, p. 54)

Observa-se que embora o Código Penal já defina o crime de hackeamento de dispositivo de computador, instituído pela Lei n. 12.737, de 30 de dezembro de 2012, esta lei agravou a pena para esse crime com reclusão de 1 a 4 anos e multa. Se resultar em prejuízo econômico para a vítima, a pena é aumentada de 1/3 a 2/3. Se tal invasão resultar na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações confidenciais, conforme definido por lei, ou o controle remoto não autorizado do dispositivo hackeado, esta lei aumentou a pena para 2 a 5 anos, mais multa.

Além do endurecimento que essa lei traz para os crimes cibernéticos, a lei resultante do “pacote anticrime” elaborado pelo ex-ministro Sérgio Moro, Lei n. 13.964, de 24 de dezembro de 2019, também alterou a condenação progressiva, do regime fechado ao semiaberto e de regime semiaberto para regime aberto (PEREIRA, 2020).

No entanto, a condenação progressiva, apesar de defendida por alguns juristas e alguns defensores dos Direitos Humanos, acaba contribuindo para a percepção de impunidade, uma vez que, apesar de seu propósito de focar na ressocialização dos presos, o sistema prisional atualmente institucionalizado funciona como uma verdadeira escola do crime e os prisioneiros deixam de cumprir a pena a qual foram submetidos por seu crime.

Por fim, segue um quadro demonstrativo que compara o antes e depois da condenação progressiva:

| **REQUISITOS DE OBJETIVO** | **ANTES** | **MAIS TARDE (AGORA)** |
|---|---|---|
| Sem violência ou ameaça grave | 1/6 da pena | Infrator pela primeira vez - 16% e infrator reincidente - 20% |
| Por meio do uso de violência ou ameaça grave | 1/6 da pena | Criminoso pela primeira vez - 25% e agressor reincidente - 30% |
| Crime hediondo ou semelhante | Criminoso pela primeira vez - 2/5<br>Ofensor reincidente - 3/5 | Delinquente primitivo - 40% e 50%, se houver morte<br>Ofensor reincidente - 60% a 70%, se houver morte |
| Comandar individual ou coletivamente uma organização criminosa estruturada para cometer um crime hediondo ou semelhante | 1/6 da pena | 50% da sentença |

| | | |
|---|---|---|
| Milícia privada | 1/6 da pena | 50% da sentença |

Quadro 4: O antes e depois da condenação progressiva
Fonte: Pereira (2020, p. 44)

Observa-se que após as alterações introduzidas pelo “pacote anticrime”, que acabaram por mitigar a impunidade. A impunidade incentiva a prática criminosa e contribui para a descrença da sociedade quanto à aplicabilidade das penas a quem as merece.

É importante ressaltar que apesar da falta de legislação específica que verse sobre crimes eletrônicos, alguns deles são passíveis de qualificação penal perante a legislação vigente, porém apesar da possibilidade de enquadramento penal, é importante que tenha uma legislação especifica para que a punição não ocorra mais através da adequação da norma, ou interpretação analógica, pois isso muitas vezes não é possível ser utilizado, pois a linha que separa a interpretação analógica da analogia em si, é muito tênue, e no Direito Penal a analogia é proibida.

Portanto é importante que se tenha a legislação adequada e que a conduta penalizada seja exatamente a prevista em lei, para não ensejar o crescimento notório dos crimes informáticos, sob a alegação de não ser possível a sua punição, diante do Princípio da Legalidade, que não permite punir condutas que não estejam expressas previamente na lei.

O crescimento dos crimes é resultado da dificuldade de punição, e também pode ser atribuído ao usuário, devido à falta de informação, ausência de cuidados à navegação na internet, não adoção a medidas e ferramentas de segurança, à demora em relatar as denúncias às autoridades e inúmeros outros motivos que acabam sendo desencadeadores desses novos golpes.

Muito tem se discutido acerca da competência para julgar os crimes virtuais. Percebe-se que, mesmo sem legislação específica, alguns Tribunais do Brasil já se posicionam sobre a competência no caso dos crimes virtuais, o que representa um avanço, e permite que enquanto isso os crimes sejam julgados pelos Juízos onde originou-se a infração, conforme os artigos já existentes.

Tudo para que não permanecermos estáticos, e principalmente para não disseminar a “sensação de impunidade”.

Enquanto o poder legislativo deve se apressar a fim de atualizar a legislação, o Poder Judiciário deve ir aplicando a norma, conciliando a lei e o direito.

Pois, apesar da falta de uma legislação especifica tratando do assunto para combater os crimes digitais, não se pode permitir que crimes como esses se proliferem por falta de punição, não se pode conceber o direito a não ser como desdobramento constante da vida dos povos.

Enquanto tal ciência ainda não evolui no sentido de criar normas específicas e programar um trabalho inicial, de base, nas graduações de Direito tornando obrigatório o aprendizado deste assunto, o poder judiciário deve realizar debates, oferecer alternativas, envolver a sociedade sobre os riscos oferecidos pela internet, investir no quesito prevenção, criar a consciência digital, e aplicar os dispositivos do atual Código Penal aos delitos praticados.

## 4.1 TIPIFICAÇÃO E SOLUÇÃO

A Constituição Federal prevê em seu art. 5º, inciso XXXIX, *in verbis*: “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal” (BRASIL, 1988, p. 5).

Desta maneira, o agente só prática um crime se este já estiver, previamente, previsto na legislação.

Em outras palavras, o indivíduo tem que praticar o “tipo penal” descrito. Esse conceito, por sua vez, é uma conduta abstrata colocada na lei em razão da sua valoração social e que recebe o tratamento necessário e adequado (BIONI, 2020).

Se a conduta não estiver previamente tipificada como crime, não conter todos os elementos do tipo, se não houver adequação que resulte em ação ou omissão do agente, a conduta é atípica e, portanto, não é crime.

Essa ideia consiste no Princípio da Legalidade já que “*nullum crimen, nulla poena sine lege*” (não há crime sem lei anterior que assim o defina”, como explicado acima (TOLEDO, 2017).

Desta maneira só a lei define o que é crime, sendo que no Direito Penal não é possível analogia “*in malam partem*” (só para o mal). Analogia seria aplicar a uma situação semelhante, a punição que a lei rege a outra conduta, é como se fosse uma integração da lei (BORGES, 2018).

No Direito Penal, segundo Leonardi (2020), a analogia só é permitida para beneficiar o acusado.

Destarte, nenhum fato pode ser considerado crime, e nenhuma pena criminal pode ser aplicada, sem que antes, desse mesmo fato, tenham sido instituídos por lei, o tipo delitivo e a pena respectiva. Caso contrário, constitui uma real limitação ao poder estatal de interferir na esfera das liberdades individuais.

Aplicando tal realidade aos crimes cometidos no caso de dados pessoais, observa-se que a lei penal é omissa e que os juízes tentam “adaptar” o caso concreto às leis existentes, aplicando a solução que a seu ver é a correta, adequada e justa (TOLEDO, 2017).

Nas palavras de Rosa (2012, p. 133): “o juiz se vê em uma árdua tarefa já que foge da sua competência e ele é forçado a legislar”.

É certo que o juiz necessita dar uma decisão, pois o poder judiciário não pode se eximir de tal responsabilidade devido ao Princípio da Inafastabilidade da Jurisdição previsto no art. 5º inciso XXXV da Constituição Federal, *in verbis*: “A lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito” (BRASIL, 1988, p. 1), o que implica na entrega da prestação jurisdicional pelo estado.

Essa resposta do judiciário deve, e também pode, respaldar-se nas leis existentes, aproveitando-as ao máximo, mas os casos em que os magistrados tem a possibilidade de enquadrar as condutas, nas tipificações existentes, são poucos, já que a eles não é permitido a analogia (WANDERLEI, 2021).

Somente casos como pedofilia, estelionato, ameaça, crimes contra a honra, pirataria, furto e dano são crimes virtuais já expressamente previstos no Código Penal, embora não na forma virtual, mas podem ter as mesmas punições previstas aplicadas (CASTRO, 2018).

Nota-se, nesses casos, que o crime continua o mesmo, o que muda é apenas o “*modus operandi*”, então não é caso de analogia, porque o que ela protege é a conduta que não pode ser equiparada a outra semelhante, e aqui (uso indevido de dados pessoais) a conduta praticada é a mesma, o que modifica é meio pelo qual é executada.

A grande dúvida é se é possível punir aqueles que façam uso indevido de dados pessoais com a legislação existente, ou se existe a necessidade de se introduzir novas normas protetivas, com base nos novos valores jurídicos.

Cogita-se ainda, segundo Feliciano (2019), a possibilidade de se negociar uma legislação internacional regulamentando a internet, bem como a criação de cortes internacionais.

Atualmente no Brasil ainda não existem leis especificas para tais condutas danosas, mas o poder legislativo já vem discutindo o assunto. Existem algumas propostas tramitando nas casas legislativas.

É evidente que para os crimes já tipificados na legislação não há necessidade de revisão ou criação de dispositivos legais. Na concepção de Feliciano (2019), se houvesse a previsão expressa na forma virtual seria legalmente mais seguro, mas nada impede que para aqueles casos em que já existe previsão em sua forma comum, seja aplicada a mesma punição quando praticados em sua forma virtual.

Entende-se que a conduta é a mesma e por isso não deve ser afastado a possibilidade de punição, a fim de que não se fortaleça o saldo dos crimes virtuais ora existentes.

Corrêa (2018) elenca, em sua obra, alguns exemplos interessantes: em se tratando, por exemplo, de um circuito integrado de computador, pode-se enquadrar o autor do crime, no crime de furto, previsto no art. 155 do Código Penal. Ou ainda se o agente furtar com a intenção de obter informações sobre esse circuito, e posteriormente lucrar com isso, pode ser enquadrado na Lei de Patentes (Lei n. 9.279/96).

Outrossim, nota-se que a ausência de legislação específica não impede o enquadramento legal do ato praticado, se as condutas forem as mesmas. De modo que delito que envolva dados pessoais não deixa de ser uma delinquência se cometido pelo meio virtual, assim como a lavagem de dinheiro não deixa de ser um crime, fraude é fraude.

Nesse sentido:

> Nota-se que estaria aplicando às mesmas penas a condutas idênticas, já previstas no Código Penal, porém cometidas de uma maneira diferente. O que a meu ver, as torna até mais grave, porque foram praticadas por um meio que aumenta consideravelmente a possibilidade de lesão, e por isso mereciam ser reprimidas de uma forma mais severa, mas enquanto não se possui essa nova legislação, busca-se a justiça com a que se tem (ROSA, 2012, p. 122).

As leis existentes, podem nesses casos serem aplicadas de plano, sem nenhuma mudança, podendo também, futuramente, vir a se tornarem mais fortes, com a adição, a soma de outras normas que se utilizadas juntas atingiriam de maneira eficaz seu objetivo.

Todavia, para os casos em que o meio virtual é utilizado e não se prevê punição, novas leis devem ser promulgadas. Deve haver uma atualização por parte do poder legislativo (CORRÊA, 2018).

Além da dificuldade na tipificação dos delitos que envolvam dados pessoais, outro impasse frente à problemática é o fato de que as vítimas preferem arcar com os prejuízos, ao invés de ser identificada como “vítimas”, isso atrapalha a punição, já que as vítimas não buscam o Poder Judiciário (BORGES, 2018).

Além disso, o trabalho de investigação, bem como o trabalho da perícia, deve ser minucioso, e infelizmente no país, como se sabe, existe pouquíssima tecnologia voltada para as práticas periciais.

Pereira (2020) chama a atenção de que não se pode viver uma utopia, imaginando que basta a inovação nas leis ou a criação de novos dispositivos que “protejam” os dados pessoais: far-se-á necessária a conscientização das pessoas, através de uma política de prevenção para os cidadãos, palestras, eventos, cartilhas, entre outros, onde as pessoas vejam que todos estão sujeitas aos crimes com seus dados pessoais e que acima disso que elas não tenham vergonha ou receio em admitir que foram vítimas de tais delitos, que elas busquem o Poder Judiciário e a reparação do dano que lhes foi causado.

Além disso, é necessário interesse e inovação dos poderes em se atentar a perícia forense computacional, para fortalecer este ramo, e facilitar ou ao menos possibilitar que exista um trabalho investigativo de perícia virtual.

Paesani (2020) idealiza que até mesmo seria possível utilizar o “talento” dos próprios agentes, imputando a eles, cumulativamente ou alternadamente, uma pena onde se submetam a ensinar, a acompanhar estudos de casos, a elaborar cursos, a atuar em um trabalho profissional junto com as autoridades policiais, ajudando e inovando em um ramo que, neste país, ainda é muito fraco: a seara tecnológica.

É evidente que a evolução da tecnologia acaba desencadeando aumento no número de crimes envolvendo o mundo virtual.

Ainda em âmbito da apuração das provas, segundo Silva e Lima (2020), é válido tratar das perícias que podem ser solicitadas pelas partes, na denúncia, para o polo ativo, ministério público ou ofendido, via de regra, enquanto que para o polo passivo na defesa, ou no momento do pedido de diligências para ambas as partes.

No tange as perícias, tem-se que:

> Para a realização da perícia, será preciso buscar e apreender o computador, na forma do artigo 240 do CPP. A busca poderá ser determinada de ofício pela autoridade ou mediante requerimento das partes (art. 242, CPP). O mandado de busca deverá conter o local da diligência, o nome do proprietário, o motivo, os fins da diligência e a assinatura da autoridade (art. 243, CPP). Realizada a busca e apreendido o material, este será encaminhado aos peritos. A lei determina que sejam dois peritos oficiais; nos locais onde não houver, duas pessoas idôneas (art. 159, CPP) (CASTRO, 2018, p. 114).

Contudo, sabidamente, a produção de provas nos crimes que envolvem a proteção de dados e segurança da informação são na maioria dificultosos, nem sempre se tem o computador físico para realização de perícia e os documentos comprobatórios podem ser frágeis como: cópia impressa de mensagens, *e-mails*, cabeçalhos de e-*mails*, *printscreen* da tela, além de *link* da página, vídeos, textos, áudios, entre outros, o que, por vezes, compromete a admissibilidade dos documentos como prova.

Em 28 de janeiro celebra-se o Dia Internacional da Proteção de Dados Pessoais. O objetivo deste dia é conscientizar sobre o tratamento de dados pessoais, a importância de protegê-los e de que sejam usados de acordo com as normas de privacidade.

Martins (2020, p. 32) reflete que: “A internet não foi concebida como um lugar para proteção de dados e segurança da informação”.

De modo que, se as medidas de proteção não forem suficientes ou corretas, pode haver vazamento de dados e a informação é exposta a todos.

Por sua vez Beviláqua (2017, p. 86) explica que a rede foi projetada com múltiplos protocolos para circulação de informações, porém a lógica de manutenção da privacidade é alheia à arquitetura básica da internet: “A privacidade é uma questão coletiva, não se tem direitos sobre dados de terceiros”.

Pinheiro (2020) recomenda consultar as políticas de privacidade, não importa quão “longas e complicadas” elas possam ser. É notório que a linguagem técnica representa uma barreira no momento de sua leitura. Por outro lado, aconselha Pinheiro (2020, p. 88): “não se deve digitalizar documentos, nem os carregar em qualquer plataforma da Internet se for necessário manter estrita privacidade”.

Empresas, profissionais e instituições devem solicitar consentimento para processar dados pessoais. Além disso, a finalidade, as consequências, os destinatários e, se estiverem armazenados em um banco de dados, o nome e os

dados de contato do responsável devem ser informados com antecedência e em linguagem clara (BIONI, 2020).

Nesse sentido, Pereira (2020) afirma que qualquer tipo de sessão realizada sem consentimento não é lídima.

Paesani (2020) da mesma forma, ressalta que as informações não podem ser vendidas sem a “autorização expressa do titular dos dados”. Ele também esclareceu que “o Estado pode ter meus dados, mas esses dados são meus e não do Estado”. O princípio da finalidade estabelece o dever de informar o titular sobre o uso dado aos seus dados pessoais pelo responsável.

É evidente que há necessidade de atualização da LGPD, vez que foi criada antes da “explosão dos fenômenos digitais e da economia digital que se deu com a pandemia”. Martins (2020, p. 231) reforça isso, por entender que é necessário maior rigor.

## 4.2 A CRIAÇÃO DE DELEGACIAS ESPECIALIZADAS E A RESPONSABILIDADE DO PROVEDOR DE ACESSO

Uma grande parte dos estados brasileiros já dispõem de delegacias especializadas para a investigação de crimes relacionados a proteção de dados e segurança da informação, sendo que as primeiras surgiram nos estados de São Paulo e Espírito Santo (PEREIRA, 2020).

Tais delegacias existem também nos seguintes estados: Bahia (Grupo Especializado de Repressão aos Crimes por Meio Eletrônicos); Distrito Federal (Delegacia Especial de Repressão ao Crime Cibernético); Espírito Santo (Delegacia de Repressão a Crimes Eletrônicos); Goiás (Delegacia Estadual de Repressão a Crimes Cibernéticos); Maranhão (Departamento de Combate aos Crimes Tecnológicos); Mato Grosso (Gerência Especializada de Crime de Alta Tecnologia); Minas Gerais (Delegacia Especializada de Investigações de Crimes Cibernéticos); Pará (Divisão de Prevenção e Repressão a Crimes Tecnológicos); Paraná (Núcleo de Combate aos Cibercrimes); Pernambuco (Delegacia de Polícia de Repressão aos Crimes Cibernéticos); Piauí (Delegacia Especializada de Repressão aos Crimes de Alta Tecnologia); Rio de Janeiro (Delegacia de Repressão aos Crimes de Informática); Rio Grande do Sul (Delegacia de Repressão aos Crimes Informáticos e Departamento Estadual de Investigações Criminais); São Paulo (4ª Delegacia de Delitos Cometidos

por Meios Eletrônicos e Departamento de Homicídios e de Proteção à Pessoa - 4ª Delegacia de Polícia de Repressão à Pedofilia); Sergipe (Delegacia de Repressão a Crimes Cibernéticos); e Tocantins (Divisão de Repressão a Crimes Cibernéticos).

Para se prevenir desse tipo de ataque, é importante agir de forma a minimizar os danos sofridos. Nesse caso, procurar uma delegacia preferencialmente especializada em crimes virtuais e realizar um boletim de ocorrência.

Considerando a problemática de identificar e responsabilizar algum autor do crime virtual, surge a questão da responsabilização jurídica do provedor de acesso, muito discutida entre os doutrinadores.

Essencialmente, é importante destacar o que vem a ser provedor de acesso, lição comentada da seguinte maneira:

> Pode-se falar em provedores de acesso como sendo aqueles que prestam serviços de conexão à internet, ao passo que os provedores de conteúdo ou serviços são aqueles que proveem e-*mail*, hospedagem de páginas, entre outros. Os provedores de acesso podem também prestar serviços de provimento de conteúdo (WANDERLEI, 2021, p 109).

De modo que é necessário diferenciar as modalidades de provedores relativos à informática e internet.

No que se refere à questão da responsabilidade do provedor, Castro (2018), em seu estudo, comenta que a responsabilidade não é da pessoa jurídica e sim de seus representantes legais.

Leonardi (2020) explica ao assunto: se os provedores de serviços não preservarem os dados técnicos de conexões e acessos e os dados cadastrais dos usuários, inviabilizando, inclusive por outros meios, a identificação ou localização dos responsáveis por atos ilícitos, sujeitam-se a responder, solidariamente, pelo ato ilícito cometido por terceiro que não puder ser identificado ou localizado, em razão desta conduta omissiva.

Assim sendo, resta ao provedor de acesso responder pelos atos de seus usuários.

Apesar do cenário de uma possível responsabilização dos provedores de acesso, a sua imputação por atos práticos pelos agentes criminosos na rede não pode ser vista de maneira abrangente, restando então alguns limites.

Quanto à norma penal não existe nenhum regulamento que obrigue uma pessoa jurídica a fiscalizar o conteúdo de informações compartilhadas pelos seus usuários (BIONI, 2020).

A esse respeito, a lei penal é clara em seu artigo 1º, em que diz, *in verbis*: “não há crime sem lei anterior que o defina. Não há pena sem previa cominação Legal” (BRASIL, 1940, p. 1).

Beviláqua (2017) explica que relativamente ao direito pátrio, a Constituição Federal admite apenas a responsabilidade penal da pessoa jurídica quanto a crimes ambientais. Assim, a ideia de se admitir a responsabilidade penal dos provedores, sejam eles de serviço, conteúdo ou mesmo os de acesso, somente seria possível com a alteração da Constituição Federal.

No entanto, ainda assim, entende-se que seria preciso melhor regulamentar, no âmbito civil e administrativo, suas obrigações relativas a impedir ilícitos na rede antes de se falar em respostas penais que, como se sabe, devem permanecer como *ultima ratio* (WANDERLEI, 2021, p 110).

Junto a isso, é relevante a questão dos *e-mails*, pois são vistos como documentos de correspondências, e a Constituição põem a salvo a inviolabilidade de seu conteúdo, tal qual prega o art. 5º XII da Constituição, *in verbis*: “XII - e inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal” (Vide Lei n. 9.296, de 1996) (BRASIL, 1988, p. 1).

Entende-se então que o provedor não poderá ser responsabilizado pelos conteúdos colocados na rede pelos seus usuários, tendo em vista a grande quantidade de pessoas ligadas à internet, e juntamente o grande volume de informações transmitidas.

Porém, é de grande relevância sua participação para a identificação dos sujeitos, fornecendo dados aos investigadores para localização da máquina que gerou o ato criminoso (BORGES, 2018).

Assim, é de suma importância que os provedores de acesso à internet adotem medidas para esclarecer aos usuários a responsabilidade em que incorrerão em razão dos conteúdos publicados na rede, bem como a consequência de seus atos quando violados os direitos legais protegidos.

## 4.3 COMPETÊNCIA PARA PROCESSAMENTO E JULGAMENTO

Em se tratando de crimes virtuais não existe noção de território no meio virtual, independentemente da lei material a ser adotada, existe uma questão de jurisdição que se torna problemática no tocante ao ciberespaço.

O tema ainda é muito controverso, já que os legisladores, bem como os juristas encontram dificuldades até mesmo em definir quais são os crimes praticados por meio da informática (WANDERLEI, 2021).

A dificuldade que se encontra na repressão dos crimes virtuais, é que uma conduta pode lesar o ordenamento jurídico de mais de um Estado, já que o indivíduo infrator não sabe onde se localiza a vítima nem tampouco a jurisdição a qual encontra-se subordinada. Ou pode ainda o produto do crime ser colocado à disposição de qualquer indivíduo que possua acesso à internet (BIONI, 2020).

Quando o agente e a vítima se encontram em países que o crime virtual já é tipificado, é mais fácil, mas pode ser o caso, por exemplo, de acordo com Feliciano (2019), de não ser tipificado em nenhum dos países, ou de ser tipificado em um e no outro não.

Levando em consideração que as normas penais são apostiladas restritivamente, em caso de conflitos de normas deve-se interpretar por aquela que menos restringir a liberdade do acusado (TARTUCE; CASTILHO, 2016).

De qualquer forma, verifica-se que o combate aos crimes virtuais, só pode se dar de um único jeito: através da lei. É a lei que determina a conduta humana dentro dos relacionamentos, é por meio dela que atos imorais e atividades destruidoras podem ser prevenidos, gerando limites, e em se tratando de crimes virtuais é muito importante a existência de limites (NIGRI, 2016).

No que tange ao local do crime, o Brasil adotou a Teoria da Ubiquidade, conforme art. 6º do Código Penal, portanto considera-se local do crime o local da conduta, ação, omissão ou resultado (BRASIL, 1940).

Nesse interim, em harmonia com a Teoria da Ubiquidade ainda que processado e punido em país diferente, o agente será julgado perante as leis Brasileiras, e terá a pena computada conforme o art. 8º do Código Penal (BRASIL, 1940).

Após o procedimento de verificação dos crimes, é necessário, segundo Leonardi (2020), a formação do processo, porém como os crimes virtuais têm a sua

complexidade voltada para o local em que se consumam, e como podem atingir vários locais, fica difícil a identificação do local onde o processo deve tramitar.

No processo, geralmente invasões a sistemas alheios não deixam vestígios, são crimes sem trações e sem evidências, além disso, em alguns casos as vítimas demoram a notar o dano, já que, por vezes, os arquivos nocivos ficam “escondidos” por um determinado tempo. Essa insuficiência de provas afasta a possibilidade de condenação (NIGRI, 2016).

No Brasil, o artigo 5º do Código Penal, preceitua, *in verbis*: “Aplica-se a lei Brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional” (BRASIL, 1940, p. 5).

Sendo assim, segundo Inellas (2019, p. 322): “A lei penal vigora dentro dos limites em que o estado exerce a sua soberania”.

Em via de regra, os crimes cometidos virtualmente se iniciam em um local e se encerram em outro, é aqui que surge o problema da competência, pois conforme a previsão do artigo acima a competência seria do Brasil para os crimes cometidos em território nacional.

Pelo Princípio da Territorialidade, nos demais casos a competência seria conforme o local do resultado, segundo o art. 70 do Código de Processo Penal, *in verbis*: “A competência será, de regra, determinada pelo lugar em que se consumar a infração” (BRASIL, 1940, p. 70).

Então, pelo art. 70, o local da competência não seria do computador do agente ou o por ele utilizado, mas sim onde se encontra o computador da vítima.

Se a interpretação for conforme art. 70 §1º, a execução iniciou-se aqui, mas a infração se consumou fora do território nacional, a competência vai ser determinada pelo local em que tiver sido praticado o último ato de execução no Brasil (BRASIL, 1940).

Ou seja, ainda puxa a competência para as leis brasileiras. Entretanto, se for o caso do artigo 70, § 2º, a infração foi praticada no exterior e seus resultados foram produzidos no Brasil, será competente parcialmente o juiz do lugar em que o crime produziu o resultado (BRASIL, 1940).

Ou seja, o agente iniciou o comando em um computador fora do território nacional, mas a vítima estava aqui e os danos foram causados aqui, o juiz brasileiro, é competente parcialmente (BIONI, 2020).

Porém, se levar em consideração o art. 109 inciso IV da Constituição, remete a competência aos juízes federais em razão da matéria, *in verbis*:

> Os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral (BRASIL, 1988, p. 109).

Considerando que a grande rede é um serviço público de telecomunicação, regulamentado pela Agência Nacional de Telecomunicações, seria de interesse da União, e desta forma apesar da competência ser brasileira, seria em todo caso conhecido e julgado pela Justiça Federal.

Contudo, existem autores que discordam desta posição, conforme salienta:

> Alguns autores entendem que nestes casos em se tratando de crimes virtuais aplica-se por analogia o art. 42 da Lei n. 5.250/1967 (Lei de Imprensa), essa lei considera competente para o processo e julgamento dos delitos, o foro do local onde for impresso o jornal, no caso em tela as provedoras de acesso seriam equiparadas a empresas jornalísticas, considerando-se como local da infração penal, aquele onde estiver hospedado o site com o conteúdo criminoso. Existe jurisprudência, nessa esteira de entendimento do Tribunal de Justiça do Estado do Rio de Janeiro (INELLAS, 2019, p. 346).

É importante ressaltar que esta lei teve a sua inconstitucionalidade declarada, sob alegação de não ter sido recepcionada pela Constituição de 1988.

Ainda o mesmo autor:

> Em se tratando de crime material, ou seja, delito necessariamente provido de conduta e evento (ação e modificação consequente operada, como projeção, no mundo exterior), sua consumação acontece no instante em que sobrevier o seu resultado, já que representa este o elemento típico que confere fecho e desfecho a figura criminosa, ultimando-a e completando-a. Nos delitos materiais, portanto o local da produção do evento é que fixa sua consumação e a competência para a "*persecutio criminis in juditio*". O mesmo sucede nos delitos plurilocais, que são aqueles que se desdobram em territórios diferentes. Ou seja, o local de produção do evento diante da qual se consuma o delito, é competente para processamento e julgamento (INELLAS, 2019, p. 462).

À risca, a competência seria, portanto, do local onde estivesse o computador que deu o comando, ainda que se trate de delitos plurilocais.

Ao abordar a questão da competência assevera-se que:

> Quando o crime for cometido pela internet, julga-se que a competência deverá ser da justiça federal, de acordo com o art. 109, IV da Constituição Federal, já que o interesse é da União, em ter a internet resguardada dentro dos limites

> brasileiros. Além do mais, este é um crime em que o resultado nem sempre se produz no lugar da ação, podendo até ocorrer em países diversos, com repercussões internacionais (BIONI, 2020, p. 99).

Entende-se que a competência é a do art. 109, IV da Constituição, *in verbis*: “IV - os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral” (BRASIL, 1988, p. 109), ou seja, da Justiça Federal em virtude da gravidade e repercussão dos crimes. Bem como por ser de interesse da União a exploração de serviços de telecomunicações, conforme art. 21, XI da Carta Magna, *in verbis*: “XI - explorar, diretamente ou mediante autorização, concessão ou permissão, os serviços de telecomunicações, nos termos da lei, que disporá sobre a organização dos serviços, a criação de um órgão regulador e outros aspectos institucionais” (BRASIL, 1988, p. 21).

Recentemente, em 2020, Leonardi (2020, p. 212) divulgou que “a Terceira Seção do Superior Tribunal de Justiça decidiu que a competência para julgar crimes praticados em blogs jornalísticos na internet é definida pelo local de onde partiu o ato delituoso”. Ou seja, onde se encontra o provedor do *site*.

Observa-se que a Teoria mais adequada seria a da Ubiquidade, ou seja, considera-se competente o local da ação, omissão e do resultado. E no caso de delitos não cometidos dentro do território nacional, uma saída é acrescentar, criar um dispositivo que reserve a competência à justiça Brasileira, assim como o exemplo elencado na obra de Inellas (2019), o art. 7º do Decreto Lei 2.848/1940 que dispõe que ficam sujeitos as legislações brasileiras, embora cometidos no estrangeiro, ilícitos penais de nacionalidade, representação, justiça universal, entre outros.

Finalmente, ainda é muito divergente a questão da competência, mas o importante é que independentemente da lei material a ser adotada, que se enfrente a problemática e que os crimes sejam devidamente julgados.

Pode-se concluir que a jurisdição aplicada será decidida pelos princípios e regras existentes, por ora, percebo que a corrente mais aceitável é que a pessoa que entrar no ciberespaço de uma nação ficará subordinada às regras do país onde originou a lesão.

## 5 PROJETO DE LEI SOBRE DESINFORMAÇÃO - *FAKE NEWS*

Um Projeto de Lei sobre desinformação foi votado no Brasil. A proposta foi apresentada em abril de 2020, em plena pandemia de Covid-19, e sofreu diversas modificações. O texto final foi analisado pelo Congresso e aprovado (WANDERLEI, 2021).

A falta de transparência é apenas mais uma margem de um processo marcado por restrições à participação de múltiplos partidos interessados e propostas legislativas mal formuladas, o que pode implicar em sérios riscos à liberdade de expressão e à privacidade (PAESANI, 2020).

Versões anteriores e posições públicas de legisladores sobre o assunto denunciam abusos na criminalização de práticas comuns, definições amplas e extensas e requisitos de identificação que ameaçam a privacidade e a liberdade de expressão e geram novas formas de discriminação.

Em sua versão mais recente e aprovada, o Projeto cria uma internet altamente controlada e coloca todos os usuários sob suspeita de realizar atividades consideradas ilícitas. Ainda mais: a obrigatoriedade de identificação por meio de documentos de identidade e número único de celular pode excluir milhões de pessoas do acesso a informações e serviços básicos *online* (PEREIRA, 2020).

Tal situação é particularmente prejudicial em um momento em que esse acesso se torna crucial para a participação na vida política e o exercício dos direitos sociais, econômicos e culturais.

O Projeto também expandiu as obrigações de retenção de dados pré-existentes para permitir o monitoramento do encaminhamento de informações em aplicativos de mensagens. A medida não só vai diretamente contra os padrões internacionais de Direitos Humanos sobre o direito à privacidade, mas também coloca em risco constante as comunicações e a vida de defensores de Direitos Humanos, jornalistas e ativistas (WANDERLEI, 2021).

Outras preocupações em relação à última versão do Projeto incluem a possibilidade de bloquear as atividades das empresas de Internet no país; a obrigação de manter bases de dados com informações de usuários brasileiros em território nacional; o aumento das penalidades criminais por injúria, calúnia e difamação (incompatível com os padrões internacionais de Direitos Humanos); e o reforço das

obrigações pré-existentes de registro de cartões de celular, como tem sido apontado por uma ampla coalizão de organizações brasileiras (PAESANI, 2020).

A versão aprovada do texto é incapaz de cumprir o suposto objetivo de combater a desinformação, ao estimular a concentração na esfera digital, por meio de obrigações desproporcionais às empresas provedoras de serviços de internet, e a autocensura, estimulada pela vigilância excessiva e pela criminalização generalizada da fala (OLTRA, 2021).

Ao fazê-lo, o Projeto de Lei está em oposição direta ao que é afirmado por especialistas internacionais em Direitos Humanos sobre o assunto, que lembram que:

> Os Estados têm a obrigação positiva de promover um ambiente de comunicação livre, independente e diversificado, incluindo a diversidade da mídia, que é um meio fundamental para enfrentar a desinformação e a propaganda", e que "as proibições gerais sobre a divulgação de informações com base em conceitos imprecisos e ambíguos, incluindo "notícias falsas" ("fake news") ou "informações não objetivas", são incompatíveis com as normas internacionais sobre restrições à liberdade de expressão, conforme indicado no parágrafo 1(a) ), e deve ser revogada (WANDERLEI, 2021, p. 22).

Uma vez aprovada, esta lei estabelece um precedente preocupante para outros países que atualmente discutem regulamentações para restringir a desinformação. Trata-se de um debate complexo, que não pode ser avançado por mecanismos de tramitação urgentes ou desconsiderando seus impactos significativos sobre os Direitos Humanos e as garantias processuais.

A desinformação pode ter impactos negativos na democracia, liberdade de expressão, jornalismo e espaços cívicos, assim como tentativas inadequadas de regulá-la. Os Estados devem abster-se de adotar marcos regulatórios que não sejam baseados em evidências e sejam resultado de um amplo debate público, com a participação de diferentes setores da sociedade (WANDERLEI, 2021).

Como foi apontado por especialistas internacionais em Direitos Humanos em suas recomendações sobre como responder ao fenômeno da desinformação, os Estados só podem estabelecer restrições ao direito à liberdade de expressão de acordo com o teste previsto no direito internacional para tais restrições, que exige que sejam estipuladas na lei, atingem um dos interesses legítimos reconhecidos pelo direito internacional e são necessários e proporcionais para proteger esse interesse (PAESANI, 2020).

A ampla discussão multissetorial e a adoção de regras para garantir mais transparência e prestação de contas das empresas de internet, bem como mecanismos para o devido processo na moderação de conteúdo, são mais do que bem-vindos (PEREIRA, 2020).

Tal discussão deve considerar os padrões de Direitos Humanos que já reconhecem o controle concentrado das comunicações digitais como uma ameaça à liberdade de expressão. No entanto, o texto aprovado não atende a tais princípios e não deve ser adotado sem o devido debate público.

Pelas razões expostas, as organizações signatárias instaram os legisladores brasileiros a rejeitar a chamada "Lei das Fake News" (PL n. 2630/2020), retirar sua tramitação urgente e convocar um multi-diálogo com as partes interessadas para discutir como responder aos desafios da desinformação *online* de acordo com os compromissos do Estado brasileiro de respeitar o Direito Internacional dos Direitos Humanos e as normas existentes sobre o assunto.

## 5.1 IMPORTÂNCIA DA LEGISLAÇÃO

Diante da iminente transformação digital, é essencial promover e incentivar uma cultura de proteção de dados para tornar a Internet um lugar seguro para toda a população, mas especialmente para os grupos mais atrasados e vulneráveis.

Destaca-se a imperatividade de orientar o uso responsável das tecnologias da informação para proteger as informações pessoais que são compartilhadas e as consequências que existem.

Tem sido um desafio difundir boas práticas para o uso seguro e responsável dos serviços de internet em torno dos desafios em termos de segurança virtual e privacidade que surgem na vida cotidiana.

Insta consignar que a chamada nova normalidade transformou o ambiente digital tanto em termos de riscos como de oportunidades, em que as tecnologias nas redes digitais são um excelente meio de comunicação, além do fato de a internet ter se tornado uma extensão da vida não digital, daí a relevância dos órgãos garantidores para promover a proteção de dados no mundo virtual.

Destaca-se que a proteção de dados pessoais é um direito individual que reflete no cotidiano, portanto, seu cuidado deve ser permanente, principalmente com relação

a grupos vulneráveis da população, como crianças, adolescentes e idosos, os quais estão mais sujeitos a sofrer violência digital.

Enfatiza-se que nas últimas décadas houve uma transição de uma sociedade da informação analógica para uma sociedade baseada na informação digital, juntamente com isso, as mudanças tecnológicas foram progressivamente aceleradas, sendo certo que, com a pandemia, o ano de 2020 será lembrado como o ano que enviou a humanidade para a era digital forçadamente.

Diniz (2018) destaca que as tecnologias da informação desempenham um papel importante no cuidado dos direitos humanos, mas também na sua violação, pois podem ser usadas para a proteção de direitos, e podem, também, ser usadas para violar direitos, tais como a privacidade, por exemplo.

Por sua vez, Doneda (2020, p. 209) destacou que ao interagir com as plataformas digitais no cotidiano, fica-se exposta a violação da informação compartilhada e utilizada para outros fins. Por isso, a relação permanente entre os órgãos garantidores é importante para promover ações para uma Internet segura. Ele acrescentou que o proprietário tem a decisão do que compartilhar através da rede, mas também os provedores de tecnologia têm a responsabilidade de proteger a privacidade de qualquer pessoa.

Gonçalves (2018) fornece elementos necessários para configurar com segurança contas e serviços de internet, além de compartilhar diretrizes de privacidade na hora de navegar: o primeiro com o objetivo de que os usuários possam identificar as principais ameaças existentes com o uso de dispositivos tecnológicos, conexão *wi-fi* ou na contratação de serviços digitais, que podem ser utilizados para extorsão, roubo de dados, intervenção de linhas de comunicação e até dispositivos.

Ante todo o exposto no trabalho, observa-se que são muitos os desafios da sociedade no âmbito do direito digital.

Neste contexto, é importante refletir sobre a falta de uma cultura de proteção de dados pessoais, pois a educação nesse sentido poderia diminuir a vulnerabilidade dos cidadãos no âmbito digital. Nesse sentido, é preciso reagir a tal contexto para tornar a Internet um lugar seguro para todos. O direito à proteção de dados, na perspectiva da Internet segura, não é apenas uma ferramenta normativa, mas também uma cultura que, se adquirida corretamente, empodera as pessoas.

Se faz necessário maior ênfase a proteção de dados pessoais, notadamente junto às instituições de ensino, para alcançar os grupos mais vulneráveis, para que

esses conheçam e exijam seus direitos, também no ambiente virtual. Deve-se proteger os dados pessoais de crianças e adolescentes e fomentar uma cultura de proteção de suas informações pessoais.

Nesta ordem, convida-se a sociedade a cuidar dos dados que partilham nas redes sociais e a utilizar os mecanismos que existem para proteção, de forma a preservar sua privacidade. Da mesma forma, incentiva-se o cuidado com informações como a imagem, o nome, a idade e o endereço, bem como a relatar qualquer incidente.

É fundamental que a população conheça seus direitos com relação a proteção dos seus dados, pois é de suma importância o exercício da autodeterminação informativa e a adoção de medidas preventivas.

## 6 CONSIDERAÇÕES FINAIS

Diante da relevância cientifica e social do trabalho, observou-se que o crescimento do acesso à Internet ensejou novos cenários no ordenamento jurídico, notadamente os conhecidos crimes cibernéticos, surgindo assim a insegurança virtual, fazendo-se necessária a intervenção do Estado para promoção da segurança no ambiente virtual, para proteger os dados dos cidadãos.

Face ao dinamismo da tecnologia, diversas são as dificuldades encontradas para resolução de tais crimes, mas sendo o Direito regulador da ordem na sociedade, cabe a ele, portanto, acompanhar os avanços e atualizar o ordenamento jurídico para tipificar tais condutas e se adaptar a tal tecnologia que já é parte imprescindível do cotidiano do ser humano.

O trabalho teve como indagações de pesquisa: Quais motivos ensejaram a criação da LGPD? Seria a LGPD uma forma residual de responsabilidade, considerando o Marco Civil da internet no que concerne a este ponto? As empresas estão preparadas para se adequarem à LGPD?

Obteve-se como resposta que a criação da LGPD deu-se em razão da necessidade de proteção dos dados dos cidadãos, tanto no ambiente físico, quando no ambiente virtual. Essa necessidade maximizou-se com os avanços tecnológicos. Por isso, foi preciso incluir na Constituição Federal a proteção de dados pessoais entre os direitos e garantias fundamentais.

A LGPD também foi responsável por estabelecer a competência privativa da União para legislar sobre a proteção e o tratamento de dados pessoais, com o escopo de garantir a uniformidade da matéria.

Questionou-se também se seria a LGPD uma forma residual de responsabilidade, considerando o Marco Civil da internet no que concerne a este ponto.

Nesse sentido, tem-se que o Marco Civil da Internet se apresentou como revolucionário à sua época, estabelecendo que a internet é essencial ao exercício da cidadania e criando mecanismos para a defesa dos direitos dos usuários no ambiente virtual. Todavia, importante consignar que as disposições trazidas pelo Marco Civil da Internet se limitam ao ambiente virtual.

A LGPD, por sua vez, estabelece regras específicas de aplicação e segurança, conceituando os diferentes tipos de dados e os resguardando durante toda a circulação, tanto online quanto offline.

Assim sendo, a LGPD e o Marco Civil da Internet se complementam, de modo que uma lei não revoga a outra.

Com relação às empresas, certamente não estão prontas para adequarem-se à LGPD, considerando a complexidade da norma, todavia, terão de aprender na prática, para manterem-se no mercado. Outrossim, para auxiliar as empresas, há a figura ado *Compliance*.

Os objetivos do trabalho foram aprofundados e discernidos de maneira satisfatória, tendo sido possível: analisar a LGPD considerando os aspectos que a cercam, sua notabilidade e atualidade; expor de forma clara os fundamentos principiológicos trazidos pela LGPD; considerar de maneira sistemática as etapas da implementação da LGPD no ordenamento, tratando, inclusive, das profissões criadas para atender ao disposto nesta; demonstrar de forma clara a importância da implementação do tratamento adequado de dados pessoais; tratar das possíveis penalidades em caso de tratamento inadequado de dados pessoais, e, ainda, em caso de vazamento; apresentar respostas às questões propostas na introdução, assim como também responder às questões que vierem a surgir no curso do desenvolvimento da pesquisa; e analisar os recentes julgados relacionados à matéria.

Conclui-se que o ordenamento jurídico já tem legislação para ser aplicada quanto crimes no ambiente virtual, porém, não há eficácia total na proteção dos cidadãos no meio digital.

Vê-se então que na realidade o ordenamento não apresenta meios para punir todas as condutas criminosas que ocorrem no cenário virtual e as que são punidas tem como base penas que são ineficazes, vez que não trazem temor suficiente para inibir os criminosos.

Em resumo, com a LGPD o país está imerso em uma estrutura nova de proteção de dados que transcende o âmbito setorial, incluindo todo o tratamento e coleta de dados dentro do território nacional.

Conclui-se que a LGPD representa uma evolução, na medida em que se nota uma preocupação do legislador com a segurança e proteção do direito ao sigilo dos dados e informações no âmbito digital, mas não se pode esquecer que a lei ainda

precisa ser aprimorada, principalmente no sentido da clareza e da aplicabilidade de suas disposições.

Em reforço a essas considerações, vale frisar que a pesquisa não esgota o assunto, pois ele pode desdobrar-se em pesquisas de maior fôlego, que exijam maior tempo de consulta teórica acerca da matéria, além da pesquisa meramente bibliográfica, tais como pesquisas de campo e pesquisa-ação, a fim de se confrontarem os pressupostos teóricos.

Todavia, em que pesem as limitações do trabalho, ele tem a virtude de apontar caminhos para futuros pesquisadores, além servir de referencial teórico inicial para quem já trabalha na área.

## REFERÊNCIAS


BEVILAQUA, Clóvis. **Teoria Geral do direito Civil**. Campinas: Servanda, 2017.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2020.

BORGES. Roxana Cardoso Brasileiro. **Direitos de personalidade e autonomia privada**. São Paulo. Saraiva. 2018.

BRASIL. **AC 70034086116**. Brasília, DF: Congresso Nacional, 2019.

_____. **Código Civil Brasileiro.** Brasília, DF: Congresso Nacional, 2002.

_____. **Código de Defesa do Consumidor**. Brasília, DF: Congresso Nacional, 1990.

_____. **Código de Processo Penal**. Brasília, DF: Congresso Nacional, 1940.

_____. **Constituição da República Federativa do Brasil**. Brasília, DF: Congresso Nacional, 1988.

_____. **Convenção de Budapeste**. Brasília, DF: Congresso Nacional, 2018.2001.

_____. **Lei do Cadastro Positivo.** Lei 12.414. Brasília, DF: Congresso Nacional, 2011.

_____. **Lei de Acesso à Informação**. Lei 12.527. Brasília, DF: Congresso Nacional, 2011.

_____. **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF: Congresso Nacional, 2018.

_____. **Lei n. 9.279, de 14 de maio de 1996.** Brasília, DF: Congresso Nacional, 1996.

_____. **Marco Civil da Internet**. Lei 12.965. Brasília, DF: Congresso Nacional, 2014.

_____. **Projeto de Lei n. 5.276/2016**. Brasília, DF: Congresso Nacional, 2016.

_____. **Projeto de Lei n. 4554/2020**. Brasília, DF: Congresso Nacional, 2020.

BULOS, Uadi Lammêgo. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2019.

CAMPOS, Diogo Leite. **Estudos sobre o direito das pessoas**. Coimbra: Almedina, 2017.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. Rio de Janeiro: Lumem Juris, 2018.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. São Paulo: Saraiva, 2018.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**: teoria geral do Direito Civil. São Paulo: Saraiva, 2018.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2020.

FELICIANO, Guilherme Guimarães. **Informática e criminalidade**: São Paulo: Atlas, 2019.

GARCIA, Aristeu. **Privacidade e dados pessoais na rede**. São Paulo: Atlas, 2020.

GARCIA, Enéas Costa. **Direito geral da personalidade no sistema jurídico brasileiro**. São Paulo: Juarez de Oliveira, 2017.

GOMES, Orlando. **Introdução ao Direito Civil**. Rio de Janeiro, Forense, 2018.

GONÇALVES, Diogo Costa. **Pessoa e direitos de personalidade**: fundamentação ontológica da tutela. Coimbra: Almedina, 2018.

INELLAS, Gabriel Cesar. **Crimes na internet**. Belo Horizonte: Juarez de Oliveira, 2019.

LEONARDI, Marcel. **Responsabilidade civil dos provedores de serviços de internet**. São Paulo: Jus Navigandi, 2020.

LIMA, Cíntia Rosa Pereira. **Estudos avançados de Direito Digital**. Rio de Janeiro, Elsevier: 2019.

LIMONGI, Rubens. **Instituições de direito civil**. São Paulo: Saraiva, 2018.

MARTINS, Guilherme Magalhães. **Direito Privado e internet**. São Paulo: Atlas, 2020.

MIRANDA, Pontes de. **Tratado de Direito Privado**. São Paulo: Revista do Tribunal, 2012.

MOROZOV, Evgeny. **A decepção da internet**: os mitos da liberdade na rede, Barcelona, Destino, 2019.

NIGRI, Deborah Fisch. **Crimes e segurança na internet**. Rio de Janeiro: Instituto dos Magistrados do Brasil, 2016.

OLTRA, Christian. ***Naked Society***. Espanha: Editorial Círculo Rojo, 2021.

PAESANI, Liliana Minardi. **Direito e internet**: liberdade de informação, privacidade e responsabilidade civil. São Paulo: Atlas, 2020.

PEREIRA, Marcelo Cardoso. **Direito à intimidade na internet**. Curitiba: Juruá, 2020.

PINHEIRO, Patrícia. **Proteção de dados pessoais**: comentários à Lei 13.709/2018. São Paulo: Atlas, 2020.

RODOTA, Stefano. **Vida e regras**: entre o direito e o não direito. Madrid: Trotta, 2020.

ROSA, Fabrizio. **Crimes de informática**. São Paulo: Bookseller, 2012.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e Direito Penal**. São Paulo: Memória Jurídica, 2014.

SMALL, Gary; VORGAN, Gigi. ***The digital brain***: como as novas tecnologias estão mudando nossas mentes. Barcelona: Urano, 2019.

SILVA, Iuri; LIMA, Fabrício. **Manual de *Compliance* Trabalhista**: teoria e prática. Salvador: Editora JusPodivm, 2020.

SZANIAWSKI, Elimar. **Direitos de personalidade e sua tutela**. São Paulo. Revista dos Tribunais. 2015.

TARTUCE, Flávio; CASTILHO, Ricardo. **Direito Civil**: Direito Patrimonial/Direito Existencial. São Paulo: Método, 2016.

TOLEDO, Francisco de Assis. **Princípios básicos de Direito Penal.** Saraiva: São Paulo. 2017.

WANDERLEI, Felipe. **Crimes cibernéticos**: obstáculos para punibilidade do infrator. Araguaína: Forense, 2021.