UNIVERSIDADE NOVE DE JULHO
PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU*
DEPARTAMENTO DE PÓS-GRADUAÇÃO EM DIREITO

EDUARDO OTACIANO DA CRUZ

COLETA, UTILIZAÇÃO INDEVIDA E PROTEÇÃO DE DADOS NO AMBIENTE DIGITAL NA LEGISLAÇÃO BRASILEIRA: A INTERNET DAS COISAS COMO SISTEMA DE TRANSFERÊNCIA DE DADOS PESSOAIS

São Paulo
2024

EDUARDO OTACIANO DA CRUZ

COLETA, UTILIZAÇÃO INDEVIDA E PROTEÇÃO DE DADOS NO AMBIENTE DIGITAL NA LEGISLAÇÃO BRASILEIRA: A INTERNET DAS COISAS COMO SISTEMA DE TRANSFERÊNCIA DE DADOS PESSOAIS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação, *Stricto Sensu,* em Direito, PPGD, da Universidade Nove de Julho, área de concentração: Direito Empresarial - Estruturas e Regulação. Linha de pesquisa: Estruturas do Direito Empresarial, como parte dos requisitos necessários à obtenção do título de Mestre em Direito Empresarial.

Orientador: Professor Doutor Eduardo Tuma.

São Paulo
2024

Cruz, Eduardo Otaciano da.
Coleta, utilização indevida e proteção de dados no ambiente digital na legislação brasileira: a internet das coisas como sistema de transferência de dados pessoais. / Eduardo Otaciano da Cruz. 2024.
115 f.

Dissertação (Mestrado) - Universidade Nove de Julho - UNINOVE, São Paulo, 2024.
Orientador (a): Prof. Dr. Eduardo Tuma.

1. Internet das coisas. 2. Dados. 3. Coleta. 4. Uso indevido. 5. Proteção. 6. LGPD.
I. Tuma, Eduardo. II. Título.

CDU 34

EDUARDO OTACIANO DA CRUZ

COLETA, UTILIZAÇÃO INDEVIDA E PROTEÇÃO DE DADOS NO AMBIENTE DIGITAL NA LEGISLAÇÃO BRASILEIRA: A INTERNET DAS COISAS COMO SISTEMA DE TRANSFERÊNCIA DE DADOS PESSOAIS

Dissertação apresentada ao Programa de Pós-Graduação Stricto Sensu em Direito da Universidade Nove de Julho como parte das exigências para a obtenção do título de Mestre em Direito.

São Paulo, 21 de agosto de 2024.

BANCA EXAMINADORA

Prof. Dr. Eduardo Tuma
Orientador
UNINOVE

Profa. Dra. Claudia Lima Marques
Examinador Interno
UNINOVE

Profa. Dra. Ana Rita De Figueiredo Nery
Examinador Externo
MACKENZIE

Dedico esta pesquisa aos meus saudosos pais, Maria José Santana da Cruz (1937-2024) e Epaminondas Otaciano da Cruz (1936-2019). Embora tenham sido um casal de negros nordestinos que viveram durante a ditadura – uma época de muitas limitações, discriminações e rejeições que os impediram de estudar e alcançar uma vida mais digna – sempre me incentivaram a estudar, bem como me ensinaram os valores da ética e do comprometimento. Eles mostraram que os únicos caminhos para o sucesso são o temor a Deus, a dedicação aos estudos e o trabalho árduo.

Minha mãe, com sua sabedoria e paciência, ensinou-me a importância da resiliência e da generosidade. Meu pai, com sua luz, força e determinação, demonstrou que a honestidade e o esforço são fundamentais para superar as adversidades. A eles devo não apenas minha formação acadêmica, mas também os princípios e valores que guiam minha vida.

Agradeço profundamente por todo o amor, apoio e sacrifício que fizeram para que eu pudesse ter as oportunidades que lhes foram negadas. Seus exemplos de vida e suas lições serão eternamente lembrados e honrados.

A eles, minha eterna gratidão, respeito e amor.

Agradeço a ***Deus*** *por confiar-me aos meus pais, como dito anteriormente, pessoas incríveis, e por me conceder a vida e as oportunidades que tenho. Agradeço-Lhe pela força e sabedoria que me foram dadas para superar os desafios ao longo desta jornada. Sou grato por Sua constante presença, orientação, força, luz e proteção, que me proporcionaram coragem e determinação para alcançar meus objetivos. Reconheço que todas as conquistas e realizações desta pesquisa são uma manifestação de Sua graça e benevolência em minha vida.*

AGRADECIMENTOS

Expresso minha profunda gratidão à minha esposa, Claudineide Alves da Cruz, que me incentivou incondicionalmente ao longo desta jornada. Sua paciência, luz e constante apoio foram fundamentais para que eu pudesse perseverar nesta longa trajetória de estudos e dedicação. Às minhas filhas, Ana Caroline Alves da Cruz e Lais Alves da Cruz, agradeço a paciência e compreensão diante da minha ausência durante esses anos.

Manifesto meu sincero agradecimento ao Dr. Ricardo Felicio Scaff, meu grande amigo, que Deus colocou em meu caminho para me incentivar, apoiar e abrir portas na vida acadêmica e profissional. Sua presença foi essencial para o meu progresso e sucesso.

Agradeço de coração ao Dr. Eduardo Tuma, orientador desta pesquisa, cuja dedicação e orientação minuciosa foram cruciais para a conclusão deste estudo. Sua liderança e sabedoria guiaram-me em cada etapa do processo.

Aos meus colegas de estudos, Dra. Julianna Moreira Reis Garcia Guedes, Dra. Thaluana Alves da Penha, Dr. José Fabio Rodrigues Maciel e Dr. Jônatas Junqueira de Mello, sou imensamente grato pelo apoio nas pesquisas e nas revisões deste trabalho. Suas colaborações, inspirações e seus conhecimentos enriqueceram significativamente esta dissertação.

Expresso, ainda, um especial agradecimento aos meus professores, Dra. Claudia Lima Marques, Dra. Renata Mota Maciel e Dr. Celso Antonio Pacheco Fiorillo. Suas aulas, orientações e conselhos foram de extrema importância para o meu desenvolvimento acadêmico e para a realização deste projeto.

Por fim, expresso novamente minha gratidão a Deus, cuja graça e generosidade possibilitaram todas essas conquistas e a conclusão desta dissertação.

"Não ande espalhando calúnias entre o seu povo. Não ponha em perigo a vida do seu próximo. Eu sou o Senhor".

Levítico 19:16

"A sabedoria é a coisa principal; adquire, pois, a sabedoria; sim, com tudo o que possuis adquire o conhecimento".

Provérbios 4:7

RESUMO

A Sociedade da Informação é caracterizada pela rápida evolução e disseminação das tecnologias da informação e comunicação. Além da Internet, destaca-se a crescente disseminação da Internet das Coisas (*IoT*), uma tecnologia emergente que conecta dispositivos físicos, sistemas e objetos, gerando uma enorme quantidade de dados. Quando processados adequadamente, esses dados se transformam em informações valiosas. A *IoT* tem um impacto significativo em todos os setores da economia e na sociedade, tendo evoluído rapidamente nos últimos anos. Ao conectar diversos dispositivos inteligentes, a *IoT* gera e armazena vastas quantidades de dados, que aprimoram a eficiência, a segurança e a qualidade de vida. Adicionalmente, a Inteligência Artificial (IA) associada à Internet das Coisas permite que os dados coletados e convertidos em informações sejam processados de forma avançada, possibilitando que os profissionais tomem decisões imediatas e bem fundamentadas. Isso resulta em escolhas mais objetivas e informadas, baseadas em relatórios detalhados. Além disso, a IA, ao utilizar dados pessoais coletados nos ambientes digitais, pode antecipar o comportamento individual de certas pessoas, influenciando decisões que impactam suas vidas. Isso abrange desde transações comerciais até interações com o Estado, afetando diretamente a obtenção de bens, serviços e oportunidades no mercado de trabalho. Nesse cenário, contudo, emergem diversas questões legais relacionadas à privacidade e à segurança dos dados armazenados no ambiente digital: o tratamento de dados oriundos das inovações nos ambientes digitais pode constituir um risco considerável para a privacidade e a proteção de dados pessoais. Assim, o objetivo geral desta dissertação é explorar os desafios relacionados à privacidade e proteção de dados decorrentes das Tecnologias da Informação e Comunicação, com foco na Internet das Coisas, considerando os riscos associados à coleta, ao processamento e ao uso inadequado de informações pessoais. Para tanto, inicialmente discorre-se sobre a Sociedade da Informação e como a Internet das Coisas tem suscitado novos bens jurídicos a serem protegidos. A seguir, apresenta-se o panorama normativo brasileiro sobre a proteção de dados e privacidade nos ambientes digitais, com especial atenção à Lei Geral de Proteção de Dados. Afinal, discutem-se as vulnerabilidades e os riscos associados à proteção inadequada de dados pessoais em ambientes digitais. A pesquisa utiliza metodologia exploratório-descritiva e abordagem qualitativa, bem como utiliza procedimento bibliográfico e documental. Conclui-se que a proteção dos dados pessoais no ambiente digital, mais especificamente no contexto da Internet das Coisas, exige uma abordagem multifacetada que envolve avanços tecnológicos, regulamentações jurídicas eficazes, práticas empresariais responsáveis e uma cidadania digital

informada. Somente através de esforços combinados em todos esses níveis é possível garantir que a privacidade e a segurança dos dados pessoais sejam plenamente respeitadas e protegidas na era digital.

Palavras-chave: Internet das Coisas; dados; coleta; uso indevido; proteção; LGPD.

ABSTRACT

The Information Society is characterized by the rapid evolution and dissemination of information and communication technologies. Beyond the Internet, the growing spread of the Internet of Things (IoT) stands out, an emerging technology that connects physical devices, systems, and objects, generating a vast amount of data. When adequately processed, this data transforms into valuable information. IoT has a significant impact on all sectors of the economy and society, having rapidly evolved in recent years. By connecting various smart devices, IoT generates and stores vast amounts of data, which enhance efficiency, safety, and quality of life. Additionally, Artificial Intelligence (AI) associated with the Internet of Things allows the collected data, converted into information, to be processed in an advanced manner, enabling professionals to make immediate and well-founded decisions. This results in more objective and informed choices, based on detailed reports. Furthermore, AI, by using personal data collected in digital environments, can anticipate the individual behavior of certain people, influencing decisions that impact their lives. This encompasses everything from commercial transactions to interactions with the state, directly affecting access to goods, services, and job market opportunities. In this scenario, however, various legal issues related to the privacy and security of data stored in the digital environment emerge: the handling of data arising from innovations in digital environments can constitute a considerable risk to privacy and the protection of personal data. Thus, the general objective of this dissertation is to explore the challenges related to privacy and data protection arising from Information and Communication Technologies, focusing on the Internet of Things, considering the risks associated with the collection, processing, and misuse of personal information. To this end, it initially discusses the Information Society and how the Internet of Things has raised new legal assets to be protected. Next, it presents the Brazilian regulatory framework on data protection and privacy in digital environments, with special attention to the General Data Protection Law. Finally, it discusses the vulnerabilities and risks associated with inadequate protection of personal data in digital environments. The research employs an exploratory-descriptive methodology and a qualitative approach, as well as employs bibliographic and documentary procedures. It concludes that the protection of personal data in the digital environment, specifically in the context of the Internet of Things, requires a multifaceted approach involving technological advances, effective legal regulations, responsible business practices, and informed digital citizenship. Only through combined efforts at all these levels can it be ensured that privacy and security of personal data are fully respected and protected in the digital age.

Keywords: Internet of Things; data; collection; misuse; protection; LGPD.

LISTA DE FIGURAS

LISTA DE SIGLAS E ABREVIATURAS

ABES	Associação Brasileira das Empresas de *Software*
ABNT	Associação Brasileira de Normas Técnicas
ACR	Reconhecimento Automático de Conteúdo
ADIn	Ação Direta de Inconstitucionalidade
ANPD	Autoridade Nacional de Proteção de Dados
ARPANET	*Advanced Research Projects Agency Network*
BNDES	Banco Nacional de Desenvolvimento Econômico e Social
CADE	Conselho Administrativo de Defesa Econômica
CBCI	Carta Brasileira para Cidades Inteligentes
CDC	Código de Defesa do Consumidor
CF	Constituição Federal
CPF	Cadastro de Pessoa Física
EC	Emenda Constitucional
EUA	Estados Unidos da América
FDD	Fundo de Defesa de Direitos Difusos
FTC	*Federal Trade Comission*
GDPR	Regulamento Geral de Proteção de Dados Pessoais Europeu
HCFMUSP	Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo
IBGE	Instituto Brasileiro de Geografia e Estatística
IA	Inteligência Artificial
ICN	Infraestruturas Críticas Nacionais
IDC	*International Data Corporation*
IDEC	Instituto Brasileiro de Defesa ao Consumidor
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
InovaInCor	Núcleo de Inovação do InCor
INSS	Instituto Nacional do Seguro Social
IoT	Internet das Coisas
IIoT	Internet das Coisas Industrial
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
LPWAN	*Low-Power Wide Area Network*

MCI	Marco Civil da Internet
MCTIC	Ministério da Ciência, Tecnologia, Inovações e Comunicações
NFC	*Near Field Communication*
NIST	*National Institute of Standards and Technology*
NSA	Agência de Segurança Nacional Norteamericana
PL	Projeto de Lei
RFID	*Radio-Frequency Identification*
RG	Registro Geral
SENACON	Secretaria Nacional do Consumidor
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TAC	Telemonitoramento do Ato Cirúrgico
TICs	Tecnologias da Informação e Comunicação
TV	Televisão
UE	União Europeia
Wi-Fi	*Wireless LAN*

SUMÁRIO

INTRODUÇÃO

A Sociedade da Informação é um termo que descreve a atual era em que vivemos, caracterizada pela rápida evolução e disseminação das tecnologias da informação e comunicação. Nessa sociedade, a informação se tornou um recurso essencial e estratégico, e a capacidade de acessá-la, processá-la e utilizá-la de maneira eficiente tornou-se fundamental para o desenvolvimento pessoal, social e econômico.

Um dos principais impulsionadores da Sociedade da Informação é a Internet, capaz de conectar bilhões de pessoas e dispositivos em todo o mundo. No entanto, além da Internet, uma tendência importante nessa sociedade é o crescimento da Internet das Coisas (*IoT*, do inglês *Internet of Things*), uma tecnologia emergente que permite a conexão de dispositivos físicos, sistemas e objetos e produz enorme quantidade de dados, que devidamente processados tornam-se informação.

É esperado que a Internet das Coisas apresente um impacto significativo em todos os setores da economia e na sociedade, visto ter evoluído muito rapidamente nos últimos anos. A *IoT* conecta diversos dispositivos inteligentes, gerando e armazenando enormes quantidades de dados que aprimoram a eficiência, segurança e qualidade de vida. Isso impulsiona novos modelos de negócios, melhora processos produtivos e operacionais, tornando a *IoT* um pilar da transformação digital e a informação o "novo petróleo" da Era Digital.

Além disso, a Internet das Coisas transforma cidades por meio de soluções inteligentes, promove o crescimento econômico, impulsiona o desenvolvimento tecnológico e torna os ambientes residenciais e empresariais mais autônomos.

Adicionalmente, destaca-se que a Inteligência Artificial (IA)[1] associada à Internet das Coisas permite que os dados coletados e convertidos em informações sejam processados pela IA possibilitando que os profissionais envolvidos tomem decisões imediatas e assim decidam os próximos passos com base em relatórios fundamentados em dados, resultando em decisões melhores e mais objetivas.

Ademais, a Inteligência Artificial, ao utilizar os dados pessoais coletados nos ambientes digitais, pode ser empregada para antecipar o comportamento individual de certos indivíduos, embasando decisões que impactam suas vidas, tanto em suas transações comerciais quanto em

[1] Inteligência Artificial (IA) é uma denominação comumente empregada para se referir ao campo da ciência destinado a fornecer máquinas com a capacidade de realizar funções como lógica, raciocínio, planejamento, aprendizagem e percepção (Santos, 2021, p. 6).

suas interações com o Estado, afetando diretamente a obtenção de bens, serviços e até mesmo oportunidades no mercado de trabalho.

Assim, com o significativo avanço das Tecnologias da Informação e Comunicação (TICs)[2], bem como a crescente utilização de dados pessoais nessas tecnologias, que são capazes de tomar decisões por meio de algoritmos, surgem preocupações quanto aos possíveis danos, demandando atenção do campo jurídico. Dessa forma, emergem diversas questões legais relacionadas à privacidade e à segurança dos dados armazenados no ambiente digital. A coleta, o processamento e o uso indevidos dos dados, ou seja, o tratamento de dados[3] oriundos das inovações nos ambientes digitais, podem constituir um risco considerável para a privacidade e a proteção de dados pessoais[4.]

Nesse contexto, embora exista um conjunto de leis que abordam a proteção de dados pessoais e os direitos a privacidade, tais como o Código de Defesa do Consumidor, a Lei de Acesso à Informação, o Cadastro Positivo, o Marco Civil da Internet e a própria Constituição Federal entre outras, a Lei Geral de Proteção de Dados Pessoais (LGPD) desponta como uma importante legislação de proteção dos direitos fundamentais de privacidade e proteção de dados pessoais.

A LGPD, além de instituir normas para coleta, armazenamento e processamento dos dados pessoais, estipula uma série de obrigações para a sua proteção, dentre as quais figuram a necessidade de consentimento[5], transparência, e implementação de medidas de segurança. A Lei Geral de Proteção de Dados ainda estabelece sanções administrativas, como multas, advertências e suspensão do tratamento de dados e, nos casos mais graves, a responsabilização civil dos agentes responsáveis pelo tratamento de dados.

Nesse cenário, o objetivo geral desta dissertação é explorar os desafios relacionados à privacidade e proteção de dados decorrentes das Tecnologias da Informação e Comunicação, com foco na Internet das Coisas, considerando os riscos associados à coleta, ao processamento e ao uso inadequado de informações pessoais. Para o alcance dessa finalidade, no primeiro capítulo, torna-se imperativo discorrer sobre a Sociedade da Informação e como a Internet das

---

[2] Tecnologias da Informação e Comunicação (TICs) podem ser definidas como o conjunto total de tecnologias que permitem a produção, o acesso e a propagação de informações, assim como tecnologias que permitem a comunicação entre pessoas (Rodrigues, 2016, p. 15).

[3] Tratamento é gênero, que compreende toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, conforme inciso X do art. 5º da LGPD (Brasil, 2018).

[4] Dados pessoais referem-se a todas as informações relacionadas a uma pessoa natural identificada ou identificável, nos termos do inciso I, art. 5º, da LGPD (Brasil, 2018).

[5] Consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, de acordo com o inciso IX do art. 5º da LGPD (Brasil, 2018).

Coisas tem suscitado novos bens jurídicos a serem protegidos. Apresenta-se o desenvolvimento da Sociedade da Informação, da Internet e da Internet das Coisas, bem como o funcionamento da Internet das Coisas e algumas de suas aplicações, destacando também os benefícios advindos dessa tecnologia.

Na sequência, o segundo capítulo tem como objetivo específico examinar a regulamentação brasileira acerca da proteção de dados e privacidade nos ambientes digitais, com especial atenção à Lei Geral de Proteção de Dados. Discute-se então a proteção de dados pessoais e a privacidade no ambiente digital, abordando seus fundamentos constitucionais e legais. São analisadas legislações importantes como o Código de Defesa do Consumidor, a Lei de Acesso à Informação, o Cadastro Positivo, a Lei de Direito à Resposta e o Marco Civil da Internet. Apresentam-se também o projeto de Lei do Marco Legal da Inteligência Artificial e o Anteprojeto de Lei para revisão e atualização do Código Civil. Tudo isso para que se compreenda o panorama da proteção de dados no Brasil.

Afinal, esta pesquisa discute as implicações legais e regulatórias relacionadas à coleta e ao uso indevido de dados gerados pelos dispositivos conectados, com foco nas vulnerabilidades e nos riscos associados à proteção inadequada de dados pessoais em ambientes digitais. Assim, no terceiro capítulo, são examinadas as diferentes formas de violações do direito à privacidade na Internet das Coisas, em suas mais diversas manifestações, bem como suas consequências. Abordam-se a temática da vulnerabilidade no tratamento dos dados pessoais na internet das coisas e os riscos associados ao tratamento inadequado desses dados para indivíduos, organizações e o ambiente econômico e social.

A pesquisa adota uma metodologia exploratório-descritiva com abordagem qualitativa. Utiliza procedimentos bibliográfico e documental, com levantamento de fontes como livros, artigos, relatórios (nacionais e internacionais) e legislações. O método dialético foi empregado para comparar e debater tais fontes. Especificamente no último capítulo, discorre-se sobre casos de empresas de tecnologia para demonstração de hipóteses de violação de dados na internet das coisas.

O estudo se justifica acadêmica e socialmente. Primeiro porque a *IoT* apresenta desafios únicos para a regulação de privacidade, devido à sua natureza distribuída e interconectada, sendo necessária a regulamentação dos direitos dos usuários e as responsabilidades das organizações. Aqui, é fornecida uma compreensão sobre tais implicações legais e regulatórias. Além disso, a coleta inadequada de dados e a falta de segurança podem ter impactos significativos na vida dos usuários, incluindo a violação de sua privacidade e a exposição a riscos cibernéticos, sendo essencial que tenham consciência disso. Afinal, a pesquisa ajuda a

identificar e mitigar esses riscos, contribuindo para a criação de soluções mais seguras e eficazes para a proteção de dados na *IoT*.

Por outra perspectiva, todos esses elementos fazem com que a investigação contribua para o fortalecimento da economia. Perceba-se que soluções seguras são essenciais para a adoção em larga escala da *IoT*, fortalecendo seu impacto econômico, e um ambiente regulatório apropriado cria confiança e segurança, estimulando investimentos e inovação. Além disso, a pesquisa sobre privacidade na *IoT* ajuda a educar e conscientizar os consumidores sobre os riscos e melhores práticas de segurança e consumidores confiantes estão mais dispostos a adotar soluções *IoT*, impulsionando o crescimento econômico. Ademais, ao abordar os desafios da *IoT*, esse estudo incentiva a busca por soluções inovadoras em segurança e privacidade.

Em resumo, um estudo sobre os desafios de privacidade na *IoT* contribui para o fortalecimento da economia ao promover soluções seguras, um ambiente regulatório adequado, confiança do consumidor, investimentos e inovação, o que aproxima o objeto investigado da Linha de pesquisa “Estruturas do Direito Empresarial” deste Programa de Pós-Graduação.

1 SOCIEDADE DA INFORMAÇÃO, INTERNET E INTERNET DAS COISAS – CONCEITOS E PERSPECTIVA HISTÓRICA

Ao longo da história, a humanidade vivenciou distintas eras, tais como a agrícola, a industrial e, mais recentemente, a Era da Informação. Cada uma delas desencadeou transformações profundas na maneira como as pessoas conduzem suas vidas, suas atividades laborais e suas interações na sociedade.

Segundo os ensinamentos de Castells (1999, p. 53), cada modo de desenvolvimento é caracterizado pelo fator fundamental que impulsiona a produtividade no processo produtivo. No contexto do modo agrário de desenvolvimento, o incremento do excedente ocorre, principalmente, por meio do aumento quantitativo da mão de obra e da exploração dos recursos naturais. Já no modo de desenvolvimento industrial, a principal fonte de produtividade reside na introdução de novas fontes de energia e na capacidade de descentralizar seu uso ao longo dos processos produtivos e de circulação.

A Era da Informação, conhecida também como Sociedade da Informação ou Era Digital, é marcada pela disseminação abrangente e pelo amplo acesso à informação. Como ensina Celso Antônio Pacheco Fiorillo (2014, p. 123), a Sociedade da Informação pode ser definida como um cenário em que as tecnologias da comunicação fornecem a infraestrutura para a integração global e facilitam o rápido intercâmbio de informações entre indivíduos, empresas e instituições. Apesar das contradições e desigualdades presentes nesse cenário, a Sociedade da Informação representa uma nova forma de estabelecer relações sociais, baseada na flexibilidade e no estímulo à capacidade criativa.

Essa nova era é caracterizada pela crescente dependência das Tecnologias da Informação e Comunicação, que desempenham um papel fundamental em várias esferas da vida moderna. Além disso, na Era da Informação, o conhecimento se tornou um recurso indispensável para o progresso individual, social e econômico. Neste sentido, ensina Tadao Takahashi (2000, p. 6):

> O conhecimento tornou-se, hoje mais do que no passado, um dos principais fatores de superação de desigualdades, de agregação de valor, criação de emprego qualificado e de propagação do bem-estar. A nova situação tem reflexos no sistema econômico e político. A soberania e a autonomia dos países passam mundialmente por uma nova leitura, e sua manutenção - que é essencial - depende nitidamente do conhecimento, da educação e do desenvolvimento científico e tecnológico.

A capacidade de acessar, compartilhar e utilizar informações de maneira eficiente tornou-se essencial para enfrentar os desafios e aproveitar as oportunidades que surgem nesse

contexto. Nas palavras de Castells (1999, p. 35): “No novo modo informacional de desenvolvimento, a fonte de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos”.

Nas últimas décadas, ocorreram avanços tecnológicos significativos que impulsionaram ainda mais a evolução da Era da Informação. Desenvolvimento de computadores pessoais mais poderosos, dispositivos móveis, Inteligência Artificial, Computação em Nuvem, Redes Sociais e o advento da Internet das Coisas ampliaram ainda mais o acesso à informação, a capacidade de processamento e a interconexão global. Tudo isso permite que indivíduos, organizações e dispositivos estejam interligados e tenham acesso rápido e fácil a uma quantidade massiva de informações em tempo real.

Nesse sentido, ensina Danilo Doneda (2011, p. 2):

> A informação, em si, está ligada a uma série de fenômenos que cresceram em importância e complexidade de forma marcante nas últimas décadas. O que hoje a destaca de seu significado histórico é uma maior desenvoltura na sua manipulação, desde a coleta e tratamento até a comunicação da informação. Aumentando-se a capacidade de armazenamento e comunicação de informações, cresce também a variedade de formas pelas quais ela pode ser apropriada ou utilizada. Sendo maior sua maleabilidade e utilidade, mais e mais ela se torna em elemento fundamental de um crescente número de relações e aumenta sua possibilidade de influir em nosso cotidiano, em um crescente que tem como pano de fundo a evolução tecnológica e, especificamente, a utilização de computadores para o tratamento de dados pessoais– conforme notou Stefano Rodotà ainda em 1973, ‘[...] a novidade fundamental introduzida pelos computadores é a transformação de informação dispersa em informação organizada.

O que caracteriza a atual revolução tecnológica não é a centralidade de conhecimentos em informação, mas a aplicação da informação para geração de conhecimentos e de dispositivos de processamento e comunicação. Informação e conhecimento sempre foram elementos para alavancar a economia, e a evolução da tecnologia determinou em grande parte a capacidade produtiva da sociedade e os padrões de vida, bem como formas sociais de organização econômica (Castells, 1999, p. 119).

A Sociedade da Informação, no entendimento de Takahashi (2000, p. 28), “representa uma profunda mudança na organização da sociedade e da economia, havendo quem a considere um novo paradigma técnico-econômico. É um fenômeno global, com elevado potencial transformador das atividades sociais e econômicas”.

Nesse contexto, uma nova economia informacional, global e em rede emergiu em escala global no último quartel do século XX:

> É informacional porque a produtividade e a competitividade de unidades ou agentes nessa economia (sejam empresas, regiões ou nações) dependem basicamente de sua capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos. É global porque as principais atividades produtivas, o consumo e circulação, assim como seus componentes (capital, trabalho, matéria-prima, administração, informação, tecnologia e mercados) estão organizados em escala global, diretamente ou mediante uma rede de conexões entre agentes econômicos. É rede porque, nas novas condições históricas, a produtividade é gerada, e concorrência é feita em uma rede global de interação entre redes empresariais. Essa nova economia surgiu no último quartel do século XX porque a revolução tecnologia da informação forneceu a base material indispensável para sua criação. É a conexão histórica entre a base de informações/conhecimentos da economia, seu alcance global, sua forma de organização em rede e a revolução da tecnologia da informação que cria um novo sistema econômico (Castells, 1999, p. 119).

No entanto, a transição da Revolução Industrial para a Sociedade da Informação foi um processo complexo que abrangeu uma série de características distintas e incorporou avanços tecnológicos, transformações econômicas e mudanças sociais e culturais ao longo do tempo. Essa evolução foi impulsionada por fatores como a rápida disseminação das tecnologias de informação e comunicação, a crescente dependência de sistemas digitais, a interconectividade global e o aumento do acesso à informação.

De acordo com Takahashi (2000, p. 28), a transformação da Sociedade da Informação tem sua origem em três fenômenos inter-relacionados. O primeiro é a convergência de conteúdos, computação e comunicações, que possibilitou a integração desses elementos. O segundo aspecto está relacionado à dinâmica da indústria, que tem promovido a constante redução dos preços dos computadores em relação à sua capacidade de processamento, tornando essas máquinas cada vez mais acessíveis e disseminadas. Por fim, o terceiro elemento, em grande parte como resultado dos dois primeiros fenômenos, é o crescimento exponencial da Internet.

A história da comunicação e do armazenamento de informações percorreu várias fases ao longo do tempo. Inicialmente, a comunicação baseava-se na forma oral e em sistemas rudimentares de escrita, como pictogramas e hieróglifos, que apresentavam limitações em termos de alcance e preservação de informações. No entanto, nas palavras de Rosa Maria Cardoso Dalla Costa (2020, p. 56), um marco significativo ocorreu com a invenção da prensa móvel por Johannes Gutenberg no século XV. Essa inovação viabilizou a produção em massa de livros e panfletos, tornando a informação mais acessível e acelerando a disseminação do conhecimento.

O surgimento da Revolução Industrial no século XVIII foi um ponto decisivo para a evolução em direção à Era da Informação. A partir do século XIX, surgiram avanços tecnológicos significativos, como a invenção da máquina a vapor, a eletricidade e a produção

em cadeia. No século XX, o desenvolvimento de tecnologias de telecomunicações e eletrônicas foi fundamental para a evolução em direção à Era da Informação.

Conforme Castells (1999, p. 71), os historiadores reconhecem a ocorrência de pelo menos duas revoluções industriais. A primeira teve início antes dos últimos trinta anos do século XVIII e se caracterizou por inovações como a introdução da máquina a vapor, a invenção da fiadeira e a substituição das ferramentas manuais por máquinas. A segunda, ocorrida aproximadamente cem anos mais tarde, foi marcada pelo desenvolvimento da eletricidade, a criação do motor de combustão interna, o surgimento de produtos químicos baseados em ciência e o advento das tecnologias de comunicação, como o telégrafo e o telefone.

Para Beltramelli Neto e Melo (2022, p. 540), as transformações na indústria dos séculos XVIII, XIX e XX, conhecidas como revoluções industriais, modificaram significativamente os métodos de produção, a economia e as interações sociais relacionadas ao trabalho. Essas mudanças resultaram em profundas alterações nas relações humanas, contribuindo para a urbanização e o crescimento das grandes cidades. A primeira revolução estabeleceu uma divisão clara de tarefas; a segunda introduziu máquinas pesadas; e a terceira promoveu o uso de tecnologia eletrônica na produção. Cada uma dessas revoluções alterou não apenas a produção, mas também a dinâmica social.

Os mesmos autores (Beltramelli Neto; Melo, 2022, p. 540) apontam ainda que, nas últimas três décadas, uma nova transformação, impulsionada pela tecnologia digital e pela Internet, tem remodelado a produção. A automação e os computadores estão sendo complementados por tecnologias inovadoras como Inteligência Artificial, Tecnologia da Informação e Comunicação, Internet das Coisas, Nanotecnologia e Computação Quântica. Esse fenômeno é conhecido como "Quarta Revolução Industrial" e promete grandes mudanças nas interações humanas e na relação com o ambiente.

Para entender essa Quarta Revolução Industrial, é importante revisitar, mesmo que em poucas linhas, aquelas revoluções anteriores. A primeira, ocorrida na Europa no final do século XVIII, foi marcada pela substituição de ferramentas manuais por máquinas a vapor e pela construção de sistemas ferroviários. Essa transição do trabalho agrícola e artesanal para o assalariado urbano, não regulamentado pelo Estado, representou a consolidação do capitalismo industrial, focado na eficiência e na otimização do tempo de produção (Gamba, 2020, p. 69-70).

A Segunda Revolução Industrial, que se estendeu do final do século XIX até a Segunda Guerra Mundial, destacou-se pelo uso do motor de combustão interna, da eletricidade e pela expansão da indústria petrolífera. O desenvolvimento do aço permitiu a expansão das ferrovias

e, posteriormente, o uso de combustíveis para automóveis e aviões. A Primeira Guerra Mundial acelerou o avanço industrial e mostrou a importância do Estado na coordenação econômica e no desenvolvimento tecnológico (Gamba, 2020, p. 70).

A Terceira Revolução Industrial, surgida no pós-guerra, é caracterizada pelo crescimento rápido da informática na gestão e produção de assuntos econômicos e políticos, associada ao capitalismo tardio (Gamba, 2020, p. 71). Nesse cenário de complexidade econômica e progresso tecnológico, o capitalista industrial tradicional foi gradualmente substituído por especialistas técnicos e financeiros. A ciência, antes uma ferramenta, tornou-se elemento central na produção, disseminando avanços técnicos em todas as esferas sociais (Gamba, 2020, p. 73). Esse período marcou o declínio do capitalismo industrial e a transição para uma economia baseada em serviços e propriedades intangíveis (Gamba, 2020, p. 75).

Atualmente, a Quarta Revolução Industrial, em andamento na terceira década do século XXI, é definida pela interconexão em rede e pelo uso crescente de tecnologias disruptivas como robótica, Inteligência Artificial, Nanotecnologia, impressão 3D, aprendizado de máquina, Internet das Coisas e *Big Data* (Gamba, 2020, p. 76). Segundo Schwab (2016, p. 16), essa revolução é caracterizada pela integração e interdependência dos campos físico, digital e biológico. Castells (1999, p. 108) argumenta que a informação é o elemento central do novo modelo, com tecnologias desenvolvidas para manipulação de dados, sendo a marca distintiva desta revolução.

A capacidade de armazenar e processar informações cresceu exponencialmente devido à natureza imaterial dos dados e ao contínuo aprimoramento das tecnologias, que permitem maior armazenamento em dispositivos menores (Gamba, 2020, p. 78). Na Era Digital, ou Era da Informação, a conexão e o acesso rápido à informação são sem precedentes (Penteado, 2023, p. 25). A Quarta Revolução Industrial e a transformação digital, impulsionadas por tecnologias como redes 5G, Realidade Virtual, Realidade Aumentada, *blockchain*, Nanotecnologia, Robótica e Inteligência Artificial, estão moldando um cenário notável (Fernandes, 2022, p. 247-248). O ponto crucial dessa revolução é a capacidade de produzir e processar informações de forma eficaz, destacando-se aqueles com conhecimento e tecnologia para coletar e processar dados adequadamente (Gamba, 2020, p. 78).

Como se observa, o advento do telégrafo, do telefone, do rádio e da televisão possibilitou uma comunicação mais rápida e eficiente em escala global. Já a eletrônica, com a invenção dos primeiros computadores, abriu caminho para a automação e o processamento de informações em larga escala, enquanto a criação da Internet nas décadas de 1960 e 1970 e o

posterior desenvolvimento das tecnologias digitais desempenharam um papel fundamental na transição para a Era da Informação.

Assim, as interações culturais e comerciais intensificaram-se, promovendo a difusão de ideias, inovações e tendências. Isso contribuiu para a formação de uma sociedade global mais interconectada e tecnológica, com as informações fluindo de forma mais rápida e abrangente.

O conceito de tecnologia engloba um conjunto de processos, métodos, técnicas e ferramentas relacionados à arte, indústria e educação, que envolvem a aplicação prática do conhecimento. De maneira mais abrangente, refere-se ao conjunto de conhecimentos, ferramentas, métodos e processos usados para criar, modificar ou aprimorar produtos, serviços ou sistemas para atender às necessidades humanas (Michaelis, 2023). É uma ciência cujo objeto é a aplicação do conhecimento técnico e científico para fins industriais e comerciais (Priberam, 2008-2021).

A tecnologia está presente em praticamente todos os aspectos da sociedade moderna. Tem um papel importante na comunicação, no emprego, na saúde, no entretenimento, na educação, e em outros setores da economia. Desempenha uma função fundamental na moldagem do estilo de vida humano, abrangendo desde os padrões de comunicação até os processos de produção e consumo de bens e serviços. Sua influência é essencial para o progresso social e econômico, contribuindo significativamente para melhorar as condições de vida da humanidade.

Nesse sentido, ensinam Carstens e Fonseca (2019, p. 5):

> Segundo a inevitável lógica da evolução, a inovação e a tecnologia são elementos propulsores da humanidade, fruto de habilidades fundamentais em que estão intrinsecamente ligados à nossa existência; não sobreviveríamos a tantos milênios se não tivéssemos capacidade criativa e a convertêssemos em inovações. Não existe inovação sem tecnologia e ambas se complementam. Inovação é mudança e avanço tecnológico.

Para atender às mais recentes demandas dos consumidores, as empresas estão desenvolvendo produtos com interfaces tecnológicas que seriam inimagináveis há uma década. A tecnologia está mudando rapidamente a maneira como interagirmos com o mundo à nossa volta (Magrani, 2019, p. 19).

A inovação e o avanço tecnológico das últimas décadas, conforme as palavras de José Fabio Rodrigues Maciel e Thaluana Alves da Penha (2023, p. 161), "vêm trazendo transformações relevantes para a humanidade. Todos os setores da sociedade passaram a se conectar no ambiente digital, e o que antes era revolucionário tornou-se corriqueiro.”

Segundo Luiz Fernando Afonso (2020, p. RB-19.1), ouvimos afirmações como “robôs são alternativas para melhorar o atendimento ao consumidor”; “as máquinas fazem diagnósticos mais precisos do que os humanos”; “os robôs mostrarão com exatidão quase infalível as chances de vitória de certo recurso em determinado tribunal”; “a Internet das Coisas já é usada como prova em julgamentos”, que estão entre muitas outras possíveis novas soluções que a tecnologia poderá trazer ao mundo. O fato é que a tecnologia nos apresenta severos desafios, inclusive, desafios jurídicos, o que demandará dos profissionais do direito do século XXI novas habilidades que lhes serão necessárias.

Nesse cenário, a presente seção tem como objetivo discorrer sobre a Internet das Coisas, seu funcionamento e algumas de suas aplicações, destacando como ela tem suscitado novos bens jurídicos a serem protegidos.

1.1 A INTERNET NA SOCIEDADE DA INFORMAÇÃO

A Internet é uma tecnologia revolucionária que conecta computadores e dispositivos eletrônicos globalmente, permitindo a rápida transferência de dados, troca de informações e comunicação entre pessoas, além de proporcionar acesso a recursos digitais.

Segundo Cunha (2022, p. 61), a tecnologia digital permite que os cidadãos acessem informações e tomem conhecimento de fatos em tempo real. Com o crescente uso dessas tecnologias, uma parte significativa da população tem obtido informações de forma instantânea. Por meio da Internet, é viável explorar locais de qualquer parte do mundo e se informar sobre acontecimentos em tempo real, mesmo que se esteja no lado oposto do planeta. Além disso, a Internet permite que indivíduos de diferentes partes do mundo interajam entre si, possibilitando visitas virtuais a museus e a descoberta de novos lugares, assim como a interação com pessoas de diversas nacionalidades.

Através da Internet é possível a realização de compras *online*, bem como o estudo e o trabalho à distância. Ao mesmo tempo, ela possibilita consultas médicas e cirurgias remotas, revolucionando a prestação de serviços de saúde. Além disso, a Internet viabiliza diversas formas de entretenimento e lazer, como jogos *online*, serviços de *streaming* de filmes e séries, e interações sociais em redes sociais, todas elas transformadoras em nosso mundo contemporâneo.

A origem da Internet remonta aos anos 1960, durante a Guerra Fria, quando o Departamento de Defesa dos Estados Unidos estava preocupado com a segurança das comunicações militares em caso de um ataque nuclear. Para evitar a interrupção das

comunicações, pesquisadores começaram a explorar a ideia de criar uma rede descentralizada e robusta, capaz de continuar funcionando mesmo em caso de falhas em pontos específicos. Nesse sentido, escreve Eduardo Magrani (2018, p. 61):

> A Internet surgiu no final da década de 1960, criada no âmbito do Projeto *Advanced Research Projects Agency Network (ARPANET)*, vinculado à *Defense Advanced Research Projects Agency (Darpa)*. Financiando pelo governo federal dos Estados Unidos, tinha o intuito de construir uma comunicação resistente a falhas ou ataques locais, por meio da criação de uma rede de computadores interconectados utilizando o protocolo TCP/IP para se comunicar entre si.

Em 1969, o *Advanced Research Projects Agency Network* (ARPANET) foi lançado nos Estados Unidos. Ele foi o precursor da Internet criado pela Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos da América (EUA). O ARPANET interligava computadores de universidades e instituições de pesquisa, permitindo a troca de informações e o compartilhamento de recursos (Forouzan; Mosharraf, 2013, p. 22).

A Internet, também chamada de Rede Mundial de Computadores, é uma rede global, descentralizada, que através de linhas comuns de telefone, linhas de comunicação privadas, cabos submarinos, canais de satélite, redes sem fio e diversos outros meios de telecomunicações, utiliza protocolos de rede padrão para interligar ampla variedade de redes locais, regionais e globais, permitindo a comunicação, o acesso a recursos e serviços e a troca de dados entre diferentes sistemas e dispositivos. Nesse sentido, ensinam Kurose e Ross (2009, p. 2):

> A Internet é uma rede de computadores que interconecta milhares de dispositivos computacionais ao redor do mundo. Há pouco tempo, esses dispositivos eram basicamente computadores de mesa, estações de trabalho, Linux, e os assim chamados servidores que armazenam e transmitem informações, como página da Web e mensagens de e-mail. No Entanto, cada vez mais sistemas finais modernos da Internet, como TVs, laptops, consoles para jogos, telefones celulares, webcams, automóveis, dispositivos de sensoriamento ambiental, quadros de imagens, e sistemas internos elétricos e de segurança, estão sendo conectados.

De acordo com informações do Instituto Brasileiro de Geografia e Estatística (IBGE, 2022), a Internet estava presente em 91,5% dos domicílios do país em 2022. Um aumento de 1,5 ponto percentual em relação a 2021. Assim, em 2021, no Brasil, dos 183,9 milhões de pessoas com 10 anos de idade ou mais, 84,7% (ou 155,7 milhões) utilizaram a Internet durante o período de referência dos últimos três meses do ano. Já em 2022, entre os 68,9 milhões de domicílios com acesso à Internet, 14,3 % (ou 9,9 milhões) possuíam algum tipo de dispositivo

inteligente conectado à rede, tais como câmeras, caixas de som, lâmpadas, ar-condicionado, geladeiras, entre outros (IBGE, 2022).

Segundo Castells (2009, p. 84), a Internet, em sua ampla gama de aplicações, é o tecido da comunicação de nossas vidas, seja para o trabalho, conexões pessoais, redes sociais, informações, entretenimento, serviços públicos, política e religião.

Além disso, a Internet é considerada uma das tecnologias mais importantes, impactantes e revolucionárias das últimas décadas. De acordo com Castells (2003, p. 7), a Internet passou a ser a base tecnológica para a forma organizacional da Era da Informação. Ela modificou, viabilizou e criou ferramentas para o acesso à informação, a comunicação global, o comércio eletrônico, as Redes Sociais e interações *online*, o trabalho e a colaboração, a educação *online*, a inovação e o empreendedorismo.

A importância da Internet vai além do entretenimento e da saúde. Ela é essencial para o desenvolvimento, difusão e implementação de tecnologias emergentes, como Inteligência Artificial, Internet das Coisas, *blockchain* e Realidade Virtual e Realidade Aumentada. A Internet serve como um meio para que empresas e indivíduos compartilhem informações, colaborem em projetos conjuntos e acessem recursos e serviços de qualquer lugar do mundo, promovendo a globalização da economia e das ideias.

A democratização do acesso à tecnologia também é um aspecto fundamental da Internet. Ela desempenha um papel significativo no desenvolvimento e distribuição de novos *softwares,* aplicativos, jogos e outros produtos digitais, possibilitando um acesso rápido e eficiente, mesmo em regiões remotas ou em países onde o acesso ao conhecimento seja precário.

Além disso, a Internet é uma peça-chave na disseminação e no avanço de tecnologias revolucionárias, como a Internet das Coisas e a Inteligência Artificial. Para a Internet das Coisas, em particular, a Internet é imprescindível, pois é por meio dela que os dispositivos se comunicam entre si e enviam dados para análise e processamento, possibilitando uma ampla gama de aplicações que têm o potencial de transformar ainda mais o mundo em que vivemos. Nesse sentido, leciona Guilherme Mucelin (2020, p. RB. 18-2):

> Assim é que a rede, anteriormente limitada a uma tela de computador, se espalhou pelos écrans de *Smartphones* e *tablets* para, hoje, se tornar onipresente – podemos observar essa transformação nos modos como as pessoas se comunicam (aplicativos de mensagens instantâneas, *e-mails*), interagem e se expressam (redes sociais), se relacionam afetivamente (aplicativos e *sites* de relacionamentos), habitam (*Smart houses*), têm lazer (jogos, passatempos, filmes, músicas *online* e *streaming*), buscam informações (buscadores *online*, *e-books*), exercem a cidadania (biometria, reconhecimento facial), contratam serviços e adquirem produtos (comércio eletrônico, economia do compartilhamento *online*, Internet das Coisas), se locomovem (geolocalização), se vestem (*wearables*) e trabalham (trabalho *on-demand,*

> teletrabalho); até mesmo os *pets* já têm sensores e *chips* – e isso muda a forma que os dados são coletados.

Em 2021, no Brasil, dos indivíduos que a acessavam, o faziam principalmente por intermédio de celulares (99,5% o utilizaram para navegar na Internet). Em seguida, a televisão foi utilizada por 44,44% das pessoas, seguida pelo computador, com uma taxa de utilização de 44,2% (IBGE, 2021), confirmando os ensinamentos de Kurose e Ross (2009, p. 8), de que até recentemente apenas computadores de mesa e servidores de grande capacidade estavam conectados à Internet. No entanto, desde a década de 1990 até os dias atuais, uma variedade crescente de dispositivos passou a ser conectada à rede. Esses dispositivos são caracterizados pela capacidade de enviar e receber dados entre si. Devido à onipresença, disponibilidade e padronização da Internet, a interconexão desses dispositivos tornou-se uma evolução natural.

Contudo, de acordo com Kurose e Ross (2009), alguns dispositivos que se conectam à Internet parecem ter sido criados exclusivamente para diversão, enquanto outros fornecem informações úteis. Por exemplo, os tênis podem enviar dados e a contagem de passos pode ser visualizada em outros dispositivos conectados à Internet, como *Smartphones*. Todas as métricas coletadas pelos sapatos podem ser analisadas, por exemplo, para verificar quantas calorias foram queimadas, possibilitando a oferta de aconselhamento personalizado sobre fitness. *Smartphones* permitem fácil navegação pela Web e transmissão de e-mails e mensagens. Uma *tag* de *RFID*[6] ou um sensor integrado ligado a qualquer objeto pode fornecer informações sobre esse objeto na Internet, o que leva ao conceito de "Internet das Coisas", o que se trata a seguir.

1.2 INTERNET DAS COISAS COMO UMA TECNOLOGIA EMERGENTE NA QUARTA REVOLUÇÃO INDUSTRIAL: CONCEITOS, CARACTERÍSTICAS E FUNCIONAMENTO

O termo Internet das Coisas, do inglês *Internet of Things - IoT*, refere-se a uma rede de dispositivos físicos que estão conectados à Internet e podem coletar e trocar dados entre si sem a necessidade de intervenção humana direta. Nas palavras de Brasileiro (2022), a Internet das Coisas, assim como a robótica, a Inteligência Artificial, a Nanotecnologia, a Computação

[6] *RFID* é a sigla em inglês que é definida por *Radio-Frequency Identification* — ou identificação por radiofrequência. É uma tecnologia pela qual os dados digitais codificados em etiquetas *RFID* e antenas são capturados por um leitor por meio de ondas de rádio (Alecrim; Marques, 2023).

Quântica, a Biotecnologia, a impressão 3D e os carros autônomos, marcam a Quarta Revolução Industrial.

Conforme ensinamento de Barcelos (2019, p. 78), a expressão “Internet das Coisas” foi empregada pela primeira vez por Kevin Ashton em uma apresentação sobre a utilização de etiquetas de radiofrequência (*RFID*), da expressão em inglês *Radio-Frequency IDentification*. O propósito de Ashton era persuadir os dirigentes empresariais de que, adotando um dispositivo que enviasse informações detalhadas sobre o estoque e o monitorasse, seria possível criar uma dimensão na comunicação em rede, caracterizada pela precisão, atualização quase em tempo real e custos operacionais reduzidos. Além disso, essa abordagem eliminaria grande parte da intervenção humana, transferindo a gestão de inventário para objetos inteligentes capazes de se comunicar entre si. Conforme Ashton (2009, p. 1):

> Se tivéssemos computadores que soubessem de tudo o que há para saber sobre as coisas, usando dados que foram colhidos, sem qualquer interação humana, seríamos capazes de monitorar e mensurar tudo, reduzindo o desperdício, as perdas e o custo. Gostaríamos de saber quando as coisas precisarão de substituição, reparação ou atualização, e se elas estão na vanguarda ou se tornaram obsoletas.

A *IoT* surgiu em decorrência dos avanços nas tecnologias de miniaturização de componentes eletrônicos e nas tecnologias de comunicação sem fio (Maschietto *et al.*, 2021). O acesso à tecnologia de sensores de baixo custo e baixo consumo de energia, juntamente com protocolos de rede e novas plataformas de Computação em Nuvem, também desempenhou um papel significativo no rápido crescimento da *IoT*. Ela representa uma evolução natural da Internet, na qual a conectividade não se restringe apenas a computadores, *Smartphones* e *tablets*, mas se estende a todos os objetos que estão equipados com sensores e capacidade de comunicação.

A Internet das Coisas transcende a simples conexão de dispositivos, como geladeiras conectadas, e abrange a automatização gradual de setores inteiros da economia e da vida social por meio da comunicação máquina-máquina. Isso inclui áreas como logística, agricultura, transporte de pessoas, saúde, produção industrial e muitos outros. Para isso, é necessário um ambiente favorável ao acesso de um número cada vez maior de dispositivos (Martinhão *apud* Magrani, 2018, p. 15).

Nota-se que o número de objetos conectados à Internet, por meios de cabos ou conexões sem fio, aumentou significativamente: na sétima edição do *IoT Business* Fórum 2023, nos dias 25 e 27 de abril de 2023, Renato Pasquini (consultor e pesquisador no setor de tecnologias da informação e comunicação – vice-presidente de pesquisa da *Frost & Sullivan*) apresentou os

resultados de uma pesquisa de campo realizada em 2022, com cerca de 600 empresas. O estudo previa que, até o final de 2023, cerca de 41,0 bilhões de dispositivos ativos estariam conectados à *IoT* globalmente. Um aumento de 18% nas conexões em relação ao ano de 2022 (Assessoria de Imprensa, 2023).

A relevância deste setor também é destacada na primeira parte do relatório divulgado em 11 de abril de 2024 pela Associação Brasileira das Empresas de Software (ABES), em parceria com a *International Data Corporation (IDC)*, intitulado "Estudo Mercado Brasileiro de Software – Panorama e Tendências 2024". O relatório prevê que, em 2024, o mercado brasileiro de *IoT* atingirá US$ 1,7 bilhão em hardware, software, serviços e conectividade, indicando um crescimento expressivo no setor (Lauterjung, 2024).

De acordo com o relatório, essa expansão da *IoT* é evidenciada pelos investimentos e pela adoção crescente de tecnologias *IoT* por diversas entidades. Estima-se que, em 2024, 50% das empresas estarão nas fases de planejamento ou execução de provas de conceito para projetos de Internet das Coisas. Aproximadamente 34% das Pequenas e Médias Empresas brasileiras planejam adotar soluções de *IoT* nos próximos dois anos, enquanto, no setor governamental, esse percentual aumenta para 50% (ABES; IDC; 2024).

Em relação a conceitos e definições da Internet das Coisas, é importante destacar que existem diversas interpretações e definições para esse termo. Nas palavras de Eduardo Magrani (2018, p. 20), a definição para a Internet das Coisas é:

> A *IoT* pode ser entendida como um ambiente de objetos físicos interconectados com a Internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua) voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia.

Adicionalmente, Morais *et al.* (2018, p. 18) contribuem para a compreensão do conceito, acrescentando que:

> O conceito de *IoT* é baseado na ideia de fusão do mundo real com o mundo digital, fazendo com que os indivíduos estejam em constante comunicação e interação com outras pessoas e objetos. A *IoT* possui funções de reconhecimento inteligente, localização, rastreamento e gerenciamento dos diversos dispositivos, trocando informações a todo o momento.

Alves *et al.* (2021, p. 100) também contribuem com a seguinte perspectiva: "A Internet das Coisas pode ser considerada um ecossistema cyber-físico de sensores e recursos interconectados, que permitem a tomada de decisões inteligentes". Por sua vez, de acordo com

Maschietto *et al.* (2021), a *IoT* "pode ser entendida como uma infraestrutura global voltada para a Era Digital, promovendo serviços avançados por meio da interconexão das coisas".

Além dessas definições, o Decreto Federal nº 9.854, de 2019, que instituiu o Plano Nacional de Internet das Coisas e dispôs sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas, define esta como "A Infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade" (Brasil, 2019).

Das citações supra apontadas é possível notar que, em todas as definições de Internet das Coisas, temos objetos e sensores conectados que interagem entre si e processam dados, ou seja, há três elementos fundamentais: conectividade, uso de sensores e capacidade computacional de processamento e armazenamento. Essas múltiplas definições refletem a complexidade e a amplitude da Internet das Coisas, enfatizando a interconectividade, a fusão entre o mundo físico e digital, a tomada de decisões inteligentes e sua importância nas esferas tecnológica e social.

De acordo com Morais *et al.* (2018, p 18), a *IoT* tem como base a Internet e conecta o mundo físico com o mundo digital. É um sistema em que objetos comuns, equipamentos e dispositivos eletrônicos equipados com sensores são conectados à Internet, fazendo com que os indivíduos estejam em constante comunicação e interação com outras pessoas e objetos, sem a necessidade de intervenção humana.

Essas aplicações são fundamentadas na capacidade de coleta e processamento de dados, os quais têm se tornado gradualmente mais refinados, onipresentes e volumosos, permitindo aumentar a eficiência em áreas como serviços de cidades inteligentes, segurança pública, saúde e sistemas de gerenciamento predial (Belli, 2023, p. 401).

Nesse sentido, Maschietto *et al. (*2021, p. 17) complementam que as aplicações de *IoT* englobam diversas áreas, como o planejamento urbano, o setor agrícola, a logística, a produção industrial, o transporte de pessoas, a saúde e a conservação do meio ambiente, entre outras. A coleta e a análise dos dados gerados pelos dispositivos conectados são essenciais para identificar padrões, melhorar a eficiência e desenvolver novos serviços e experiências para os usuários. O diferencial proporcionado pelas tecnologias ao tratamento de dados pessoais consiste nos perfis quantitativos e qualitativos, fundamentados na capacidade de processar grandes volumes de dados em menos tempo e na aplicação de métodos, algoritmos e técnicas

sofisticadas nesse processamento, com o objetivo de obter resultados mais valiosos (Doneda 2021, p. RB-2.5 - RB-2.6).

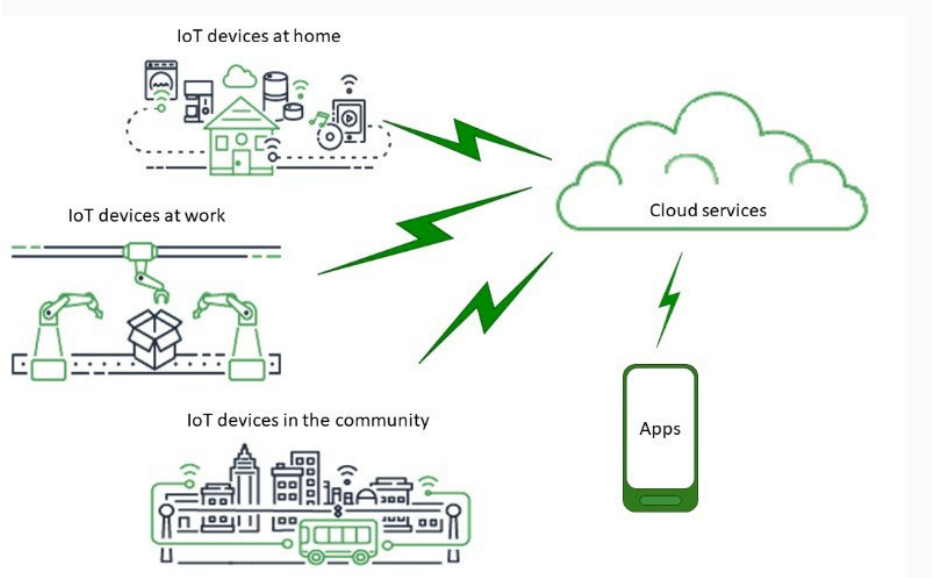
Assim, diante do potencial da Internet das Coisas, o seu desenvolvimento é acompanhado com grande atenção tanto pelo setor privado quanto pelo setor público. Este último tem o objetivo de facilitar negócios e atrair investimentos, enquanto tenta prevenir e mitigar os riscos de privacidade e segurança aos quais os sistemas de *IoT* são expostos (Belli, 2023, p. 401).

Nesse cenário, buscando desenvolver a Internet das Coisas no país, o Banco Nacional de Desenvolvimento Econômico e Social (BNDES), em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), apoiaram a realização de um estudo para diagnóstico e proposição de um plano de ação para a Internet das Coisas (BNDES, 2017). Esse projeto resultou no Plano Nacional de Internet das Coisas, instituído pelo Decreto nº 9.854, de 25 de junho de 2019.

Entre os objetivos do plano estão: melhorar a qualidade de vida das pessoas, promover ganhos de eficiência nos serviços, promover capacitação profissional, incrementar a produtividade e fomentar a competitividade das empresas brasileiras no contexto da Internet das Coisas (Brasil, 2019).

Seus fundamentos incluem a promoção da livre concorrência e a livre circulação de dados, seguindo as diretrizes de segurança da informação e proteção de dados pessoais. Além disso, o Decreto nº 9.854/2019 cria a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas, responsável por monitorar a implementação do Plano, fomentar parcerias e propor projetos. O Decreto também define as diretrizes para parcerias, desenvolvimento de tecnologias, infraestrutura e regulamentação do setor de *IoT* no Brasil (Brasil, 2019).

Figura 1 – Funcionamento básico *IoT*: dispositivos – conectividade – aplicação



Fonte: O que é a Internet (2023).

Três elementos fundamentais caracterizam uma plataforma *IoT*: coisas equipadas com sensores e atuadores, um ambiente de conectividade e aplicações. As coisas a serem conectadas possuem um ou mais sensores que farão o monitoramento ou a medição de uma ou mais condições específicas. Os dados coletados poderão ser analisados ou não localmente e serão compartilhados, em tempo real ou não, com um ambiente remoto, para que as aplicações os transformem em informações e executem as ações necessárias (Souza Junior, 2021).

Nas palavras de Souza Junior (2021), essas "Coisas", sejam elas seres vivos ou objetos físicos, estão relacionadas a qualquer entidade que requeira monitoramento ou medição de dados. Isso pode incluir, por exemplo, uma turbina de avião, um relógio inteligente, robôs, medidores de serviços públicos, equipamentos médicos, motores de automóveis, lâmpadas inteligentes e organismos vivos, como plantas, animais e seres humanos.

Na Internet das Coisas, os sensores desempenham um papel fundamental. Eles podem ser definidos como "dispositivos ou equipamentos sensíveis a estímulos magnéticos, motores, de calor, de luz, de pressão, som entre outros e são capazes de converter essa energia e transmitir um impulso correspondente" (Michaelis, 2023). Os sensores estão presentes em dispositivos *IoT*, coletando dados do ambiente ou do usuário, como temperatura, umidade, pressão, localização geográfica e movimento. São responsáveis por produzir informações básicas e específicas na rede *IoT*, havendo sensores que podem colaborar com outros sensores para produzir informações e outros que estão integrados a *tags RFID* (Maschietto *et al.*, 2021, p. 34).

A conectividade em *IoT* desempenha um papel fundamental na eficácia e no funcionamento de sistemas. Conforme ensinamentos de Ideali (2021, p. 18), a conectividade refere-se à habilidade de interligar, de maneira adequada, *hosts,* computadores, máquinas e outros dispositivos eletrônicos, permitindo a troca de dados e informações entre si. Pode ainda ser entendida como o conjunto de infraestruturas, físicas e de *software*, que garantem a interação em rede, entre dispositivos e informações digitais. É a capacidade de conectar dispositivos, sistemas, ambientes e dados, garantindo não só o acesso, mas o compartilhamento em tempo real de dados, em vários locais e por diversos usuários (Ascenty, 2024).

Nas palavras de Matthieu (2017), existem dezenas, se não centenas, de protocolos públicos para utilização em dispositivos inteligentes, sem mencionar que muitos deles realmente usam seus próprios protocolos proprietários. É preciso ter em mente que cada um desses protocolos tem aspectos negativos e positivos; alguns protocolos são melhores para baterias limitadas ou processadores limitados, ou largura de banda limitada. Outros protocolos são melhores em comunicações de longo alcance, mas consomem mais energia.

A escolha e uso do protocolo dependerá dos requisitos do projeto, como alcance da comunicação, consumo de energia, largura de banda necessária e ambiente de implantação. Assim, é importante selecionar a tecnologia adequada para garantir uma conexão confiável e eficiente entre os dispositivos *IoT* e os sistemas.

Na próxima seção, serão apresentadas as principiais características da tecnologia *Big Data*, bem como sua integração com a Internet das Coisas, a Inteligência Artificial e a Computação em Nuvem.

1.3 INTERNET DAS COISAS, COMPUTAÇÃO EM NUVEM, *BIG DATA* E INTELIGÊNCIA ARTIFICIAL

A ascensão da Internet das Coisas na Era Digital tem impulsionado um aumento significativo no volume de dados provenientes de dispositivos conectados. Contudo, conforme mencionado por Clive Humby (*apud* Belli, 2023, p. 394), “Os dados são como óleo bruto: são valiosos, mas, se não refinados, não podem realmente ser usados”, ressaltando a importância do tratamento dos dados coletados.

Nesse contexto, a tecnologia *Big Data* desempenha um papel importante na capacidade de processamento e análise desses dados, ao passo que a Computação em Nuvem oferece a infraestrutura necessária para armazenar, gerenciar e processar esses grandes conjuntos de dados da *IoT*, permitindo que sejam extraídas informações valiosas e relevantes para uma

variedade de aplicações e setores. Nesse sentido, ensinam Newton De Lucca e Guilherme M. Martins (2022, p. 19): “Informações de todo tipo podem ser associadas de tal forma a determinar um conteúdo de relevância à soberania estatal, à dignidade da pessoa humana, por exemplo prevenir doenças, a pornografia infantil ou atos de terrorismo e racismo”.

Salienta-se que os sistemas de Big Data normalmente são integrados a tecnologias de Inteligência Artificial e Aprendizado de Máquina (Taurion, 2013, p. 41), que possuem a capacidade de aprender com conjuntos de dados, identificar padrões, prever resultados futuros, realizar inferências ou tomar decisões com base nesses padrões, além de serem menos dependentes da intervenção humana. A Inteligência Artificial dedica-se a realizar tarefas que normalmente exigiriam inteligência humana (Cardoso, 2024).

Nas palavras de Davenport (2014, p. 1) a tecnologia *Big Data* pode ser conceituada como:

> *Big Data* é um termo genérico para dados que não podem ser contidos nos repositórios usuais; refere-se a dados volumosos demais para caber em um único servidor; não estruturados demais para se adequar a um banco de dados organizado em linhas e colunas; ou fluidos demais para serem armazenados em um data Warehouse estático. Embora o termo enfatize seu tamanho, o aspecto mais complicado do *Big Data*, na verdade, envolve sua falta de estrutura.

Da mesma forma, Taurion (2013, p. 20) ensina:

> *Big Data* não trata apenas da dimensão volume, como parece à primeira vista, mas existe também uma variedade imensa de dados, não estruturados, dentro e fora das empresas (coletados das mídias sociais, por exemplo), que precisam ser validados (terem veracidade para serem usados) e tratados em velocidade adequada para terem valor para o negócio. A fórmula é então, *Big Data* = volume + variedade + velocidade + veracidade, gerando valor.

A tecnologia *Big Data* foi caracterizada inicialmente por três aspectos principais conhecidos como as “três V’s”: volume, variedade e velocidade. Nesse contexto, Basso (2020, p. 16) ensina: o Volume é caracterizado pela enorme quantidade de dados criados e coletados pela Internet das Coisas, sejam eles estruturados ou não estruturados. A Variedade diz respeito à diversidade dos tipos de dados coletados, incluindo texto, áudio, imagens, vídeo, redes sociais e dados de sensores. A Velocidade refere-se à rapidez com que esses dados são gerados e transmitidos, o que acontece em tempo real ou quase em tempo real.

Com o avanço da tecnologia, contudo, o *Big Data* passou a ter um conceito mais amplo, baseado em 5 Vs (velocidade, volume, variedade, veracidade e valor) (Basso, 2020, p. 17). A **velocidade** dos dados na era da Internet das Coisas está diretamente ligada à rapidez com que

são gerados, produzidos e acessados. Com o crescimento exponencial dos dados, a análise em tempo real do *Big Data* torna-se crucial, pois as informações podem se tornar obsoletas rapidamente. Estimativas indicam que a velocidade continuará a aumentar à medida que a utilização da *IoT* se expandir. Quanto ao **volume**, cada indivíduo produz uma quantidade significativa de informações em suas atividades diárias, abrangendo preferências, localização, deslocamentos, interesses, compras, negócios, entre outros. Estima-se que o volume de informações dobre a cada 18 meses, representando um desafio para o *Big Data* em termos de armazenamento e processamento. A **variedade** de dados refere-se à diversidade de formatos e tipos, como texto, vídeo, áudio, imagens, publicações em mídias sociais e navegação na Internet. O *Big Data* enfrenta o desafio de lidar, simultaneamente, com dados estruturados, semiestruturados e não estruturados, provenientes de várias fontes e dispositivos conectados (Basso, 2020, p. 17).

Complementa Basso (2020, p. 17) que a **veracidade** dos dados é fundamental, exigindo autenticidade e segurança das fontes de coleta. Nem todas as informações postadas em mídias sociais ou outros sistemas são verdadeiras, o que pode resultar em dados incorretos e falta de confiabilidade. Já o **valor** dos dados é um aspecto relevante no *Big Data*. Embora as informações possam ter grande importância, nem sempre estão alinhadas aos objetivos das organizações, destacando a necessidade de identificar quais dados são realmente valiosos para gerar informações e tomar decisões estratégicas.

Tais atributos são sintetizados por Taurion (2013, p. 37) da seguinte forma:

> Volume está claro. Geramos *petabytes* de dados a cada dia. E estima-se que este volume dobre a cada dezoito meses. Variedade também, pois estes dados vêm de sistemas estruturados (hoje já são minoria) e não estruturados (a imensa maioria), gerados por e-mails, mídias sociais (Facebook, Twitter, YouTube e outros), documentos eletrônicos, apresentações estilo Powerpoint, mensagens instantâneas, sensores, etiquetas *RFID*, câmeras de vídeo etc. A variedade é um parâmetro importante pois, com diversas fontes de dados aparentemente sem relações, podemos derivar informações extremamente importantes e fazer análises preditivas mais eficientes. Por exemplo, conectando dados meteorológicos com padrões de compra dos clientes podemos planejar que tipos de produtos deverão estar em destaque nas lojas quando for detectado que haverá um período de alguns dias de temperatura elevada, daqui a três dias. Ou conectar dados geográficos com detecção de fraudes. Velocidade porque muitas vezes precisamos agir praticamente em tempo real sobre este imenso volume de dados, como em um controle automático de tráfego nas ruas. Veracidade porque precisamos ter certeza de que os dados fazem sentido e são autênticos. E valor porque é absolutamente necessário que a organização que implemente projetos de *Big Data* obtenha retorno destes investimentos.

As características supramencionadas representam um desafio para as capacidades de armazenamento, processamento e análise tradicionais, destacando a Computação em Nuvem

como uma solução viável. A integração da Computação em Nuvem com o *Big Data* representa uma sinergia eficaz. O *Big Data* requer capacidade contínua de armazenamento e processamento de informações, e a infraestrutura de Computação em Nuvem oferece acesso a recursos tecnológicos de alto desempenho, que podem ser dimensionados com facilidade e gerenciados com segurança. Essa combinação resulta em uma solução de elevada eficiência, conforme lecionam Jackson e Goessling (2018, p. 1):

> A Computação em Nuvem é um modelo para permitir o acesso de rede onipresente, conveniente e sob demanda a um conjunto compartilhado de recursos de computação configuráveis (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) que podem ser rapidamente provisionados e liberados com o mínimo de gerenciamento esforço ou interação do prestador de serviços." – Instituto Nacional de Padrões e Tecnologia dos EUA.

Nas palavras de Rountree e Castrillo (2014), a definição de Computação em Nuvem do *National Institute of Standards and Technology (NIST*)[7] apresenta cinco características principais: o autoatendimento sob demanda permite que os usuários acessem e provisionem recursos de forma autônoma; o amplo acesso à rede garante que os serviços sejam acessíveis de qualquer lugar; o agrupamento de recursos permite o compartilhamento eficiente de recursos entre usuários; a elasticidade rápida permite aumentar ou reduzir os recursos conforme a demanda e, por fim, o serviço medido permite que os usuários sejam cobrados com base no uso real dos recursos.

A Computação em Nuvem ainda traz benefícios como: agilidade, confiabilidade, escalabilidade, redução de custos, acesso remoto, *backup* automatizado, atualizações de *software* simplificadas, desempenho, economia de escala, eficiência energética, facilidade de manutenção, maior flexibilidade, integração simplificada, recursos compartilhados, segurança, recuperação de desastres e implementação rápida de novas aplicações e serviços (Carreira, 2022; Microsoft, 2023).

A Computação em Nuvem oferece recursos escaláveis, flexíveis e acessíveis para lidar com as demandas do *Big Data* proveniente da *IoT*. Por meio da nuvem, é possível armazenar grandes volumes de dados em servidores remotos, reduzindo a necessidade de infraestrutura local. Além disso, a Computação em Nuvem fornece recursos de processamento paralelo e distribuído, permitindo que o *Big Data* seja processado de forma eficiente e rápida. Dessa forma, possibilita a execução de algoritmos complexos de análise de dados e aprendizado de

[7] O *National Institute of Standards and Technology* (*NIST)* é uma agência não reguladora que promove a inovação por meio do avanço da ciência, padrões e tecnologia de medição (O que é o NIST..., 2023).

máquina, bem como a geração de informações acionáveis para melhorar a tomada de decisões e impulsionar a inovação.

A combinação do *Big Data* e da Computação em Nuvem na Internet das Coisas oferece várias vantagens significativas. Primeiro, essa combinação permite o armazenamento e processamento eficiente de grandes volumes de dados gerados pela *IoT*, reduzindo a necessidade de investimentos em infraestrutura local onerosa. A capacidade da Computação em Nuvem de se adaptar às necessidades do sistema, aumentando vertical e horizontalmente, possibilita que as empresas se ajustem facilmente ao crescimento da *IoT* e às variações nas demandas de dados. Esta característica é conhecida como autoatendimento sob demanda (Sousa Neto, 2015, p. 43).

Outra vantagem é que a Computação em Nuvem proporciona escalabilidade e flexibilidade, permitindo que as organizações acompanhem o aumento contínuo do número de dispositivos *IoT* conectados e a explosão de dados gerados por eles. Essa capacidade de dimensionar os recursos computacionais conforme necessário é fundamental para lidar com os desafios de gerenciamento e análise de dados em constante crescimento (Sousa Neto, 2015, p. 43). Um exemplo prático que ilustra a importância da Computação em Nuvem é a migração da principal plataforma jurisdicional do Tribunal de Justiça do Rio Grande do Sul para um sistema de Computação em Nuvem. A transferência de 200 *terabytes* de dados proporcionará não apenas a modernização do funcionamento da Justiça Estadual, mas também lhe garantirá maior segurança, acessibilidade e infraestrutura (Rio Grande do Sul, 2024).

A terceira vantagem é que a análise de *Big Data* realizada na nuvem possibilita a descoberta de informações valiosas a partir dos dados da *IoT*. Ao empregar técnicas avançadas de análise de dados, como aprendizado de máquina e mineração de dados, a Computação em Nuvem provida de Inteligência Artificial pode identificar padrões, correlações e tendências nos dados da *IoT*. Essas informações podem impulsionar a inovação, melhorar os processos operacionais e apoiar a tomada de decisões estratégicas em diversos setores, como saúde, manufatura, transporte e energia.

Em síntese, a Internet das Coisas é responsável por gerar vastos volumes de dados a partir dos dispositivos interconectados. O *Big Data* e a Computação em Nuvem oferecem as ferramentas e estruturas necessárias para a coleta, o armazenamento e o processamento desses dados em larga escala. Por sua vez, a Inteligência Artificial analisa esses dados, identificando padrões, realizando previsões sobre os mais variados assuntos, inclusive em relação aos comportamentos individuais, e tomando decisões inteligentes em tempo real.

Conforme ensinamentos de Mendes, Mattiuzzo e Fujimoto (2023, p. 425), “A função mais importante de *Big Data* é elaborar previsões baseadas em um grande número de dados e informações: desde desastres climáticos até crises econômicas, do surto de uma epidemia até o vencedor de um campeonato de esportes”.

Assim, em conjunto, a IA, a *IoT*, o *Big Data* e a Computação em Nuvem formam um ecossistema robusto que impulsiona a automação inteligente, a otimização de processos e a criação de novos modelos de negócios.

Na seção seguinte, são apresentadas, de forma sucinta, algumas das principais aplicações e alguns dos benefícios da Internet das Coisas, destacando-se as inovações tecnológicas que têm impulsionado seu crescimento e impacto em diversos setores.

1.4 INTERNET DAS COISAS: APLICAÇÕES E BENEFÍCIOS

Nesta seção, são apresentados os impactos da Internet das Coisas em diferentes áreas: Casa Inteligente, Medicina, Cidades Inteligentes e *IoT* Industrial. Estão em destaque as inovações tecnológicas e os benefícios para os usuários, fornecendo uma visão abrangente das transformações proporcionadas pela *IoT*.

Destacam-se também os benefícios proporcionados pela Internet das Coisas à sociedade em geral, que abrangem não apenas o ambiente doméstico ou individual, mas também o ambiente empresarial, comercial, de serviços, industrial e governamental.

Conforme se demonstra, a *IoT* possibilita uma maior eficiência operacional, redução de custos, melhoria na qualidade de vida das pessoas e dos serviços, além de promover maior segurança em diversas áreas e uma integração mais inteligente e eficaz entre diferentes setores da sociedade.

1.4.1 Internet das Coisas na Casa Inteligente

Uma casa inteligente, também conhecida como “*Smart home*”, é uma residência equipada com dispositivos e sistemas que utilizam Internet das Coisas para melhorar a qualidade de vida e a eficiência dos moradores. Esses dispositivos estão conectados à Internet e podem ser controlados remotamente por meio de *Smartphones*, *tablets* ou outros dispositivos eletrônicos.

Com a *IoT* residencial, é possível criar ambientes personalizados conforme as preferências dos moradores. Através do controle de dispositivos conectados, é possível ajustar

a temperatura, a iluminação, a música e outros aspectos do ambiente, segundo as preferências individuais, criando um ambiente mais confortável e agradável. Nesse sentido, ensinam Takashi e Moraes (2021, p. 163) que as experiências dos sistemas de *IoT* para multimídia em casa conectada estão cada vez mais integrando os mundos virtual e real. De maneira confortável, a *IoT* permite a interação com o sistema multimídia através de linguagem natural, possibilitando o acionamento de músicas, filmes ou podcasts no ambiente da casa conectada, onde o contexto ambiental já está bem estabelecido, com realidades imersivas, efeitos de localização e interações 3D progressivamente mais realistas.

A Internet das Coisas também possibilita o monitoramento e controle em tempo real do consumo de energia, água, gás e outros recursos. Além disso, permite ajustar o uso de energia, identificar vazamentos, desligar dispositivos ociosos e otimizar a eficiência dos sistemas de aquecimento, ventilação e ar-condicionado. Essa integração de dispositivos inteligentes permite a conservação de recursos naturais e a redução do desperdício, resultando na contenção de custos (Silva, 2021, p. 12).

Os sistemas de segurança residencial baseados em *IoT* permitem monitorar e controlar remotamente a segurança da casa. Dispositivos como fechaduras, câmeras de segurança e detectores de vazamentos podem usar *machine learning* para detectar ameaças, tomar medidas e enviar alerta para proprietários das residências, tudo isso de forma automática. Por exemplo, é possível receber notificações em tempo real sobre atividades suspeitas, visualizar câmeras de segurança e controlar travas de portas remotamente, o que aumenta a tranquilidade dos moradores e contribui para a segurança da residência (Amazon, 2023).

A *IoT* residencial pode incluir dispositivos de monitoramento de saúde, como sensores de frequência cardíaca, sensores de sono e dispositivos de assistência médica conectados. Tais tecnologias permitem que os moradores monitorem sua saúde e bem-estar, recebam avisos sobre suas condições médicas e melhorem sua qualidade de vida.

1.4.2 Internet das Coisas na Medicina

A integração de dispositivos médicos e sistemas conectados oferece uma série de benefícios e possibilidades. A *IoT* permite o monitoramento remoto de pacientes, especialmente aqueles com condições crônicas ou em recuperação. Dispositivos conectados, como sensores vestíveis, podem coletar dados vitais em tempo real, como frequência cardíaca, pressão arterial, níveis de glicose e atividade física, o que permite o monitoramento contínuo da saúde, ajudando na adoção de abordagens preventivas e personalizadas. Com base nos dados coletados, os

profissionais de saúde podem identificar padrões, prever riscos de saúde e fornecer intervenções. A *IoT* também possibilita a criação de casas de cuidados inteligentes equipadas com sensores e dispositivos conectados. Esses sistemas podem monitorar a saúde e o bem-estar dos residentes, detectar quedas, controlar a temperatura ambiente, ajudar na administração de medicamentos e fornecer alertas e lembretes personalizados.

Nesse sentido, lecionam Telles e Kolbe Junior (2022, p. 122) que a assistência médica inteligente consiste em uma abordagem proativa de detecção precoce e prevenção de doenças. Ela permite a prestação de serviços médicos nas residências dos pacientes, que podem ser monitorados continuamente por meio de diversos dispositivos conectados à Internet. Isso reduz a necessidade de internações e os custos com saúde, além de promover o bem-estar dos pacientes.

O InCor (Instituto do Coração do Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo – HCFMUSP) lançou uma plataforma de telemedicina que visa a orientação de cirurgias de alta complexidade. O Telemonitoramento do Ato Cirúrgico (TAC), desenvolvido pelo Núcleo de Inovação do InCor (InovaInCor), utiliza tecnologias de colaboração interativa, videoconferência, óculos inteligentes e Internet das Coisas.

Como resultado da aplicação da *IoT*, destaca-se a intervenção cirúrgica realizada em maio de 2023:

> Médicos operam coração de criança a 3 mil quilômetros de distância. Helena, de 4 anos, nasceu com cardiopatia congênita e teve coração renovado em projeto pioneiro do Hospital Universitário (SP) e Instituto do Coração. Os pais, preocupados com os custos e o estresse de deslocamento até o Sudeste, ficaram aliviados quando souberam que participariam do projeto pioneiro do Hospital Universitário e Instituto do Coração para realizar cirurgias à distância. O procedimento foi realizado com os médicos de São Paulo acompanhando imagens, sons e dados de Helena, junto a médicos em São Luís. A criança teve o coração renovado na cirurgia de sucesso (Fantástico, 2023).

Por meio da *IoT*, é possível conectar e comunicar equipes médicas que estejam distantes, viabilizando a troca de informações, experiências e orientações antes, durante e após cirurgias de casos complexos. Além disso, torna viável o diagnóstico remoto e o monitoramento de pacientes anestesiados durante esse período crítico (SAP, 2023). Essas aplicações resultam em redução de custos, otimização de recursos e aprimoramento no tratamento e cuidado das pessoas, proporcionando-lhes maior dignidade.

Assim, a Internet das Coisas tem desempenhado um papel importante na transformação da assistência médica. A capacidade de conectar dispositivos médicos e sistemas de saúde tem possibilitado o monitoramento remoto de pacientes, diagnósticos precisos e intervenções

proativas e à distância, melhorando a qualidade de vida e reduzindo os custos do setor de saúde (Telemedicina..., 2023).

1.4.3 Internet das Coisas e as Cidades Inteligentes

Em cidades inteligentes, a *IoT* desempenha importante papel na coleta e análise de dados em tempo real para gerenciar eficientemente recursos e serviços urbanos. Sensores e dispositivos conectados são instalados em infraestrutura urbana, como iluminação pública, semáforos, redes de água e esgoto, e sistemas de transporte. Esses dispositivos monitoram continuamente o ambiente, detectam problemas e enviam dados para sistemas centralizados de gestão que podem tomar decisões informadas e automatizadas. A integração da Internet das Coisas em cidades inteligentes proporciona uma abordagem inovadora e eficiente para enfrentar os desafios urbanos contemporâneos. Ao utilizar dados em tempo real e automação avançada, as cidades inteligentes conseguem oferecer melhores serviços públicos, melhorar a qualidade de vida dos cidadãos e promover um desenvolvimento urbano sustentável e resiliente.

Conforme ensinamentos de Silva (2021, p. 33):

> As cidades inteligentes envolvem principalmente os seguintes pontos: inovação, pessoas, tecnologias, mobilidade, meio ambiente, segurança, educação, economia e saúde. O foco das cidades inteligentes é o desenvolvimento sustentável e qualidade de vida para o cidadão, uma vez que é preciso harmonia entre meio ambiente e as tecnologias da informação e comunicação.

Nas palavras de Telles e Kolbe Junior (2022, p. 118) “As cidades inteligentes com base em *IoT* estão revolucionando o planejamento urbano e facilitando a vida dos cidadãos por meio do aumento da eficiência, da qualidade e da acessibilidade dos serviços públicos”.

Nesse contexto, por intermédio da aplicação da tecnologia e uso da *IoT*, busca-se aprimorar a qualidade de vida dos habitantes e promover o desenvolvimento econômico sustentável. Essa abordagem oferece benefícios diretos para a população, abrangendo áreas como eficiência energética, controle de tráfego, preservação do meio ambiente, gestão de resíduos e segurança pública, alinhando-se com os princípios da Carta Brasileira para Cidades Inteligentes (CBCI):

> CIDADES INTELIGENTES São cidades comprometidas com o desenvolvimento urbano e a transformação digital sustentáveis, em seus aspectos econômico, ambiental e sociocultural, que atuam de forma planejada, inovadora, inclusiva e em rede, promovem o letramento digital, a governança e a gestão colaborativas e utilizam tecnologias para solucionar problemas concretos, criar oportunidades, oferecer serviços com eficiência, reduzir desigualdades, aumentar a resiliência e melhorar a

> qualidade de vida de todas as pessoas, garantindo o uso seguro e responsável de dados e das tecnologias da informação e comunicação (Artigo19; Internetlab; Lapin, 2022, p. 24).

Segundo Telles e Kolbe Junior (2022, p. 117), "[...] o impacto em alguns pilares de uma cidade inteligente é resultante da importância da mobilidade, como sustentabilidade, economia e moradia, questão vital para os cidadãos e os governos municipais".

Nesse sentido, ensina Silva (2021, p. 31): "[...] os principais objetivos das cidades inteligentes são: interatividade, redução do consumo de recursos, segurança, consumo consciente de vários serviços, qualidade de vida e aproximação entre cidadãos e governos".

Conforme destacado por Telles e Kolbe Junior (2022, p. 118), as cidades inteligentes baseadas na *IoT* estão transformando o planejamento urbano e simplificando a vida dos cidadãos através do aprimoramento da eficiência, qualidade e acessibilidade dos serviços públicos. Além disso, a *IoT* viabiliza o monitoramento e gerenciamento mais eficaz e em tempo real do tráfego, permitindo a reconfiguração de rotas com base nas condições monitoradas. Essas iniciativas contribuem para a redução de congestionamentos, a melhoria da fluidez do tráfego e a diminuição das emissões de gases poluentes.

Além disso, a Internet das Coisas possibilita o monitoramento e o controle inteligente do consumo de energia nas cidades. Sensores coletam dados em tempo real sobre o uso de energia em edificações, iluminação pública e infraestrutura, possibilitando ajustes automáticos para reduzir o desperdício e otimizar a eficiência energética.

Dispositivos *IoT* podem coletar dados sobre a qualidade ambiental e fornecer informações precisas, permitindo uma resposta rápida a problemas e a implementação de medidas para melhorar a sustentabilidade e o bem-estar dos cidadãos. Contêiner de lixo inteligente, por exemplo, pode ser equipado com sensores que monitoram os níveis de enchimento, permitindo que as equipes de coleta otimizem as rotas e reduzam a frequência de coleta desnecessária (Palhoça, 2022). Isso resulta em economia de custos e redução do impacto ambiental.

Na mesma perspectiva, câmeras de vigilância conectadas em rede podem transmitir imagens em tempo real para centros de monitoramento, permitindo uma resposta rápida a incidentes. Além do mais, sensores podem detectar atividades suspeitas, como disparos de armas de fogo (Conheça..., 2023) ou movimentos incomuns, acionando avisos para as autoridades competentes (Miglior, 2023).

A seguir, será apresentado o exemplo da cidade de Barcelona, uma cidade inteligente que utiliza partes das tecnologias mencionadas.

Figura 2 – Cidade Inteligente de Barcelona

Fonte: Cisco (2014)

A cidade de Barcelona, na Espanha, destaca-se como um exemplo emblemático no aproveitamento das tecnologias apresentadas como a Internet das Coisas, e na obtenção de melhorias e recursos para a população. Por meio de uma abordagem inovadora e do uso estratégico dessas tecnologias, Barcelona tem se transformado em uma cidade inteligente de referência global. Conforme o relatório elaborado pela CISCO (2014), a cidade implementou projetos voltados para a conectividade urbana, gestão inteligente de recursos, mobilidade sustentável, segurança pública e participação cidadã. Com soluções baseadas na *IoT*, Barcelona tem alcançado resultados significativos, como a otimização do transporte público, a redução do consumo de energia, o monitoramento ambiental e a melhoria na qualidade de vida dos cidadãos.

O resumo executivo elaborado pela CISCO em 2014 oferece informações valiosas sobre as iniciativas adotadas por Barcelona. O documento destaca a visão estratégica da cidade em aproveitar a *IoT* e outras tecnologias digitais como ferramentas para impulsionar a inovação e melhorar a eficiência dos serviços urbanos. Além disso, o resumo enfatiza o impacto positivo dessas ações no desenvolvimento econômico, sustentabilidade ambiental e na criação de uma cidade mais inclusiva e conectada. O exemplo de Barcelona serviu e serve como inspiração para outras cidades no mundo, demonstrando o potencial transformador das tecnologias emergentes quando aplicadas de forma inteligente e estratégica, no contexto urbano.

Conforme evidenciado naquele resumo executivo, o projeto da Cidade de Barcelona propõe-se à aprimoração da qualidade de vida da população e ao incentivo da atividade econômica em uma inovadora cidade inteligente. A estratégia traçada tem como objetivo a reconfiguração urbana por meio da aplicação direcionada de Tecnologias da Informação e Comunicação (CISCO, 2014).

A proposta concebida envolveu a instalação de sensores amplamente distribuídos pela cidade, desempenhando um papel crucial na coleta de informações pertinentes que serviram como base para iniciativas voltadas à gestão inteligente de recursos, abrangendo aspectos como água, iluminação e energia. Esses sensores desempenham um papel crucial ao capturar dados essenciais que serão utilizados para otimizar os sistemas urbanos (CISCO, 2014).

Os desdobramentos resultantes da execução dessa estratégia são consideráveis. Conforme o resumo executivo CISCO (2014), a adoção da tecnologia de gestão inteligente de água propiciava à época uma economia anual estimada em torno de US$ 58 milhões. Paralelamente, a aplicação da tecnologia de estacionamento inteligente se traduzia em um aumento anual de cerca de US$ 50 milhões nas receitas provenientes da cobrança deste serviço. Um efeito adicional de destaque foi a geração de aproximadamente 47 mil novos postos de trabalho, impulsionada pela dedicação à edificação e operação da cidade inteligente.

1.4.4 Internet das Coisas Industrial – *IIoT*

A Internet das Coisas Industrial, também conhecida como *IIoT* (*Industrial Internet of things*), refere-se à aplicação da tecnologia *IoT* em ambientes industriais, especialmente no que diz respeito à instrumentação e ao controle de sensores e dispositivos que envolvem tecnologias de nuvem (Oracle, 2022).

A *IIoT* revoluciona como as empresas operam, melhorando a eficiência, a produtividade e a segurança no ambiente industrial, permitindo o monitoramento em tempo real de máquinas, equipamentos e processos industriais. Sensores e dispositivos conectados podem coletar dados e transmiti-los para sistemas de análise, o que possibilita identificar gargalos, ineficiências e oportunidades de melhoria, bem como antecipar problemas e falhas iminentes (Certi, 2023).

Tais ações e mecanismos, uma vez implementados, permitem manutenções preventivas, evitam paradas não planejadas, reduzem custos de manutenção, otimizam processos, diminuem tempo de produção, melhoram a qualidade do produto e aumentam a eficiência do sistema de produção.

Dispositivos e sensores conectados também podem ser integrados para controlar e monitorar remotamente máquinas e sistemas, reduzindo a necessidade de intervenção humana direta, o que aumenta a eficiência operacional, reduz erros e riscos associados a atividades manuais, e possibilita o controle das operações em tempo real a partir de qualquer localização. Nesse sentido, leciona Almeida (2019, p. 60):

> Sistemas integrados a redes de Internet conhecidos pela sigla *IoT* (do inglês *Internet of things* ou Internet das Coisas) utilizam sinais a partir de sensores, dispositivos com controles integrados, dados armazenados em nuvem e códigos específicos dos usuários, que possibilitam um alto grau de automação remota, sendo possível desde a automação de objetos do cotidiano doméstico, como abertura e fechamento de portas, controle de temperatura e iluminação de ambientes etc. até a automação de robôs, esteiras transportadoras, máquinas de usinagem, controle das dimensões e expedição do produto em qualquer quantidade.

A *IIoT* facilita a gestão de ativos, como equipamentos, veículos e ferramentas, ao fornecer informações em tempo real sobre sua localização, condição e desempenho. Permite também um melhor planejamento de uso e manutenção desses ativos, além de rastreá-los e prevenir perdas e roubos (ItForum, 2018).

Ela ainda permite o monitoramento contínuo das condições de trabalho e segurança no ambiente industrial (Oracle, 2023). Nesse sentido, destaca-se o projeto da Petrobrás, de uniforme inteligente, batizado de Anjo da Guarda: o referido projeto tem como objetivo transformar o uniforme em um equipamento de proteção individual avançado. Sensores capazes de identificar potenciais situações de risco para os colaboradores, tais como a presença de cargas sendo movimentadas acima da cabeça ou a aproximação de máquinas operando em alta temperatura. Além disso, esses sensores podem monitorar parâmetros biomédicos, identificando sinais de fadiga inadvertida por parte dos trabalhadores. Dessa forma, seriam acionados avisos para permitir que o colaborador descanse, ou, em caso de necessidade, um alerta seria encaminhado ao setor médico competente (Cunha, 2019).

Além disso, os sensores podem detectar vazamentos, níveis perigosos de gás, temperaturas excessivas, movimentos suspeitos, entre outros parâmetros, e enviar alerta em tempo real para ações corretivas imediatas. As mencionadas ações ajudam a prevenir acidentes, garantir a conformidade com os regulamentos de segurança e criar um ambiente de trabalho mais seguro (Oracle, 2023).

A Internet das Coisas industrial fornece uma quantidade significativa de dados, o que permite tomadas de decisões mais embasadas e assertivas. A análise desses dados pode fornecer

informações valiosas para otimizar a produção, melhorar a eficiência energética, identificar oportunidades de redução de custos e apoiar o planejamento estratégico.

Conforme mencionado até o momento, a *IoT* abrange setores como mobilidade urbana, agricultura, cidades inteligentes, casas inteligentes, saúde, bem-estar, meio ambiente, além de outros segmentos da indústria e do entretenimento. Essa abrangência reflete a capacidade da *IoT* de integrar dispositivos e sistemas, permitindo a coleta e a troca de dados em tempo real, bem como o monitoramento remoto e a tomada de decisões com base em dados precisos. Essa tecnologia tem contribuído para a redução de custos, a otimização de processos, o aumento da eficiência operacional, o fomento do desenvolvimento sustentável e a melhoria da qualidade de vida em diversos contextos. Por esses motivos, a *IoT* é um tema muito discutido dentro e fora da indústria. Espera-se que essa tecnologia revitalize os milagres científicos do passado: a máquina a vapor, a impressora e a eletricidade que conduziram as revoluções industriais anteriores.

Como se observa afinal, a *IoT* proporciona aplicabilidade e benefícios tanto para usuários individuais quanto para organizações empresariais, áreas urbanas e setores industriais. Trata-se de tecnologia que está promovendo transformações significativas na sociedade. A ascensão da *IoT* como catalisadora da geração massiva de dados provenientes de dispositivos conectados evidencia a necessidade de tratamento e refinamento desses dados para extrair valor significativo, conforme enfatizado por Belli (2023, p. 401).

Diante desse cenário, no próximo capítulo apresenta-se um panorama sobre a proteção de dados e a privacidade no ambiente digital.

2 PROTEÇÃO DE DADOS E PRIVACIDADE NO AMBIENTE DIGITAL

De acordo com Ana Frazão (2020, p. RB-1.2), a violação da privacidade e dos dados pessoais tornou-se um negócio lucrativo, fundamentado na extração e monetização de dados, o que permite a acumulação de um grande poder que se retroalimenta indefinidamente.

Considerando-se como ambiente digital o espaço virtual interconectado por meio da Internet, compreendendo redes mundiais de computadores, dispositivos móveis, plataformas digitais, sistemas de comunicação *online* e quaisquer outras tecnologias interativas que permitam a criação, o armazenamento, a transmissão e a recepção de dados e informações (Senado Federal, 2024), neste capítulo apresenta-se um panorama normativo que garante a necessária proteção da privacidade e da proteção de dados.

2.1 PROTEÇÃO DE DADOS NO AMBIENTE DIGITAL

A proteção de dados pessoais é a proteção da pessoa humana, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018). Segundo os ensinamentos de Ingo Wolfgang Sarlet (2023, p. 26), a proteção de dados pessoais constitui tanto um direito humano quanto um direito fundamental. Os direitos humanos são aqueles reconhecidos e protegidos no âmbito do sistema internacional de tratados de direito humanos, enquanto os direitos fundamentais são aqueles direitos humanos consagrados expressa ou implicitamente na esfera do Direito Constitucional de cada Estado.

De acordo com as análises de Laura Schertel Mendes (2014), a proteção dos dados pessoais surge na Sociedade da Informação como um mecanismo para salvaguardar a integridade pessoal do indivíduo, diante dos possíveis riscos associados ao tratamento desses dados, inclusive no ambiente digital. Sua finalidade não reside na proteção dos dados em si, mas sim na proteção da pessoa titular desses dados. A proteção de dados pessoais consiste em proteger o indivíduo contra os riscos que ameaçam sua personalidade decorrentes do tratamento de dados pessoais e atribui ao indivíduo a garantia de controlar o fluxo de seus dados na sociedade. Ruaro e Sarlet (2023, p. 179) lecionam que “a proteção de dados pessoais é, em síntese, a proteção da pessoa humana, mormente quanto ao resguardo do livre desenvolvimento de sua personalidade”.

Laura Schertel Mendes (2014) explica que o direito à proteção de dados pessoais encontra seus fundamentos nos princípios da finalidade, do esquecimento, da qualidade dos

dados, da transparência e do consentimento. Para assegurar a concretização desse direito, é necessário que o titular dos dados exerça controle efetivo sobre a circulação de suas informações na sociedade, o que só pode ser alcançado mediante a garantia do direito geral de informação, do amplo direito de acesso aos dados, do direito de notificação, do direito de retificação, e dos direitos de cancelamento e bloqueio dos dados.

Nas palavras de Sarlet (2023, p. 33), o direito à proteção de dados é um direito fundamental autônomo, vinculado à proteção da personalidade que vai além da tutela da privacidade. Enquanto o bem jurídico tutelado na privacidade se concentra na preservação da informação e do sigilo, a proteção de dados confere ao titular dos dados poderes para controlar a coleta e o processamento das informações que lhe digam respeito.

A proteção de dados na era informacional é de suma relevância, como evidenciado pelo reconhecimento do Supremo Tribunal Federal (STF), em maio de 2020, ao declará-la um direito fundamental autônomo no julgamento da Ação Direta de Inconstitucionalidade (ADIn) 6393. Este reconhecimento conferiu especial proteção aos dados pessoais como um mecanismo para reforçar a proteção individual e garantir uma limitação na intervenção do Estado. O Ministro Luiz Fux, em seu voto, afirmou: “a proteção de dados pessoais e autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada e, consectariamente, do princípio da dignidade da pessoa humana” (Brasil, 2020b).

Além disso, em 10 de fevereiro de 2022, o Congresso Nacional promulgou a Emenda Constitucional nº 115/2022, que incluiu a proteção de dados pessoais entre os direitos e garantias fundamentais (Brasil, 2022a). O referido texto também estabelece a competência exclusiva da União para legislar sobre a proteção e o tratamento de dados pessoais.

Salienta-se que o sancionamento da Lei Geral de Proteção de Dados, em conjunto com a promulgação da EC 115/2022, elevou o Brasil ao rol dos países considerados como adequados para proteger a privacidade e o uso de dados (Ruaro; Sarlet, 2023, p. 179).

Nas palavras do então presidente do Senado Federal, Rodrigo Otavio Soares Pacheco, ressalta-se a relevância da emenda para o fortalecimento das liberdades públicas. Sua avaliação considera que o novo mandamento constitucional complementa, fundamenta e reforça os dispositivos recentemente inseridos na legislação ordinária, ao mesmo tempo em que fortalece a liberdade dos brasileiros e a privacidade dos cidadãos. Além disso, a emenda também estimula os investimentos em tecnologia no país (Brasil, 2022c). Nesse contexto, segue o texto publicado pela Agência do Senado Federal:

> Os dados, as informações pessoais pertencem, de direito, ao indivíduo e a mais ninguém. Sendo assim, cabe a ele, tão somente a ele, ao indivíduo, o poder de decidir a quem esses dados podem ser revelados e em que circunstâncias, ressalvadas as exceções legais muito bem determinadas, como é o caso de investigações de natureza criminal, realizada de acordo com o devido processo legal. As informações voam à velocidade da luz, e as novas tecnologias, como a revolucionária Inteligência Artificial, são capazes de prever e descrever comportamentos e interesses coletivos e individuais com grande precisão. Desse modo, faz-se imperativo na modernidade que tenhamos no Brasil um preceito com força constitucional que deixe muito patente nosso compromisso de nação com o valor inegociável do valor da liberdade individual (Brasil, 2022c).

A Emenda Constitucional 115 acresceu, ao art. 5º da Constituição Federal de 1988, um novo inciso, LXXIX, ao estabelecer que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (Brasil, 1988), bem como inseriu alterações nos arts. 22 e 23 da CF. Com a promulgação dessa Emenda Constitucional, a proteção dos dados pessoais, independentemente do meio em que são aplicados (sejam físicos ou digitais), foi elevada ao patamar de cláusula pétrea constitucional. Assim, esses direitos se tornaram fundamentais e inalienáveis, integrando o rol dos direitos fundamentais, como o direito à vida, à liberdade, à segurança, à propriedade, à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, dentre outros direitos consagrados na Constituição.

Destaca-se que a coleta, o armazenamento, o uso e o compartilhamento não autorizados de dados pessoais podem resultar em diversas violações de privacidade e danos ao seu titular. Nesse contexto, conforme os ensinamentos de Laura Schertel Mendes (2014, p. 33, 37), os dados, por constituírem uma parte intrínseca da personalidade da pessoa humana, requerem proteção jurídica para garantir autonomia, liberdade, igualdade do titular e proteção contra situações potencialmente discriminatórias.

A consolidação do direito da privacidade, um direito fundamental, em conjunto com a evolução do direito à proteção de dados como igualmente fundamental, assinala a necessidade premente da adoção de medidas apropriadas para proteger os dados contra acessos não autorizados, infrações e utilização indevida. Assim, é fundamental evitar a manipulação indevida de dados com o propósito de discriminar ou marginalizar grupos específicos com base em características individuais, tais como etnia, gênero, faixa etária ou orientação sexual. Buscar a acessibilidade igualitária às tecnologias e aos seus proveitos torna-se essencial para salvaguardar a dignidade de todos os indivíduos.

Ademais, o anteprojeto de revisão e atualização do Código Civil, apresentado ao Senado Federal em 17 de maio de 2024, ao estabelecer um livro sobre o Direito Civil Digital e incluir normas de proteção de dados pessoais, adaptando a legislação às novas demandas tecnológicas

e de segurança informacional, entre outras providências, demonstra a crescente importância da proteção de dados e da privacidade no ambiente digital (Senado Federal, 2024).

2.2 PRIVACIDADE NO AMBIENTE DIGITAL

Os dados pessoais representam nossa identidade no mundo virtual. É por meio deles que diversos aspectos de nossas vidas são decididos, como crédito, seguros, propagandas e políticas públicas. Dessa forma, garantir que os dados pessoais sejam utilizados de modo adequado, transparente e para finalidades benéficas para os usuários é primordial (Lemos; Branco, 2023, p. 450).

Sobre privacidade, Stefano Rodotà (*apud* Magrani, 2019, p. 56), pensador italiano, a conceitua como o direito de exercer controle sobre as informações pessoais e determinar o modo de construção da esfera particular individual. Nesse sentido, Laura Schertel Mendes e Gabriel Campos Soares Fonseca (2023, p. 75) definem privacidade "Como barreira de acesso à vida privada do indivíduo, formando uma garantia de inviolabilidade e de imunidade quanto a certos aspectos da sua vida pessoal e da sua intimidade. Uma liberdade individual negativa traduzida como o direito de ser deixado em paz/só". Laura Schertel Mendes (2014, p. 32) afirma também que "a sociedade somente poderá usufruir efetivamente das vantagens do desenvolvimento tecnológico se este for acompanhado da tutela jurídica da privacidade".

Rosner (2016) ensina que na Europa a privacidade é concebida como um "direito fundamental" com o qual as pessoas nascem. As políticas europeias usam principalmente o termo "proteção de dados", em vez de "privacidade". É um conceito mais restrito, aplicado especificamente a políticas e direitos relacionados ao tratamento justo de dados pessoais por parte das organizações e à boa governança de dados. Já a privacidade abrange uma gama mais ampla de áreas temáticas e diz respeito a interesses além da justiça, como dignidade, vigilância inadequada, invasões da imprensa e outros.

A taxonomia de privacidade criada por Solove (2006) identifica quatro grupos básicos de atividades prejudiciais à privacidade: coleta de informações, processamento de informações, disseminação de informações e invasão e cada grupo abrange uma série de práticas distintas.

Na coleta de informações, há a vigilância, que se refere à observação, escuta ou gravação das atividades de um indivíduo, e o interrogatório, que envolve questionar ou sondar informações (Solove, 2006). De acordo com os ensinamentos de Laura Schertel Mendes (2016), "a vigilância de todos os seus comportamentos pelas empresas enseja a perda de controle sobre

as suas informações que circulam na sociedade e gera uma pressão causada pela participação social em informações privadas."

Em relação ao processamento de informações, várias etapas são consideradas, tais como a agregação, que consiste em combinar diversos dados relacionados a uma pessoa; a identificação, que vincula informações a indivíduos específicos; a insegurança, relacionada ao descuido na proteção das informações armazenadas; o uso secundário, que implica a utilização de informações para finalidades diferentes das originalmente coletadas, sem o consentimento da pessoa; e a exclusão, que representa a falha em permitir que alguém tenha conhecimento dos dados que outros possuem sobre ele e participe do seu manuseio e uso (Solove, 2006).

No contexto da disseminação de informações, diversas ações são abordadas, como a quebra de confidencialidade, a qual envolve romper uma promessa de manter as informações de alguém confidenciais; a divulgação, consistente na revelação de informações que afetam a forma como os outros julgam alguém; a exposição, englobando a revelação da nudez, luto ou funções corporais de outra pessoa; a maior acessibilidade, que visa ampliar a acessibilidade da informação, a chantagem, representando a ameaça de divulgar informações pessoais; a apropriação, que se refere ao uso da identidade de alguém para servir aos interesses de outra pessoa; e, por fim, a distorção, que implica em disseminar informações falsas ou enganosas sobre alguém (Solove, 2006).

O grupo de invasão compreende duas facetas distintas: a intrusão, que se refere a invadir a tranquilidade ou a solidão de alguém, invadindo seu espaço pessoal; e a interferência de decisão, a qual envolve a incursão nas decisões de alguém sobre seus assuntos privados, afetando sua autonomia e liberdade de escolha (Solove, 2006).

Warren e Brandeis (*apud* Rosner, 2016) tratam dos danos à privacidade como uma lesão incorpórea, referindo-se a danos dignitários. Estes afetam a dignidade, a reputação, os sentimentos e a angústia emocional de uma pessoa, em vez de causar lesões físicas diretas. Um exemplo clássico de dano dignitário é o dano reputacional, que ocorre quando as ações de alguém levam a uma diminuição da estima da pessoa aos olhos dos outros, como no caso de difamação. Além disso, há outros tipos de danos dignitários que podem ser causados, como a incivilidade e o desrespeito, os quais também podem resultar em angústia emocional.

Nos ensinamentos de Rosner (2016), os danos à privacidade transcendem a "dor mental e angústia" causada a indivíduos específicos; tais danos influenciam a sociedade e obstaculizam atividades individuais que contribuem para o bem social mais amplo. A preservação da privacidade e a proteção dos dados são elementos vitais para o funcionamento da sociedade e da democracia.

Nas palavras de Marineli (2019), a privacidade nos remete a uma ideia de exclusão, abrigo ou reserva; de manter longe do conhecimento de algumas pessoas ou de toda a coletividade determinadas informações, ou momentos que dizem respeito somente ao indivíduo. A privacidade pode ser definida como o direito personalíssimo atribuído a toda pessoa de manter certos momentos, aspectos e dados relacionados à própria vida ao abrigo de invasões e divulgações não autorizadas.

No ordenamento jurídico vigente, a privacidade é considerada um direito fundamental, previsto no inciso X do art. 5º da Constituição Federal de 1988 e no Código Civil, no rol de Direito da Personalidade, e na Lei Geral de Proteção de Dados, inclusive estabelecendo que o direito à privacidade deve ser observado desde a concepção do produto ou do serviço até a sua execução (art. 46, da LGPD). O direito à privacidade abrange variados aspectos, incluindo os direitos à intimidade, à honra, à imagem, à inviolabilidade do domicílio, ao sigilo de correspondência e das comunicações telegráficas, bem como à proteção dos dados das comunicações telefônicas.

Nesse sentido, ensina Laura Schertel Mendes (2014, p. 170), "a partir do art. 5º, X, da CF, que garante a inviolabilidade da intimidade e da vida privada, é possível extrair uma tutela ampla da personalidade e da vida privada do cidadão, nas mais diversas situações em que ele se encontra."

Os direitos à intimidade, à honra e à imagem estão previstos na Constituição Federal de 1988, mais especificamente no art. 5º, inciso X, que assegura o direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas: "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).

Esses direitos também são protegidos pelo Código Civil Brasileiro, Lei nº 10.406/2002, em seus art. 20 a 21, e reforçados pelo Código Penal Brasileiro, Decreto-Lei nº 2.848/1940, nos arts. 138, 139 e 140, que prescrevem os crimes de calúnia, difamação e injúria, respectivamente, e art. 154-A, o qual define o crime de invasão de dispositivo informático. É importante ressaltar que a legislação brasileira também está em conformidade com tratados e convenções internacionais de direitos humanos, responsáveis por fortalecer a proteção dos direitos à intimidade, à honra, à imagem e à privacidade das pessoas[8].

[8] A Declaração Americana dos Direitos e Deveres do Homem (1948), no art. V; Convenção Americana sobre Direitos Humanos ("Pacto de São José") (1969) no art. 11; Declaração Universal dos Direitos Humanos (arts. 12, 18-20); o Pacto Internacional sobre os Direitos Civis e Políticos (art. 17-19); a Convenção para a Proteção dos Direitos Humanos e das Liberdades Fundamentais (arts. 8-10); a Carta dos Direitos Fundamentais da União Europeia (arts. 1, 7, 8, 10-12) e a Carta Africana sobre os Direitos Humanos e dos Povos (arts. 5, 8-11 e 28).

A Constituição Federal de 1988 também trata da proteção de dados pessoais por intermédio do remédio constitucional *Habeas Data*, previsto no art. 5º, LXXII, que assegura o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público e concede o direito de retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo (Brasil, 1988).

Conforme os ensinamentos de Danilo Doneda (2023, p. 12), as legislações dos estados do Rio de Janeiro[9] e de São Paulo[10], antes da CF/88, já dispunham de leis sobre o direito de acesso e retificação de dados pessoais, apresentando elementos como o princípio da finalidade e do consentimento informado, que prepararam o caminho para o debate referente ao *habeas data* na Constituição de 1988.

Em defesa do direito à privacidade, bem como em razão do caso emblemático de Edward Snowden[11], o Conselho de Direitos Humanos das Nações Unidas, em 21 de novembro de 2016, aprovou a Resolução sobre o Direito à Privacidade na Era Digital, apresentada pelo Brasil e pela Alemanha (Brasil, 2013). A finalidade do documento é convocar os Estados a respeitarem e protegerem o direito à privacidade, bem como a pôr fim às violações, adotando medidas efetivas para a reparação (Ruaro; Sarlet, 2023, p. 182).

A seguir, apresenta-se um panorama normativo brasileiro sobre os direitos de privacidade e proteção de dados.

2.3 PREVISÃO LEGAL NO BRASIL: DIREITOS DE PRIVACIDADE E PROTEÇÃO DE DADOS

No Brasil, além dos mandamentos constitucionais, existe um conjunto de leis que atuam de forma complementar, proporcionando uma estrutura legal abrangente para a proteção dos dados pessoais. Esse arcabouço jurídico visa salvaguardar a privacidade e a segurança das informações dos indivíduos e estabelece diretrizes e garantias fundamentais para o tratamento adequado dos dados pessoais, com o objetivo de proteger os direitos individuais e promover

[9] Lei Estadual nº 824, de 28 de dezembro de 1984, que "Assegura O direito de obtenção de informações pessoais contidas em banco de dados operando no Estado do Rio de Janeiro e dá outras providencias" (Rio de Janeiro, 1984).

[10] Lei Estadual nº 5.702, de 5 de junho de 1987, que "Concede ao cidadão o direito de acesso às informações nominais sobre sua pessoa" (São Paulo, 1987).

[11] Edward Snowden, um ex-funcionário terceirizado da Inteligência dos Estados Unidos, baixou milhares de documentos da Agência de Segurança Nacional (NSA) e revelou ao mundo a extensão do sistema de espionagem norte-americano, expondo como o serviço de inteligência dos Estados Unidos era capaz de coletar dados de pessoas de todo o mundo (Lucena, 2023).

confiança na utilização dessas informações.

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, assume um papel central nessa proteção desde sua entrada em vigor em setembro de 2020. Essa lei estabelece diretrizes para o tratamento de dados pessoais por parte de empresas e organizações, visando garantir a privacidade e a segurança desses dados.

Além da LGPD, participa da proteção de dados pessoais e privacidade o Código de Defesa do Consumidor, Lei nº 8.078/1990, que contém disposições que protegem a privacidade e os dados pessoais dos consumidores. A Lei de Acesso à Informação, Lei nº 12.527/2011, assegura o direito de acesso a informações públicas, enquanto a Lei nº 12.414/2011 instituiu o Cadastro Positivo, regulamentando como são tratados os dados financeiros dos consumidores. No âmbito da Internet, o Marco Civil da Internet, Lei nº 12.965/2014, estabelece princípios e direitos relacionados à privacidade e proteção de dados pessoais *online*. Há ainda a Lei do Direito de Resposta, Lei nº 13.188/2015, que prevê procedimentos para garantir o direito à retificação de informações divulgadas por veículos de comunicação.

Nas próximas seções, serão analisadas, em ordem cronológica, as disposições de proteção de dados previstas nas legislações supramencionadas.

2.3.1 Código de Defesa e Proteção do Consumidor – CDC

O Código de Defesa do Consumidor, Lei nº 8.078/1990 (Brasil, 1990), conforme seu art. 1º, estabelece normas de proteção e defesa do consumidor, de ordem pública e interesse social, nos termos dos arts. 5º, XXXII e 170, V, da Constituição Federal e do art. 48 de suas Disposições Transitórias.

O CDC representa uma legislação que regula minuciosamente as interações no âmbito das transações de consumo, estabelecendo direitos e responsabilidades tanto para os consumidores como para os fornecedores de produtos e serviços. Essa regulação visa assegurar que os consumidores estejam devidamente informados acerca dos produtos e serviços que adquirem, ao tempo em que proporciona mecanismos eficazes para apresentar reclamações e buscar reparação em situações adversas ou litigiosas.

A relação entre o Código de Defesa do Consumidor e a proteção de dados reside na salvaguarda dos interesses dos consumidores em relação ao tratamento das informações pessoais. Ressalta-se que o Código de Defesa do Consumidor, na Seção VI, que trata dos Bancos de Dados e Cadastros de Consumidores, já previa a proteção de dados pessoais:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
> § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
> § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
> § 6 Todas as informações de que trata o caput deste art. devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.
> Art. 44. Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor.
> § 1° É facultado o acesso às informações lá constantes para orientação e consulta por qualquer interessado.
> § 2° Aplicam-se a este artigo, no que couber, as mesmas regras enunciadas no art. anterior e as do parágrafo único do art. 22 deste código (Brasil, 1990).

Além disso, empresas que efetuam a coleta de dados pessoais de consumidores como parte de suas atividades comerciais estão sujeitas à obrigação de cumprir os princípios constitucionais e as disposições da Lei Geral de Proteção de Dados, garantindo, assim, que as informações pessoais dos consumidores sejam manipuladas com segurança e em estrita conformidade com o arcabouço legal.

É observável que a proteção do consumidor encontra previsão legal no inciso VI do art. 2º da Lei Geral de Proteção de Dados: "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...] VI – a livre iniciativa, a livre concorrência e a defesa do consumidor" (Brasil, 2018).

Além disso, o art. 45 da referida lei estabelece que a responsabilidade civil prevista no Código de Defesa do Consumidor é aplicável no contexto de infrações envolvendo a violação de dados pessoais nas relações de consumo, nos seguintes termos: "Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente" (Brasil, 2018).

Esse imperativo legal abrange a obtenção de consentimento apropriado, a proteção contra eventuais violações de dados e a promoção da transparência no tratamento das informações pessoais.

Desse modo, considerando que o Código de Defesa do Consumidor se dedica à regulamentação das relações de consumo em sua amplitude, cabe destacar que a Lei Geral de Proteção de Dados e outras normativas de proteção de dados desempenham um papel complementar, assegurando a devida salvaguarda das informações pessoais dos consumidores com meticulosa atenção à preservação da privacidade e a intimidade.

2.3.2 Lei de Acesso à Informação – LAI

A Lei de Acesso à Informação (LAI), Lei nº 12.527/2011 (Brasil, 2011b), de direito público, visa dar transparência às atividades da administração pública, permitindo ao cidadão o acesso a informações, conforme previsto no art. 5º, XXXIII, da Constituição Federal de 1988, que estabelece que todos têm o direito de receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo, ou geral, as quais serão prestadas no prazo da lei, sob pena de responsabilidade, exceto aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

O direito de acesso à informação disponibilizado pela LAI permite aos cidadãos consultar os seus dados pessoais armazenados pelos órgãos governamentais, dando-lhes a possibilidade de corrigir ou remover esses dados, caso estejam errados ou insuficientes.

A LAI, além de prever no art. 31 que o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais, determina, em seu art. 31, § 1º, II, que existem duas hipóteses para divulgação da informação: (i) previsão legal; ou (ii) consentimento do titular. Entre as hipóteses legais (art. 31, § 3º), incluem-se: prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, exclusivamente para utilização no tratamento médico; realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstas em lei, com vedação à identificação da pessoa a que as informações se referem; cumprimento de ordem judicial; defesa de direitos humanos; ou proteção do interesse público e geral preponderante.

2.3.3 Lei de Cadastro Positivo – LCP

A Lei de Cadastro Positivo, Lei nº 12.414/2011 (Brasil, 2011a), disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de

pessoas jurídicas, para formação de histórico de crédito, sem prejuízo do disposto no Código de Proteção e Defesa do Consumidor (Brasil, 1990).

A Lei do Cadastro Positivo foi alterada pela Lei Complementar nº 166 de 2019, estabelecendo requisitos importantes para o tratamento de dados no âmbito da formação do histórico de crédito dos consumidores. De acordo com o art. 4º da referida Lei, a inclusão passou a ser automática, sem a necessidade de autorização prévia do cadastrado. Dessa forma, os dados tratados resultam em uma espécie de nota de crédito, chamada de "score", com base no histórico do consumidor no mercado.

Conforme o site do Ministério Público do Estado do Ceará, o cadastro positivo é um reservatório de informações que contém referências sobre pessoas físicas ou jurídicas, com informações sobre o nível de adimplemento (pagamento), idade, sexo, estado civil, comércio, rendimentos, tamanho da família e endereço do comprador. A confluência dessas informações produz um histórico de crédito abrangente, destinado a auxiliar as entidades financeiras na avaliação da viabilidade de concessão de crédito aos clientes, mediante solicitação (Ceará, 2023).

O registro da positividade, na sua essência, é uma compilação de indivíduos que demonstraram capacidade de cumprir suas obrigações financeiras, conquistando assim a confiança das instituições financeiras. Estas instituições tendem a favorecer aqueles que mantiveram um histórico de crédito positivo, concedendo-lhes acesso a linhas de crédito com maior facilidade. Ao realizar uma análise meticulosa da avaliação de risco, um indivíduo pode garantir termos e condições de compra mais favoráveis, com uma redução proporcional nas taxas de juros, baseado no seu histórico de crédito (Ceará, 2023).

Em abril de 2019, foi publicada a Lei Complementar nº 166, com a finalidade de alterar a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores, regulamentando a Lei nº 12.414/2011.

A referida modificação tornou automática a participação do cidadão no cadastro positivo. Esse sistema de ponderação de concessão de risco é chamado de *credit scoring*, também conhecido no Brasil como "escore de crédito" (Ceará, 2023).

Nos termos da Súmula 550-STJ – SISTEMA *CREDIT SCORING*[12], não é necessário o consentimento do consumidor para sua inclusão no banco de dados, porém este terá direito de

[12] **DIREITO DO CONSUMIDOR - SISTEMA *CREDIT SCORING.*** A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que

solicitar esclarecimentos sobre as fontes das informações valoradas no cálculo, inclusive solicitar a exclusão de seu cadastro ou de informações incorretas ou excessivas, que não sejam pertinentes à análise de crédito, tais como referências acerca de etnia, orientação sexual, religião, saúde ou convicções políticas. Nesse sentido, o § 3º do art. 3ª da Lei nº 12.414/2011 prescreve:

> § 3º Ficam proibidas as anotações de:
> I – informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e
> II – informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas (Brasil, 2011a).

Segundo o Ministério Público do Estado do Ceará (2023), a utilização excessiva ou abusiva das informações do consumidor configura abuso de direito, previsto no art. 187 do Código Civil, e enseja a responsabilidade objetiva e solidária de todos os fornecedores responsáveis pelo banco de dados e fontes, podendo acarretar danos morais e materiais ao consumidor, nos termos do art. 16 da Lei nº 12.414/2011.

2.3.4 Lei do Marco Civil da Internet – MCI

A Lei do Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, Estados, Distrito Federal e dos Municípios em relação à matéria (Brasil, 2014).

Nas palavras de Nazareno e Pinheiro (2021, p. 8), o Marco Civil da Internet "foi a primeira abordagem legislativa que previu a extensão dos direitos e garantias individuais para essa nova forma de se estabelecer negócios, de usufruir e prestar serviços e de se relacionar em sociedade".

A referida lei prevê como princípios que regulam o uso da Internet no Brasil, enumerados no art. 3º, dentre outros, o princípio da proteção da privacidade e dos dados pessoais e neutralidade da rede (Brasil, 2014). Os direitos de privacidade e proteção de dados pessoais estão previstos na Constituição Federal de 1988.

---

terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo (**Segunda Seção**, julgado em **14/10/2015**, DJe **19/10/2015**) (Brasil, 2015b).

O princípio da neutralidade da rede assegura que as informações que trafegam na rede mundial de computadores recebam o mesmo tratamento e trafeguem à mesma velocidade. Esse princípio visa garantir o livre acesso a qualquer tipo de informação, com o objetivo de manter uma internet livre e aberta, promovendo uma comunicação igualitária e imparcial (Fiorillo, 2015, p. 39).

Além disso, a lei do MCI assegura, no art. 7º, a inviolabilidade e o sigilo das comunicações dos usuários de Internet, exceto por ordem judicial.

De acordo com os ensinamentos de Nazareno e Pinheiro (2021, p. 10), os principais eixos em que a lei se concentrou foram: i) a neutralidade da Internet (art. 9º); ii) a guarda dos registros de conexão (arts. 10 a 14) e de aplicação (a navegação, arts. 15 a 17); e iii) a responsabilidade por material infringente (arts. 18 a 21).

Consigna-se que a Lei Geral de Proteção de Dados foi promulgada em 14 de agosto de 2018 e revogou alguns dispositivos do Marco Civil da Internet, por ser mais abrangente. Enquanto o Marco Civil prevê a segurança de dados apenas em ambiente *online*, a LGPD cria diretrizes mais específicas de aplicação e segurança, detalhando os tipos de dados existentes e assegurando toda a movimentação de dados, inclusive no ambiente *offline* (Chaves; Vidigal, 2020). Nesse contexto, considerando o objeto de estudo desta dissertação, passa-se à análise da Lei de Direito à Resposta e posteriormente ao Marco Regulatório da Proteção de Dados – Lei Geral de Proteção de Dados.

2.3.5 Lei de Direito à Resposta (Lei nº 13.188/2015)

A Constituição Federal de 1988, em seu art. 5º, IV, consagra a liberdade de expressão como um direito fundamental, garantindo a livre manifestação do pensamento. Este princípio é estendido tanto às pessoas físicas quanto aos meios de comunicação, sendo uma salvaguarda reforçada à liberdade de imprensa. A Carta Magna dedica o Capítulo V, especificamente, à comunicação social, reiterando a liberdade de expressão da imprensa e estipulando que a manifestação do pensamento, criação, expressão e informação não devem sofrer restrições, desde que estejam em conformidade com os princípios constitucionais, consoante disposto no art. 220 (Brasil, 1988).

Observa-se que a liberdade de expressão não é absoluta, havendo limites e consequências para seu uso abusivo (Rais, 2022, RB-16.4). Tanto o direito de manifestação do pensamento quanto a liberdade de imprensa devem respeitar os demais dispositivos constitucionais. A pessoa que publica informações falsas, especialmente aquelas que imputam

a prática de um crime a outra pessoa, pode ser responsabilizada civil e penalmente. Nesse sentido, sujeita-se à indenização por danos morais e materiais, conforme estabelecido no art. 5º, V, da Constituição Federal de 1988, que assegura o direito de resposta proporcional ao agravo, além da indenização por dano material, moral ou à imagem. Ademais, pode enfrentar processo criminal por calúnia, conforme previsto no art. 138 do Código Penal.

Segundo o ministro Marco Buzzi (Brasil, 2021a), o direito de resposta é a faculdade reconhecida ao afetado por uma informação inverídica, inexata ou abusiva de retificar ou contestar, pelo mesmo meio, consistindo em uma modalidade de integração da informação e de esclarecimento de seu conteúdo.

Já o § 1º do art. 2º da Lei de Direito à Resposta (Lei nº 13.188/2015) estabelece:

> Para os efeitos desta Lei, considera-se matéria qualquer reportagem, nota ou notícia divulgada por veículo de comunicação social, independentemente do meio ou da plataforma de distribuição, publicação ou transmissão que utilize, cujo conteúdo atente, ainda que por equívoco de informação, contra a honra, a intimidade, a reputação, o conceito, o nome, a marca ou a imagem de pessoa física ou jurídica identificada ou passível de identificação (Brasil, 2015a).

A referida lei promove a regulamentação do direito de resposta, conforme previsto na Constituição Federal. Esta legislação representa uma iniciativa voltada para proporcionar meios mais céleres e eficazes, visando a salvaguarda da honra e da imagem daqueles que se considerem lesados por informações divulgadas pela imprensa, seja via Internet ou qualquer outra plataforma de distribuição de conteúdo (Brasil, 2015a).

2.3.6 Marco Regulatório da Proteção de Dados no Brasil: Evolução Legislativa e Principais Aspectos da LGPD

Esta seção aborda a evolução da legislação brasileira de proteção de dados, desde sua inspiração na Lei de Proteção de Dados da União Europeia – GDPR até a implementação da Lei Geral de Proteção de Dados Pessoais – LGPD no Brasil. Destaca-se o impacto e a relevância da LGPD para a salvaguarda dos direitos individuais. Além disso, são apresentados os objetivos da lei e é enfatizada a função da LGPD na proteção dos dados pessoais, assegurando a privacidade e os direitos individuais dos cidadãos. Também é destacada a abordagem da LGPD em relação à responsabilidade civil, que estabelece diretrizes e normativas para proteger os titulares de dados e responsabilizar as organizações por danos decorrentes da manipulação

inadequada das informações. Por fim, são analisados os princípios basilares da LGPD, os direitos dos titulares de dados e sua interação com os princípios estabelecidos na legislação.

Conforme os ensinamentos de Garrido (2023), a liderança na discussão sobre proteção de dados teve origem na União Europeia (UE), com destaque para o partido *The Greens*, que resultou na promulgação do Regulamento Geral de Proteção de Dados Pessoais Europeu nº 679 (GDPR), em 27 de abril de 2016. Esse regulamento estabeleceu um prazo de dois anos para a adaptação, que expirou em 25 de maio de 2018, quando as penalidades começaram a ser aplicadas.

A promulgação da GDPR desencadeou um efeito dominó, levando outros países e empresas com relações comerciais com a União Europeia a adotarem também legislação de proteção de dados semelhante. A ausência de uma lei com o mesmo nível de proteção poderia resultar em barreiras econômicas ou dificuldades nas negociações com os países da UE, o que se tornou um desafio para a maioria das nações, especialmente as da América Latina, considerando as condições econômicas atuais (Garrido, 2023).

Com base nos ensinamentos de Donda (2020), a LGPD é um marco jurídico regulatório inédito no Brasil, aplicável a todas as instituições públicas e privadas, com o intuito de proteger os direitos fundamentais de liberdade e privacidade dos cidadãos brasileiros. A lei, se bem aplicada, promoverá o desenvolvimento econômico e tecnológico no país.

O STJ (Brasil, 2020a) também destaca que a LGPD representa um marco histórico na regulamentação do tratamento de dados pessoais no Brasil, abrangendo tanto meios físicos quanto plataformas digitais, aplicável a instituições públicas e privadas. A proteção de dados pessoais também foi incluída no rol de direitos e garantias fundamentais após a promulgação da Emenda Constitucional nº 115/2022, como já mencionado.

A LGPD, Lei nº 13.709, de 14 de agosto de 2018, entrou em vigor em diferentes fases: no dia 28 de dezembro de 2018, vigoraram os arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; em 1º de agosto de 2021, os arts. 52, 53 e 54; e em setembro de 2020, após 24 meses de sua publicação, os demais artigos. Essas fases foram estabelecidas para permitir uma transição e adaptação gradual das organizações à nova legislação de proteção de dados no Brasil, especialmente considerando o impacto da pandemia de Covid-19.

Desde então, a LGPD tem sido aplicada para regular o tratamento de dados pessoais, garantir a privacidade dos indivíduos e estabelecer diretrizes para o uso adequado e seguro das informações pessoais no país.

A Lei Geral de Proteção de Dados Pessoais, conforme previsto no art. 1º, estabelece diretrizes e regras para o tratamento de dados pessoais, inclusive nos meios digitais, por organizações públicas e privadas:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

O propósito da lei é assegurar a proteção dos dados, com foco na preservação da privacidade, da autodeterminação informativa, das liberdades de expressão, informação, comunicação e opinião, bem como na inviolabilidade da intimidade, honra e imagem. Além disso, a legislação visa garantir o direito ao livre desenvolvimento da personalidade, fomentar o progresso econômico e tecnológico, promover a livre iniciativa, a concorrência justa e a defesa dos direitos do consumidor. A lei também se pauta na proteção dos direitos humanos, na dignidade e no exercício da cidadania das pessoas naturais, como delineado em seu art. 2º.

Nesse sentido, ensina Garrido (2023, p. 37) que "A legislação visa fortalecer a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico".

Segundo Maimone (2022, p. 18), trata-se de uma lei principiológica, cujos princípios, ao lado da boa-fé, devem ser atendidos no tratamento de dados pessoais. É uma legislação de caráter preventivo, que procura antecipar os riscos de violação à privacidade, estabelecendo formas eficazes para evitar danos à pessoa natural.

Saliente-se que a LGPD será aplicada quando os dados forem coletados ou tratados dentro dos limites territoriais do Brasil, independentemente da nacionalidade ou origem do titular dos dados, conforme prescreve o art. 3º da referida lei:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I – a operação de tratamento seja realizada no território nacional; - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> II – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta (Brasil, 2018).

Nesse contexto, a LGPD terá aplicação em situações em que os dados tenham sido coletados no Brasil, mas seu tratamento tenha ocorrido no exterior, bem como nos casos de coleta ou tratamento de dados pessoais de cidadãos estrangeiros realizados dentro das fronteiras brasileiras.

Além das disposições sobre o tratamento de dados, a Lei Geral de Proteção de Dados também enfrenta a questão da responsabilidade civil no contexto da proteção de dados pessoais. Essa abordagem estabelece um conjunto de princípios e regras que visam proteger os direitos dos titulares de dados, e garantir que as organizações que tratam dados pessoais assumam a responsabilidade por eventuais danos decorrentes do seu tratamento.

De acordo com a LGPD, as organizações que realizam o tratamento de dados pessoais são responsáveis por adotar medidas técnicas e administrativas adequadas para proteger esses dados contra acessos não autorizados, vazamentos, perdas ou qualquer tipo de incidente que possa comprometer a sua segurança e integridade, como reza o inciso VII do art. 6º da LGPD. A designação de um Encarregado de Proteção de Dados, a elaboração de políticas internas de proteção de dados e a implementação de protocolos de segurança fazem parte dessas medidas.

Além disso, a LGPD, em sua Seção III, da Responsabilidade e do Ressarcimento de Danos, estabelece que, em caso de violação de dados que resulte em danos ao titular, a organização responsável pelo tratamento é passível de responsabilidade civil. Isso significa que a organização pode ser acionada judicialmente pelo titular de dados para reparação dos danos sofridos. A lei prevê que a indenização poderá incluir indenização por danos materiais e morais, bem como medidas para coibir a infração e prevenir danos futuros.

A perspectiva da responsabilidade civil na LGPD busca garantir que os titulares de dados tenham meios eficazes para salvaguardar seus direitos em relação à proteção dos dados pessoais e buscar reparação em caso de violações, estipulando assim que organizações adotem práticas de tratamento de dados seguras e responsáveis, uma vez que a negligência na proteção de dados pode resultar em consequências financeiras significativas (Brasil, 2018, art. 52 e ss). Tal perspectiva enfatiza a importância da conformidade com a lei e do investimento em segurança de dados para todas as organizações que lidam com informações pessoais no Brasil.

A Lei Geral de Proteção de Dados incorpora uma variedade de terminologias e conceitos de fundamental importância para a compreensão da legislação e seu mecanismo de atuação, sendo que os principais são tratados a seguir.

Dados pessoais referem-se a todas as informações relacionadas a uma pessoa natural identificada ou identificável, conforme o inciso I do art. 5º da LGPD. Nas palavras de Garrido (2023, p. 28), essas informações podem abranger elementos como nome, CPF, RG, endereço,

número de telefone, endereço de e-mail, dados de localização, placas de veículos, histórico de compras, informações acadêmicas e números de protocolo de Internet, entre outros. É importante destacar que esses dados devem estar vinculados a pessoas naturais vivas para se enquadrarem na definição de dados pessoais.

Dados pessoais sensíveis, conforme previsto no inciso II do art. 5º da LGPD, são informações sobre a vida privada de uma pessoa e incluem, entre outras coisas, a sua herança racial ou étnica, suas crenças religiosas, filosóficas ou morais, sua filiação sindical, suas opiniões políticas, sua informação genética, informação biométrica, informações de saúde ou sua vida sexual. Trata-se de dados que devem ser protegidos de forma mais rigorosa, pois podem ensejar discriminação ilícita ou abusiva de seu titular (Doneda, 2023).

Conforme o ensinamento de Maldonado e Blum (2022), **dados pessoais indiretos** são aqueles que, por meio de tratamento, tornam a pessoa natural identificável, pois necessitam de informações adicionais para identificá-las, como gostos, interesses, hábitos de consumo, profissão, sexo, idade e geolocalização.

Maldonado e Blum (2022) também lecionam que **dados pseudoanonimizados** são os dados que perdem a possibilidade de associação direta ou indireta a um indivíduo, exceto pelo uso de informações adicionais mantidas separadamente pelo controlador em um ambiente controlado e seguro. São dados que mantêm a sua qualidade de dados pessoais, pois referem-se a uma pessoa natural identificável.

Dado anonimizado, que não constitui dado pessoal, refere-se às informações pessoais que foram processadas ou manipuladas de forma a não poderem mais ser associadas, direta ou indiretamente, a uma pessoa específica, conforme previsto no inciso III do art. 5º da LGPD. Segundo Danilo Doneda (2021, p. RB-2.3), a chamada “anonimização” de dados pessoais, que consiste na retirada do vínculo da informação com a pessoa a qual se refere, é um recurso utilizado por algumas leis de proteção de dados para reduzir os riscos associados ao tratamento desses dados.

De acordo com o inciso V do art. 5º da LGPD, **titular** é a pessoa natural a quem pertencem ou estão vinculados os dados tratados (Brasil, 2018).

Tratamento de dados é um conjunto de operações realizadas sobre dados pessoais, as quais incluem a coleta, o armazenamento, a organização, a estruturação, a recuperação, a consulta, o uso, a divulgação por transmissão, a disseminação ou qualquer outra forma de disponibilização, a comparação ou a interconexão, a restrição ou a destruição de dados pessoais, nos termos do inciso X do art. 5º da LGPD (Brasil, 2018).

Conforme o inciso XII do art. 5º da LGPD, **consentimento** é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (Brasil, 2018).

Danilo Doneda (2021) leciona que o consentimento do titular para o tratamento de seus dados pessoais representa um dos aspectos mais críticos da proteção de dados pessoais. Esse consentimento confere à pessoa o poder de alterar sua própria esfera jurídica com base na manifestação de sua vontade. Através dele, o direito civil tem a oportunidade de desenvolver uma estrutura que leve em consideração a autonomia da vontade, a circulação de dados e os direitos fundamentais, a fim de regular os efeitos desse consentimento de acordo com a natureza dos interesses envolvidos. O consentimento é sempre revogável, e sua caracterização como um ato jurídico unilateral reforça essa revogabilidade. A noção de revogabilidade incondicional está fundamentada na proteção da própria personalidade, da qual a indisponibilidade é um dos atributos.

A LGPD define **agentes de tratamento** como o controlador e o operador. **Controlador**, nos termos do inciso VI do art. 5º da LGPD, é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. **Operador**, por sua vez, é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, nos termos do inciso VII do art. 5º da LGPD (Brasil, 2018).

De acordo com o inciso VIII do art. 5º da LGPD, o **Encarregado** é a pessoa designada pelo controlador e operador para servir como intermediário e canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (Brasil, 2018). Conforme ensina Garrido (2023, p. 31), o "Encarregado também é chamado de *Data Protection Officer (DPO)* e pode ser tanto uma pessoa física como uma pessoa jurídica, atuando interna ou externamente, de forma individual ou em conjunto, como parte de um comitê".

Além disso, o art. 6º da LGPD faz previsão de que as atividades de tratamento de dados pessoais deverão observar a boa-fé e uma série de princípios. Nas palavras de Claudia Lima Marques (2019, RB-1.14), a boa-fé pode ser interpretada como:

> [...] uma atuação refletida, uma atuação refletindo, pensando no outro, no parceiro contratual, respeitando-o, respeitando os seus interesses legítimos, suas expectativas razoáveis, seus direitos, agindo com lealdade, sem abuso, sem obstrução, sem causar lesão ou desvantagem excessiva, cooperando para atingir o bom fim das obrigações [...].

No Direito, de acordo com os ensinamentos de Martins (2014, p. 29), princípio é o fundamento, é a base que irá moldar e orientar as normas jurídicas. Os princípios inspiram, orientam, guiam e fundamentam a construção do ordenamento jurídico.

Nas palavras de Cíntia Rosa Pereira de Lima (2020, p. 81), a regulação sobre proteção de dados está fundamentada nos princípios, uma vez que eles podem ser adaptados com maior facilidade aos casos concretos, considerando os avanços tecnológicos. Esses princípios elucidam a razão de existir da lei de proteção de dados pessoais e facilitam a sua aplicação, embasando, inclusive, diversos direitos listados na legislação.

A Lei Geral de Proteção de Dados estabeleceu, no art. 6º, os seguintes princípios: 1º) finalidade; 2º) adequação; 3º) da necessidade; 4º) livre acesso; 5º) qualidade dos dados; 6º) transparência; 7º) segurança; 8º) prevenção; 9º) não discriminação; e 10º) princípio da responsabilização e prestação de contas. Todos eles têm o propósito de promover a proteção dos dados, a privacidade e os direitos dos titulares de dados pessoais (Brasil, 2018).

Dentre os princípios previstos na LGPD, destaca-se o princípio da finalidade, que, juntamente com o princípio da boa-fé e observado o consentimento, desempenha papéis essenciais no cumprimento das diretrizes estabelecidas pela referida legislação. De acordo com os ensinamentos de Claudia Lima Marques (2019, RB-6.1): “Não se exige mais que o consentimento seja apenas livre – exige-se que o consentimento seja refletido, oriundo de informações verídicas, baseado na oportunidade de conhecimento do conteúdo das obrigações que estão sendo assumidas.”

A inclusão dos princípios previstos no art. 6º reflete a importância de práticas éticas e transparentes por parte das organizações ao lidar com informações pessoais. De acordo com Bruno Miragem (2020a, p. RB-1.34), o princípio da finalidade é o ponto central da proteção de dados pessoais. O titular dos dados, ao consentir com o tratamento de suas informações pessoais, o faz para uma finalidade específica, que deve ser claramente determinada, expressa e legítima.

Na obtenção do consentimento, as finalidades devem ser informadas de maneira explícita, vinculando-se assim ao tratamento dos dados. Qualquer utilização de dados para finalidades diversas das consentidas torna a conduta de tratamento de dados ineficaz e ilícita, acarretando a devida responsabilização. Além disso, o consentimento assegura que os titulares dos dados tenham controle sobre como suas informações são utilizadas (Miragem, 2020b).

De acordo com Maimone (2022, p. 20), os princípios da adequação e da necessidade estão intimamente ligados ao princípio da finalidade. “O princípio da adequação trata da compatibilização do uso dos dados com a finalidade informada” e o “princípio da necessidade

consiste na limitação do uso do dado ao mínimo necessário para se atingir a finalidade desejada". A soma dos princípios da finalidade, da adequação e da necessidade resulta no denominado mínimo essencial, a menor quantidade necessária de dados pessoais para alcançar, de forma adequada, o fim pretendido (Maimone, 2022, p. 20).

Ao definir estes princípios, a Lei Geral de Proteção de Dados destaca a importância da responsabilidade por parte das organizações, promovendo a confiança e o respeito à privacidade dos indivíduos. A implementação eficaz desses princípios contribui para um ambiente de tratamento de dados pessoais mais seguro e em conformidade com os direitos dos titulares dos dados.

A Lei Geral de Proteção de Dados não somente definiu os princípios que regem a proteção de dados, mas também estabeleceu os direitos e garantias do titular dos dados pessoais. Conforme estabelecido no art. 18, uma série de direitos foi outorgada aos titulares de dados, que desempenham um papel fundamental na garantia da proteção de suas informações pessoais. De acordo com os ensinamentos de Cíntia Rosa Pereira de Lima (2020, p. 86), muitos dos direitos assegurados aos titulares de dados decorrem dos já mencionados princípios estipulados no art. 6º da LGPD.

Os direitos garantidos aos titulares de dados abrangem: o direito de confirmar a existência do tratamento, permitindo que os titulares tenham ciência de como seus dados estão sendo processados (art. 18, I, da LGPD: Direito à Informação); e o direito que proporciona aos titulares a capacidade de obter informações sobre quais dados pessoais estão sendo processados e para quais finalidades (art. 18, II, da LGPD: Direito de Acesso aos Dados) (Brasil, 2018).

Além disso, a Lei Geral de Proteção de Dados garante ao titular o direito de correção de dados incompletos, imprecisos ou desatualizados (art. 18, III, da LGPD: Direito de Retificação). Outros direitos incluem o direito de bloquear ou eliminar dados desnecessários, excessivos ou processados em desconformidade com a lei, concedendo aos titulares controle sobre quais dados são retidos (art. 18, IV, da LGPD: Direito de Oposição e Cancelamento); o direito à transferência dos dados pessoais entre diferentes provedores de serviços (art. 18, V, da LGPD: Direito de Portabilidade dos Dados); bem como o direito à eliminação dos dados pessoais tratados com o consentimento do titular (art. 18, VI, da LGPD: Direito de Eliminação dos Dados Pessoais) (Brasil, 2018).

Adicionalmente, a LGPD impõe o direito à informação, o que significa que as organizações são obrigadas a fornecer informações claras e acessíveis sobre o tratamento de dados aos titulares (art. 18, VII, da LGPD: Direito à Informação). Por fim, os titulares têm o direito de revogar o consentimento a qualquer momento, garantindo que possam retirar sua

anuência para o tratamento de seus dados quando desejarem (art. 18, VIII, da LGPD: Direito ao Consentimento) (Brasil, 2018).

Consigna-se que o direito à informação decorre diretamente do princípio da transparência, pois obriga os agentes de tratamento de dados a informar a existência do mencionado tratamento (art. 18, I), bem como suas finalidades, compartilhamento de dados (art. 18, VII) e condições do consentimento e consequências de eventual negativa (art. 18, VIII) (Lima, 2020, p. 86).

Esses direitos, juntamente com os princípios estabelecidos e as sanções previstas, visam prevenir os riscos de violação à privacidade, como também frustrar tratamentos abusivos de informações e vazamento de dados (Viola; Teffé, 2023, p. 144). Visam ainda proporcionar uma proteção integral da pessoa humana ao consagrar a obrigatoriedade do gerenciamento seguro em todas as etapas do tratamento de dados pessoais, permitindo que o titular dos dados exerça maior controle sobre suas informações.

Na próxima seção, apresentam-se os projetos de lei em andamento que estabelecem o Marco Legal da Inteligência Artificial, bem como o anteprojeto de revisão e atualização do Código Civil, os quais preveem o fortalecimento da proteção de dados na legislação brasileira e estabelecem princípios e fundamentos para a proteção de dados e privacidade no ambiente digital.

2.4 PROJETO DE LEI DO MARCO LEGAL DA INTELIGÊNCIA ARTIFICIAL E O ANTEPROJETO DE LEI PARA REVISÃO E ATUALIZAÇÃO DO CÓDIGO CIVIL

Esta seção tem o propósito de apresentar dois projetos de lei relevantes: O Marco Legal da Inteligência Artificial e o anteprojeto de lei para revisão e atualização da Lei nº 10.406/2002, o Código Civil, ambos em tramitação nas casas legislativas. Expõem-se os fundamentos e objetivos dos projetos de lei e abordam-se as principiais implementações.

Destaca-se que os projetos têm como objetivo incorporar direitos relacionados à proteção de dados e privacidade no contexto digital, harmonizando a liberdade de informação com a garantia da segurança e privacidade dos usuários.

2.4.1 Projeto de Lei nº 2.338/2023 – Marco Legal da Inteligência Artificial

O Projeto de Lei (PL) nº 2.338, de 2023, Marco Legal da Inteligência Artificial (Senado Federal, 2023), visa regulamentar a Inteligência Artificial, estabelecendo normas gerais para

seu desenvolvimento, sua implementação e respectivo uso responsável no Brasil. Além disso, propõe prescrever direitos às pessoas eventualmente afetadas pela IA, com o objetivo de proteger os direitos fundamentais e garantir a instituição de sistemas seguros e confiáveis em benefício da pessoa humana, do regime democrático e do desenvolvimento científico e tecnológico (Senado Federal, 2023).

O referido projeto, em seu art. 2º, estabelece diversos fundamentos para o desenvolvimento de IA, como a centralidade da pessoa humana, o respeito aos direitos humanos, o desenvolvimento sustentável, a igualdade e a inovação, entre outros. Dentre esses, destacam-se a privacidade, a proteção de dados e a autodeterminação informativa. Além disso, a lei define, em seu art. 3º, os princípios a serem seguidos, como crescimento inclusivo, transparência, justiça e responsabilização (Senado Federal, 2023).

As pessoas afetadas por sistemas de IA têm direitos, incluindo direito à privacidade e à proteção de dados pessoais, direito à informação, explicação das decisões tomadas, contestação das decisões e solicitação de intervenção humana, nos termos do art. 5º do referido projeto de lei (Senado Federal, 2023).

O projeto de lei ainda estabelece, no art. 27, a responsabilidade civil do fornecedor ou operador de sistema de Inteligência Artificial que cause dano patrimonial, moral, individual ou coletivo, sendo obrigado a repará-lo integralmente, independentemente do grau de autonomia do sistema. Para sistemas de alto risco ou risco excessivo, a responsabilidade é objetiva, na medida da participação no dano, enquanto nos demais casos a culpa do agente é presumida, com inversão do ônus da prova em favor da vítima (Senado Federal, 2023).

Para casos de violação das regras, o projeto de lei prevê, na "Seção II Das Sanções Administrativas", dentre outras sanções, multa de até R$ 50 milhões por infração ou até 2% do faturamento da empresa ou conglomerado empresarial, visando garantir a proteção dos indivíduos e promover o uso ético e responsável da Inteligência Artificial. Além disso, o Projeto de Lei nº 2338/2023 complementa e fortalece as leis existentes de proteção de dados pessoais.

Em decorrência do recebimento das Emendas nº 5 e 6, de autoria do Senador Vanderlan Cardoso, no dia 23 de abril de 2024, a Comissão Temporária Interna sobre Inteligência Artificial no Brasil encaminhou o projeto para análise do Relator (Senado Federal, 2023). Em maio de 2024, o Senado estava examinando este projeto juntamente com outras nove propostas, incluindo o Projeto de Lei nº 21/2020, que estabelece princípios, direitos e deveres para o uso de inteligência artificial no Brasil e já foi aprovado pela Câmara dos Deputados.

Em 7 de julho de 2024, a Comissão Temporária Interna sobre Inteligência Artificial no Brasil recebeu do Senador Eduardo Gomes a Complementação de Voto, que conclui pela

aprovação do PL nº 2.338, de 2023; pela aprovação das Emendas n° 4, 8, 11, 13, 15, 16, 17, 18, 19, 35, 38, 44, 47, 49, 50, 52, 75, 86, 96, 108 e 125, pela aprovação parcial das Emendas n° 1, 3, 5, 7, 10, 22, 27, 34, 42, 43, 45, 46, 53, 84, 105, 106, 107, 114, 126 e 127; rejeição das demais, na forma do substitutivo consolidado; e pela declaração de prejudicialidade do PL nº 21, de 2020; PL nº 5.051, de 2019; PL nº 5.691, de 2019; PL nº 872, de 2021; PL nº 3.592, de 2023; PL nº 210, de 2024; e PL nº 266, de 2024 (Senado Federal, 2023).

2.4.2 Anteprojeto de Lei para revisão e atualização do Código Civil

A seguir, analisa-se o projeto de revisão e atualização do Código Civil, com foco nos aspectos relacionados à proteção de dados e à privacidade no ambiente digital, objeto desta dissertação.

Por meio do Ato do Presidente do Senado nº 11, de 2023, foi instituída uma Comissão de Juristas responsável pela revisão e atualização do Código Civil. Sob a presidência do Ministro Luiz Felipe Salomão, do Superior Tribunal de Justiça, a comissão iniciou seus trabalhos em 4 de setembro de 2023, tendo um prazo de 180 dias para a apresentação do relatório final.

O relatório final foi apresentado no dia 17 de abril de 2024, tendo como um de seus objetivos a criação do Direito Civil Digital. De acordo com o anteprojeto apresentado, o Direito Civil Digital fortalece a legislação atual de proteção de dados e a autonomia privada, além de procurar preservar a dignidade das pessoas, definindo direitos e proteções específicas no espaço virtual (Senado Federal, 2024).

O anteprojeto estabelece as bases do Direito Civil Digital ao trazer princípios, fundamentos e conceitos focados na proteção da dignidade, privacidade e propriedade no ambiente digital. Seus preceitos incluem o respeito à privacidade, à liberdade de expressão e à inviolabilidade, definindo direitos e proteções específicas para as pessoas no espaço virtual. O Direito Civil Digital aborda os diversos direitos das pessoas, tanto naturais quanto jurídicas, no ambiente digital, destacando a proteção de dados, a garantia dos direitos de personalidade e a liberdade de expressão. Trata da responsabilidade civil e dos critérios para aferir a licitude dos atos digitais, assegurando um ambiente digital seguro e transparente. Ressalta a importância de práticas de moderação de conteúdo que respeitem as liberdades individuais e a liberdade de expressão, com o objetivo de evitar danos (Senado Federal, 2024).

Adicionalmente, o anteprojeto detalha o conceito de patrimônio digital e estabelece diretrizes para a gestão e transmissão hereditária de ativos digitais, além de discutir tratamento

de dados e informações pessoais no contexto digital. Foca também na proteção integral de crianças e adolescentes no ambiente digital, exigindo que os provedores adotem medidas para garantir seu livre desenvolvimento dentro deste ambiente, o que inclui a verificação da idade dos usuários e a garantia do acesso a conteúdo apropriados, entre outros pontos.

A legislação ainda estipula diretrizes para o desenvolvimento e implementação de sistemas de Inteligência Artificial, enfatizando a não discriminação, a transparência e a responsabilidade civil, bem como a definição de regras para a criação de imagens de pessoas vivas e falecidas por meio de IA (Senado Federal, 2024).

Sobre os fundamentos do Direito Civil Digital, o anteprojeto de revisão do Código Civil define como princípios: Respeito à Privacidade e Proteção de Dados, enfatizando a proteção da privacidade e dos dados pessoais e patrimoniais, assegurando a autodeterminação informativa dos indivíduos; Liberdade de Expressão e Informação, que assegura a liberdade de expressão, informação, comunicação e opinião no ambiente digital, balanceando esses direitos com a proteção de dados pessoais e a privacidade; Inviolabilidade da Intimidade, protegendo a intimidade, a honra, a vida privada e a imagem das pessoas no ambiente digital; Desenvolvimento Tecnológico e Inovação, promovendo o desenvolvimento econômico, científico e tecnológico, garantindo a integridade e a privacidade mental, a liberdade cognitiva e a proteção contra práticas discriminatórias; e Inclusão Social e Igualdade, incentivando a inclusão social, a promoção da igualdade e a acessibilidade digital (Senado Federal, 2024).

No tocante aos Direitos das Pessoas no Ambiente Digital, o reconhecimento da identidade digital é fundamental, assegurando a proteção de dados pessoais conforme a legislação específica. Os direitos de personalidade são garantidos, incluindo a dignidade, a honra, a privacidade e o livre desenvolvimento. Além disso, é assegurado o acesso a mecanismos justos para composição e reparação integral dos danos em caso de violação de direitos no ambiente digital (Senado Federal, 2024).

A Exclusão de Dados Pessoais é um direito que permite que a pessoa solicite a remoção de dados pessoais e sensíveis que não tenham finalidade justificada ou sejam tratados ilegalmente. As condições para exclusão definem quais dados podem ser removidos e sob que circunstâncias. No campo dos Neurodireitos, a proteção é estabelecida como parte indissociável da personalidade, abrangendo a privacidade mental, a integridade mental e a liberdade cognitiva. Além disso, proíbe-se o uso coercitivo de neurotecnologias e assegura-se a proteção contra a manipulação não autorizada da atividade mental. A Identidade Digital é reconhecida oficialmente como meio de identificação no ambiente digital, emitida pelo Poder Público e

protegida por tecnologias de segurança. São estipulados altos padrões de segurança e inclusão, promovendo a inclusão digital para todos os cidadãos (Senado Federal, 2024).

Em relação à Transparência e Segurança no Ambiente Digital, é garantido a todos o direito a um ambiente digital seguro e confiável, fundamentado em princípios de transparência, boa-fé e prevenção de danos. As práticas de moderação de conteúdo devem respeitar a não discriminação e a liberdade de expressão, oferecendo mecanismos eficazes de reclamação e reparação de danos. Além disso, os termos de uso transparentes das plataformas digitais devem ser claros e detalhar os processos de moderação e curadoria de conteúdo (Senado Federal, 2024).

A Proteção de Crianças e Adolescentes no Ambiente Digital é assegurada no Capítulo VI, em conformidade com o Estatuto da Criança e do Adolescente e o Código em questão. No quesito, os provedores de serviços digitais têm várias obrigações, incluindo a verificação de idade dos usuários para evitar o acesso a conteúdo inadequado; a provisão de meios para que pais e responsáveis possam exercer controle parental; a proteção de dados pessoais das crianças e adolescentes, conforme a Lei nº 13.709/2018 (LGPD); e o desenvolvimento de ambientes digitais que considerem os melhores interesses das crianças e adolescentes, desde a concepção até a utilização dos produtos e serviços, maximizando a proteção da privacidade e reduzindo a coleta e utilização de dados pessoais. Além disso, é necessário utilizar uma linguagem adequada à idade do público-alvo (Senado Federal, 2024).

No que tange à Inteligência Artificial, o desenvolvimento de sistemas deve respeitar os direitos de personalidade, assegurando a não discriminação, a transparência e governança, a acessibilidade e confiabilidade, bem como a responsabilidade civil. Pessoas que interagem com sistemas de IA têm direito à informação sobre essas interações e sobre os critérios de decisão automatizada que possam influenciar diretamente seus direitos ou interesses econômicos. A criação de imagens de pessoas, vivas ou falecidas, por IA é permitida para atividades lícitas, desde que haja consentimento informado obtido da pessoa ou de seus herdeiros legais e respeito à dignidade e ao legado da pessoa. Para o uso comercial, é necessária autorização prévia de cônjuges, herdeiros ou representantes legais (Senado Federal, 2024).

É possível observar que o projeto do Novo Código Civil tem como objetivo incorporar diversos direitos ao Código Civil, alguns dos quais já estão previstos em outras legislações. Destaca-se o direito de proteção de dados e informações pessoais em consonância com a legislação de proteção de dados pessoais atualmente vigente, bem como a garantia dos direitos de personalidade em todas as suas expressões, como a dignidade, a honra, a privacidade e o livre desenvolvimento.

Assim, o Direito Civil Digital busca equilibrar a liberdade de informação, a proteção de dados e a regulação adequada dos serviços disponibilizados nos ambientes digitais. No próximo capítulo, são discutidas as vulnerabilidades no tratamento dos dados pessoais na Internet das Coisas, abordando as violações de dados e dos direitos à privacidade e correlatos nesse contexto.

3 VULNERABILIDADES NO TRATAMENTO DOS DADOS PESSOAIS NA INTERNET DAS COISAS

De acordo com as análises apresentadas nos capítulos anteriores, a Internet das Coisas desempenha um papel fundamental ao revolucionar a interação entre os seres humanos. A interconexão de dispositivos inteligentes e sistemas automatizados na *IoT* oferece uma ampla gama de soluções destinadas a melhorar significativamente diferentes aspectos da vida humana, como saúde, segurança, mobilidade, sustentabilidade e inclusão social. Ao fornecer soluções tecnológicas voltadas para o aprimoramento da qualidade de vida, a *IoT* promove maior autonomia, segurança e bem-estar para os indivíduos.

No entanto, o uso de novas tecnologias pelas empresas implica a coleta massiva e invasiva de dados pessoais, a fim de compor perfis de consumo. Nesse cenário, tanto o Estado quanto o setor privado expõem os indivíduos a novos riscos, principalmente o da vigilância eletrônica. Esses riscos são exacerbados pelo uso de algoritmos avançados e pela capacidade de aprendizado de máquinas (Lucca; Martins, 2022).

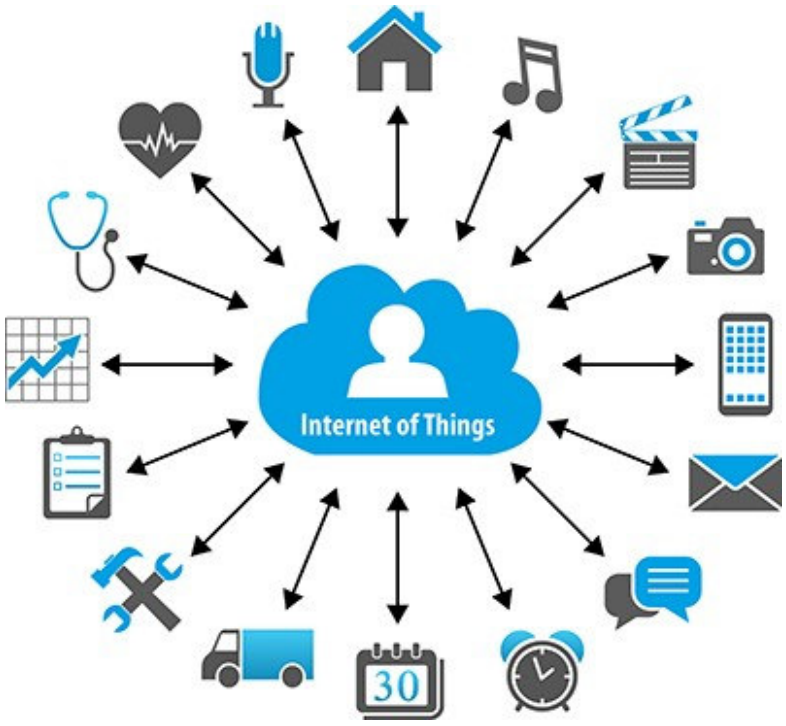
Assim, nas próximas seções demonstram-se a coleta de dados e o seu uso indevido, bem como as violações no tratamento desses dados e nos direitos à privacidade no ambiente da Internet das Coisas.

3.1 COLETA E USO INDEVIDO DE DADOS NO AMBIENTE DIGITAL

Nesta era informacional, os dados são frequentemente chamados de “novo petróleo” da Era Digital, pois são esses dados, transformados em informações, que impulsionam a economia atual, reduzem custos operacionais, aprimoram processos, aumentam eficiências de serviços relacionados à segurança pública, saúde, entre outros, além de contribuir para a melhoria das condições de vida humana. De acordo com Laura Schertel Mendes (2016), a informação tornou-se uma matéria-prima de produção e possui uma função tão significativa quanto os recursos humanos e os ativos financeiros.

Conforme ensinamentos de Newton De Lucca e Guilherme M. Martins (2022, p. 18), não é apenas a informação em si que possui valor significativo, mas principalmente o que é possível fazer com ela. A informação viabiliza diversas ações, desde estratégias de marketing até o sequenciamento de perfis, muitas vezes sem o conhecimento do titular dos dados, de forma que alcançar lucro pela utilização dessas informações torna-se inevitável.

Figura 2 – Coletando dados



Fonte: Lins (2015).

Nesse contexto, a Internet das Coisas desempenha um papel fundamental, pois, por meio de uma ampla gama de dispositivos de *IoT*, que incluem desde pequenos sensores e dispositivos vestíveis até grandes máquinas industriais, como *smartphones*, roupas inteligentes, *smartwatches,* automóveis, entre outros, os dados são coletados e armazenados (Almeida, 2019, p. 68).

Nas palavras de Belli (2023, p. 401), a Internet das Coisas é uma das tecnologias fundadas no tratamento de dados progressivamente mais volumosos e refinados, capazes de expandir o alcance da Internet no mundo físico, permitindo o monitoramento contínuo e onipresente dos objetos conectados e dos ambientes ao redor. Nesse cenário, a interconexão dos objetos pode ocasionar riscos à proteção da privacidade e dos dados pessoais dos indivíduos próximos a esses dispositivos, bem como à sua segurança e à segurança pública, caso os dispositivos sejam hackeados. Além disso, o fato de os dispositivos estarem permanentemente conectados a outros dispositivos, a aplicações diversas e à rede de comunicação, somado à possibilidade de serem controlados remotamente, afeta os indivíduos e o pleno gozo de suas liberdades e direitos fundamentais.

Para Alves *et al.* (2021, p. 101 - 102), a Internet das Coisas é amplamente fundamentada na integração de sensores do mundo real com a conectividade da Internet. Os sensores capturam dados do ambiente externo, os quais são combinados com dados armazenados na nuvem e submetidos a análises holísticas, resultando na geração de ações ou conselhos contextualizados. Na atualidade, existem sensores disponíveis que possuem capacidade para registrar praticamente todos os dados do ambiente. Alguns exemplos desses sensores são os de imagem, som, proximidade geográfica, temperatura, umidade, aceleração, pressão, presença de gases e batimentos cardíacos. Em um mundo onde os dados adquiriram um valor econômico significativo, o âmbito da Internet das Coisas tem se tornado cada vez mais comum com a presença de sensores que se configuram como uma ameaça legítima.

Essa diversidade de dispositivos permite que a *IoT* seja aplicada em diversos setores, como saúde, agricultura, transporte, cidades inteligentes, manufatura, entre outros (Almeida, 2019, p. 62), aumentando exponencialmente a quantidade de dados coletados e armazenados. Consequentemente, quanto maior a disponibilidade de dados, maior a capacidade do sistema em produzir resultados otimizados. Em contraste com sistemas dependentes de intervenção humana, a *IoT* é caracterizada pela sua operacionalidade ininterrupta, durante 24 horas por dia e 365 dias por ano, além de armazenar todos os dados coletados.

Como ensinam Morais *et al.* (2018, p. 15): "A coleta e o armazenamento de dados têm como finalidade a extração de informações que possam gerar vantagens competitivas para as organizações, bem como auxiliar nas tomadas de decisões". Para uma compreensão mais aprofundada do tema, é fundamental apresentar os conceitos de dados, informações e conhecimento. De acordo com Finoto e Museti (2023, p. 20),

> **Dado** pode ser interpretado como o aglomerado de números, letras, sinais que não foram decifrados, não tendo, assim, um significado concreto. Pode ser considerado os insumos para a produção de informações. As **informações** se referem ao conjunto de dados que foram interpretados e inseridos em um contexto, de modo a ganharem significado. Conhecimento, por sua vez, é a forma como as informações chegam e são captadas pelos indivíduos ou máquinas, sendo inseridas em um contexto. O **conhecimento** sofre reflexos das percepções pessoais dos que o adquirem, podendo ser interpretado da forma que melhor convém ao receptor.

A coleta de dados em sistemas *IoT* abrange diversas categorias. Em primeiro lugar, destacam-se os dados de saúde, que incluem histórico médico, informações genéticas e parâmetros biométricos, como frequência cardíaca e pressão arterial. Em seguida, há os dados de localização em tempo real, que fornecem informações sobre os deslocamentos e hábitos de uma pessoa, além de dados financeiros e de pagamento, como números de cartão de crédito e

informações bancárias. Outra categoria relevante compreende os dados de comportamento e preferências pessoais, que revelam informações sobre interesses, histórico de compras e atividades *online*. Também é importante considerar os dados de crianças, que requerem proteção especial devido à sua vulnerabilidade. Por fim, mencionam-se os dados relacionados a características pessoais protegidas por leis de privacidade já mencionadas, como origem racial ou étnica, crenças religiosas ou filosóficas e orientação sexual, os quais exigem cuidados específicos em sua coleta e armazenamento.

A coleta indiscriminada de informações em ambientes sensíveis, como residências inteligentes, as quais demandam proteção robusta de dados e mecanismos de controle de privacidade, é um exemplo característico. Por exemplo, é possível a coleta dos seguintes dados por meio de aplicações *IoT*:

> **Fechaduras inteligentes:** a que horas você geralmente está em casa; quem visita sua casa; em que horário; quanto tempo permanecem; **Geladeira inteligente:** o que você costuma comer; o horário das refeições; o que pode faltar em sua dieta; **Alto-falantes inteligentes:** como está o tempo na sua região; tópicos pesquisados; músicas que você ouve; conversas próximas ao alto-falante que podem ser gravadas acidentalmente; **Monitores de condicionamento físico:** suas atividades; seu estado de saúde; objetivos de condicionamento físico; locais e horários em que você se exercita; quando você vai dormir e quanto você dorme (Latto, 2019).

Outro exemplo apresentado por Burdova (2021) e Asher (2021) se refere às *Smart* TVs, que coletam uma ampla gama de dados enquanto os usuários assistem a programas de TV, filmes, streaming e jogam videogames, por meio do Reconhecimento Automático de Conteúdo (ACR). Essa tecnologia registra as preferências de visualização do usuário, cujos dados são posteriormente vendidos a anunciantes e empresas especializadas em análise de dados. Além do registro do conteúdo visualizado, essas TVs inteligentes também capturam informações demográficas, como idade, etnia, gênero e nível de educação. O endereço IP também é coletado, fornecendo detalhes sobre a localização e, possivelmente, a situação socioeconômica do usuário. A combinação desses dados cria um perfil detalhado do espectador, possibilitando seu reconhecimento em diferentes dispositivos, como *Smartphones* e computadores, a fim de permitir publicidade direcionada de produtos específicos, de acordo com o perfil do consumidor.

De acordo com Burdova (2021), as *Smart* TVs utilizam três principais métodos para coletar dados. O primeiro deles é a Tecnologia ACR, na qual a coleta de dados ocorre registrando o conteúdo visualizado, o que resulta na criação de um perfil de visualização com fins de marketing. Além disso, a coleta de dados também é efetuada por meio da câmera

embutida na *Smart* TV, que captura imagens sem o conhecimento ou consentimento do usuário. O terceiro método envolve o uso do microfone da *Smart* TV, por meio do qual a coleta de dados acontece através de áudio, permitindo que o microfone embutido no aparelho grave conversas e sons ao seu redor.

Com base nesses dados e na análise realizada, os dispositivos *IoT* podem tomar decisões automaticamente ou fornecer informações para que os usuários tomem decisões informadas (Almeida, 2019, p. 61).

Nesse sentido, conforme ensinamento de Almeida (2019, p. 60), a Internet das Coisas possibilita o controle remoto de dispositivos por meio da Internet, o que implica na possibilidade de gerenciar dispositivos *IoT*, utilizando um aplicativo em um dispositivo móvel, como *Smartphone*, *tablet* ou computador, independentemente da localização física. Por exemplo, é possível realizar ações como ativar ou desativar sistemas de iluminação, ajustar a temperatura de um termostato ou monitorar a segurança de uma residência ou uma empresa, sendo possível ainda o controle de robôs, esteiras, emissão de ordens de serviço, aquisição de matérias-primas e insumos.

A título de exemplos, podemos citar: a) um sistema de irrigação automatizado pode ajustar a quantidade de água fornecida às plantas com base nos dados de umidade do solo; b) um dispositivo de saúde *IoT* pode enviar alerta para os médicos com base nos dados vitais do paciente.

No entanto, a exposição dos dados pessoais coletados pode acarretar questões relacionadas à privacidade e segurança dos usuários. E apesar dos inúmeros benefícios resultantes da coleta e utilização de dados provenientes da Internet das Coisas, a coleta, o processamento e a utilização desproporcionais, injustificadas, inadequadas, abusivas e excessivas de dados pessoais, bem como condutas inadequadas, como a falta de consentimento adequado, o acesso não autorizado, o uso indevido por terceiros, o desvio de finalidade, a discriminação e a má-fé na manipulação desses dados, representam uma violação de direitos fundamentais. Essas práticas podem causar danos aos titulares das informações, comprometendo, assim, os benefícios proporcionados pela tecnologia.

Entre os eventuais danos causados aos titulares dos dados, destacam-se a perda de privacidade, a exposição vexatória de intimidades, a difamação da reputação, a exposição a riscos de segurança cibernética e fraudes financeiras, além da discriminação injusta, como será exposto a seguir.

Na próxima seção, demonstra-se como ocorrem as violações no tratamento dos dados pessoais no contexto da Internet das Coisas. Analisam-se diferentes formas de violação, como

a coleta inadequada de dados, o uso indevido das informações, o armazenamento inseguro, o acesso não autorizado e o compartilhamento não autorizado.

3.2 VIOLAÇÃO DE DADOS NA INTERNET DAS COISAS

Segundo a Comissão Europeia, uma violação de dados acontece quando uma empresa ou organização enfrenta um incidente de segurança que afeta os dados sob sua responsabilidade, resultando em uma quebra de confidencialidade, disponibilidade ou integridade desses dados. (Europa, 2023). Essa definição se alinha com a perspectiva da Autoridade Nacional de Proteção de Dados (ANPD) (Brasil, 2022b), que define um incidente de segurança com dados pessoais como sendo qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou ainda qualquer forma de tratamento de dados inadequada ou ilícita, que possa ocasionar risco para os direitos e as liberdades do titular dos dados pessoais. Essas definições refletem a gravidade das violações de dados e a importância de se proteger a privacidade e a segurança das informações pessoais.

Nesse contexto, a violação da proteção de dados na Internet das Coisas surge quando ocorre uma quebra de segurança ou uma infração das leis e regulamentos relacionados à proteção de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e as liberdades do titular dos dados pessoais (UFRJ, 2023).

Essa situação pode manifestar-se de várias formas, como acesso não autorizado, ataques de negação de serviço, desfiguração de *sites*, desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso, falta de consentimento adequado, falta de proteção adequada dos dados, falhas de segurança nos dispositivos ou na infraestrutura de rede, modificações em um sistema sem conhecimento, instruções ou consentimento prévio do proprietário, retenção excessiva ou desnecessária de dados, sequestro de dados, uso inadequado, vazamento de dados, vírus e outros códigos maliciosos (UFRJ, 2023).

De acordo com a ANPD (2021), a violação por acesso não autorizado ocorre quando indivíduos não autorizados conseguem obter acesso aos dados coletados pela *IoT*. Essas violações de acesso podem surgir devido a lacunas na segurança dos dispositivos *IoT* ou a vulnerabilidades na rede que interconecta esses dispositivos.

Por outro lado, a violação por vazamento de dados acontece quando as informações coletadas são expostas ou divulgadas sem o consentimento dos envolvidos. Essas violações podem advir de falhas de segurança nos sistemas, invasões maliciosas ou compartilhamento inadequado de informações. As implicações para os titulares dos dados podem variar amplamente e incluir fraudes, tentativas de golpes, utilização inadequada dos dados e comercialização das informações[13] (Brasil, 2021b).

Além disso, a violação por uso inadequado ocorre quando os dados coletados são empregados para propósitos diferentes dos autorizados pelos indivíduos ou sem a obtenção do consentimento adequado. Tal situação pode resultar em sérias implicações, como violações de privacidade e manipulação de informações pessoais (DocuSign, 2023).

Por sua vez, as violações por falhas de segurança nos dispositivos ou na infraestrutura de rede se materializam quando os dispositivos *IoT* apresentam vulnerabilidades ou quando a rede que interconecta esses dispositivos não está devidamente protegida. Em tais situações, indivíduos mal-intencionados podem explorar essas fragilidades para acessar ou modificar os dados (DocuSign, 2023).

No tocante às violações por falta de proteção adequada dos dados, essas ocorrências acontecem quando medidas de segurança essenciais, como criptografia, controle de acesso e salvaguarda contra-ataques cibernéticos, não são aplicadas para assegurar os dados armazenados e transmitidos na *IoT*. Como resultado, a confidencialidade das informações fica comprometida (DocuSign, 2023).

As violações por retenção excessiva ou desnecessária de dados ocorrem quando os dados coletados são mantidos por um período mais prolongado do que o necessário, aumentando assim o risco de exposição. Prolongar a retenção além do requerido amplia a probabilidade de os dados serem alvo de violações ou de serem utilizados de maneira inadequada (DocuSign, 2023).

A falha por falta de consentimento adequado ocorre quando a coleta e o processamento de dados pessoais não são realizados com o assentimento apropriado dos indivíduos envolvidos, ressalvadas as hipóteses de dispensa do consentimento, previstas na Lei Geral de Proteção de Dados Pessoais. Isso envolve garantir que as pessoas sejam devidamente informadas sobre

[13] Um exemplo recente de violação de dados, atribuível a deficiências nas medidas de segurança, é o incidente relatado pelo Instituto Nacional do Seguro Social (INSS) em 24 de junho de 2024. Esse incidente resultou na exposição de dados de até 40 milhões de segurados. As informações comprometidas incluem dados cadastrais e tipos de benefícios, como aposentadorias e auxílios-doença, os quais foram acessados através de meios legítimos, porém sem o devido controle. Esta violação de dados não ocorreu exatamente no contexto da Internet das Coisas, mas sim no ambiente digital mais amplo (Cisoadvisor, 2024).

quais dados serão coletados e como serão usados. O consentimento obtido também deve ser genuíno, para finalidades determinadas e não deve ser baseado em informações enganosas (DocuSign, 2023).

Também ocorre violação quando há discriminação. Nesse sentido, Mendes, Mattiuzzo e Fujimoto (2023, p. 432, 440, 441) ensinam que, para que as discriminações sejam consideradas abusivas, é necessária uma análise acerca do abuso, e os critérios para a definição da abusividade devem seguir os princípios da LGPD, além dos princípios constitucionais sobre o tema.

A discriminação por abuso pode ser categorizada da seguinte forma: (i) discriminação por erro estatístico, que ocorre devido a imprecisão amostral, resultando em restrição de direitos, tratamento desigual e comparação com indivíduos que deveriam ser submetidos ao mesmo tratamento; (ii) discriminação pelo uso de dados sensíveis, que acontece quando, além de se utilizarem dados sensíveis, são destacadas características de grupos historicamente discriminados; (iii) discriminação por generalização injusta ou correlação abusiva, que ocorre por tratamento diferenciado de determinado grupo, sem considerar as características individuais, ou quando algumas pessoas são equivocadamente classificadas em certo grupo devido à aleatoriedade ou ausência de causalidade; e (iv) discriminação limitadora do exercício de direitos, vedada pela LGPD no seu art. 21, o qual estabelece que “os dados pessoais referentes ao exercício regular de direitos não podem ser utilizados em seu prejuízo”. Nesta situação, a problemática está entre a proibição da realização de um direito e a informação empregada (Mendes, Mattiuzzo e Fujimoto, 2023, p. 432, 440, 441).

De acordo com os ensinamentos de Laura Schertel Mendes (2016), o tratamento de dados pessoais cujo efeito é a discriminação do consumidor do mercado será considerado ilegítimo, por ferir não apenas o direito à proteção de dados, mas especialmente o princípio da igualdade, protegido constitucionalmente.

Nas próximas seções, são apresentados alguns exemplos de violações no tratamento de dados no contexto da Internet das Coisas. Esses casos foram selecionados considerando a natureza das violações, como coleta indevida de dados, uso inadequado de dados, armazenamento indevido e acesso não autorizado aos dados coletados, bem como violação por discriminação racial relacionada aos dados coletados. A abordagem desses exemplos reais destaca as vulnerabilidades e os desafios enfrentados por empresas e usuários em relação à segurança e à privacidade dos dados na *IoT*.

3.2.1 Concessionária do Metrô de São Paulo – Via Quatro

Um caso emblemático de coleta indevida e não consentida de dados pessoais ocorreu em 2018 com a Empresa Via Quatro, concessionária da Linha Amarela do Metrô de São Paulo. Nesse caso, a empresa utilizava indevidamente o sistema de câmeras de segurança, para captar imagens dos usuários com propósitos comerciais e publicitários, sem obter a autorização adequada dos indivíduos afetados:

> A 8ª Câmara de Direito Público do Tribunal de Justiça de São Paulo manteve a condenação da Via Quatro, concessionária da Linha Amarela do Metrô de São Paulo, por utilizar indevidamente o sistema de câmeras de segurança para captação de imagens de usuários com fins comerciais e publicitários. O órgão colegiado votou pelo aumento do valor do dano moral coletivo, que foi fixado em R$ 500 mil e será revertido para o Fundo de Defesa de Direitos Difusos (FDD). O Instituto Brasileiro de Defesa ao Consumidor (IDEC) moveu uma ação civil pública contra a Via Quatro, buscando proibir a coleta e o tratamento dos dados biométricos dos passageiros sem autorização prévia. O pedido visava impedir o uso de qualquer forma de identificação dos usuários da linha, além de requerer indenização pela utilização indevida de imagens e a fixação de dano moral coletivo. Em primeira instância, foi determinada a proibição do uso das imagens sem autorização, bem como a fixação de indenização por dano moral coletivo de R$ 100 mil. O relator do recurso, desembargador Antonio Celso Faria, classificou a conduta da empresa como reprovável e ofensiva à moral coletiva, ressaltando que é praticamente impossível calcular o número de passageiros que utilizam a plataforma da ré diariamente, fato que caracteriza o dano moral coletivo. Além disso, o julgador destacou que os passageiros dos trens da concessionária tiveram sua intimidade invadida com fins lucrativos, sem autorização e sem controle adequado sobre a captação de imagens. "À ré, na condição de concessionária de serviço público, incumbe arcar com o risco das atividades econômicas que explora, especialmente por envolver os direitos fundamentais à intimidade, à privacidade, à imagem e à honra dos usuários consumidores, o que não ocorreu", frisou o Tribunal de Justiça do Estado de São Paulo (São Paulo, 2023b).

Nessa situação, por meio da decisão judicial supramencionada, ficou evidenciada a violação da privacidade dos passageiros, que foi invadida com fins lucrativos, ocorrendo sem a devida autorização, sem explicitar o propósito da coleta dos dados e sem um controle apropriado sobre a captação de imagens. A conduta representa uma afronta aos direitos fundamentais, à intimidade, privacidade, imagem e honra dos usuários consumidores.

3.2.2 Empresa *Amazon*, Subsidiária *Ring* e a Assistente Virtual *Alexa*

No contexto da coleta, acesso e armazenamento de dados na Internet das Coisas, apresenta-se um caso recentemente reportado pelo jornal Estadão (2023), envolvendo a empresa norte-americana *Amazon*, sua subsidiária *Ring* e a assistente virtual *Alexa*.

Para melhor entendimento da violação de dados a ser apresentada, primeiramente se explica o funcionamento dos produtos da subsidiária *Ring e* da Assistente Virtual *Alexa.* Esses

produtos coletam e processam, de forma constante e abrangente, dados pessoais que incluem gravações de áudio, preferências do usuário e histórico de comandos.

3.2.2.1 Funcionamento dos produtos da subsidiária Ring

A *Ring*, uma subsidiária da *Amazon*, é uma empresa que oferece campainhas de vídeo e câmeras de segurança integradas a um aplicativo móvel. Seu sistema permite que os usuários tenham controle total sobre a segurança de suas residências. As campainhas de vídeo possibilitam que os usuários vejam e interajam com visitantes em tempo real, independentemente de estarem dentro ou fora de casa. Por meio do aplicativo móvel, eles podem visualizar as imagens em tempo real e até mesmo conversar com os visitantes por meio de áudio bidirecional (Machado, 2023).

Além disso, a *Ring* também oferece câmeras de segurança que fornecem vigilância constante do ambiente externo e interno. Essas câmeras estão equipadas com sensores de movimento e notificam os usuários sobre qualquer atividade suspeita detectada em torno de suas propriedades. Através do aplicativo móvel, os usuários podem receber alertas em tempo real sobre essas atividades, permitindo-lhes monitorar e responder a eventuais situações de risco ou intrusões não autorizadas (*Ring*, 2023).

A proposta da empresa *Ring* é fornecer aos usuários uma solução completa de segurança residencial, utilizando a tecnologia de vídeo e a conectividade móvel para oferecer uma experiência de vigilância inteligente e conveniente. Essa integração entre campainhas de vídeo e câmeras de segurança, combinada com a capacidade de controlar tudo por meio do aplicativo móvel, oferece aos usuários uma maior sensação de tranquilidade e proteção em relação à segurança de suas casas, mesmo quando estão ausentes.

3.2.2.2 Funcionamento da assistente virtual Alexa

Conforme o site XP Educação (2022), a assistente virtual *Alexa*, desenvolvida pela *Amazon*, é ativada por comandos de voz e oferece diversas funcionalidades inovadoras. Com base em processamento avançado de linguagem natural e Inteligência Artificial, a *Alexa* pode interpretar solicitações, fornecendo informações relevantes e resolvendo dúvidas. Além de

responder perguntas, a *Alexa* age como uma assistente pessoal multifuncional, auxiliando na gestão de compromissos, lembretes e listas de compras.

Outra característica importante da *Alexa* é sua capacidade de controlar dispositivos domésticos inteligentes, permitindo uma experiência de casa conectada e eficiente. Através de comandos de voz, é possível ajustar a iluminação, temperatura e operar dispositivos eletrônicos, tornando a rotina diária mais simples e confortável. Adicionalmente, a *Alexa* oferece a funcionalidade de realizar gravações de câmera, vídeos e áudios para segurança e monitoramento. Ao ativar o modo vigia (*Alexa Guard*), a assistente pode detectar sons suspeitos, como vidros quebrando ou alarmes de detectores de fumaça, e emitir alertas para os dispositivos conectados ao *Echo*.

A interação com a *Alexa* é feita por meio de dispositivos habilitados, como os alto-falantes *Echo* da *Amazon*, em que comandos simples permitem acessar recursos como informações climáticas, notícias, reprodução de música e audiolivros. Para iniciar a interação, basta utilizar a palavra de ativação padrão, como "*Alexa*", "*Amazon*" ou "*Echo*" (Machado, 2023).

3.2.2.3 Amazon – Violações de privacidade

Em 31 de maio de 2023, a *Amazon* chegou a um acordo com a Comissão Federal de Comércio (FTC)[14] para pagar uma multa de US$ 25 milhões, visando encerrar alegações de que a empresa violou uma lei de privacidade infantil e enganou os pais das crianças que foram gravadas pelo sistema. Essas alegações estão relacionadas à assistente de voz *Alexa*, que supostamente manteve por anos os dados de voz e localização das crianças gravados sem o devido consentimento dos responsáveis. Além disso, a *Amazon* também concordou em pagar US$ 5,8 milhões em reembolsos para clientes que foram supostamente afetados por violações de privacidade relacionadas à sua câmera de campainha, a *Ring* (Estadão, 2023).

Conforme veiculado pelo jornal Estadão (2023), a FTC alega também que terceiros, incluindo funcionários da *Amazon*, poderiam acessar os dados pessoais dos usuários e que a empresa manteve os dados das crianças para refinar seu algoritmo de reconhecimento de voz, a Inteligência Artificial por trás da *Alexa*, que alimenta o *Echo* e outros alto-falantes inteligentes. No que se refere à câmera *Ring*, a FTC alega que a subsidiária de câmeras de

[14] *A Federal Trade Comission* (FTC), Comissão Federal de Comércio, é a agência nacional de proteção ao consumidor norte-americana. Sua missão é proteger as pessoas de práticas enganosas e fraudulentas e promover a concorrência (Espanha, 2023).

segurança doméstica da *Amazon* permitiu o acesso de funcionários e contratantes aos vídeos privados dos consumidores, e implementou práticas de segurança negligentes, que possibilitaram que *hackers* assumissem o controle de algumas contas.

Além da multa imposta no caso envolvendo a assistente de voz *Alexa*, a proposta também inclui uma proibição à *Amazon* de utilizar informações de voz e geolocalização, com o propósito de criar ou aprimorar qualquer produto de dados. A ordem requer ainda que a *Amazon* estabeleça um programa de privacidade específico para o uso de informações de geolocalização.

O caso apresentado descreve como ocorrem as violações na coleta de dados, muitas vezes realizadas sem o conhecimento e o devido consentimento dos usuários, violando direitos de privacidade. Isso evidencia a falta de transparência das empresas em relação ao tratamento dos dados coletados e a importância de os usuários estarem cientes de como suas informações são utilizadas. A análise deste caso reforça a importância de entender os riscos associados ao uso de tecnologias conectadas e as medidas necessárias para mitigar esses riscos, garantindo a proteção dos direitos fundamentais dos indivíduos.

3.2.3 Violação por Discriminação Racial: Tecnologia de Reconhecimento Facial – Projeto *Smart* Sampa

No contexto de preocupações relacionadas à violação de tratamento de dados por discriminação racial, destaca-se o projeto "*Smart* Sampa", implementado na cidade de São Paulo em agosto de 2023. Conforme o site da Secretaria Especial de Comunicação (São Paulo, 2023a), esse projeto integra várias instituições, incluindo a Polícia Civil, Polícia Militar, Guarda Civil Metropolitana, Companhia Estadual de Trânsito, Companhia Paulista de Trens Metropolitanos, Metrô e SAMU, por meio de uma avançada e inteligente Central de Monitoramento, com o propósito de aprimorar a segurança pública na cidade.

O sistema inclui 20 mil câmeras inteligentes de segurança equipadas com tecnologia de biometria facial, permitindo o monitoramento em tempo real de incidentes. Há planos de serem instaladas 2,5 mil câmeras na região central da cidade e em áreas movimentadas. O sistema tem capacidade para até 40 mil câmeras, incluindo a integração de câmeras privadas (São Paulo, 2023a).

Contudo, a utilização em larga escala da tecnologia de reconhecimento facial enfrentou críticas e desafios legais devido a preocupações com discriminação racial e proteção de dados. A licitação do sistema foi temporariamente suspensa para abordar essas preocupações,

retomando posteriormente com modificações no edital. Em maio, uma liminar suspendeu novamente o processo devido a preocupações com a proteção de dados e o risco de perpetuação do racismo estrutural (São Paulo, 2023b).

Apesar das controvérsias, o Tribunal de Justiça do Estado de São Paulo revogou a proibição, e o prefeito da capital paulista, Ricardo Nunes, enfatizou a importância de um sistema rigoroso de controle e avaliação para garantir a proteção de dados e a segurança pública. O prefeito ainda detalhou os critérios para a utilização das imagens, destacando a necessidade de mais de 90% de similaridade na biometria facial e a ausência de transmissão automática às forças policiais em caso de detecção de procurados pela Justiça, ressaltando que todas as identificações suspeitas passarão pela análise de um comitê integrado à Controladoria Geral do Município antes de qualquer ação ser tomada (São Paulo, 2021).

Nesse exemplo, destaca-se a preocupação com a violação de tratamento de dados por discriminação racial, devido à captura em massa de biometria facial. A implementação do projeto "*Smart* Sampa" em São Paulo, com sua capacidade de monitoramento em larga escala por meio dessa tecnologia, tem intensificado debates sobre os riscos potenciais para a privacidade e os direitos individuais, especialmente em relação à comunidade racialmente discriminada. Embora o reconhecimento facial possa ser valioso para a segurança pública, seu uso generalizado traz desafios significativos relacionados à discriminação racial e à proteção de dados, o que pode resultar numa situação em que a comunidade se torne suscetível a potenciais abusos, seja por parte do governo ou do setor privado.

3.2.4 *Meta Platforms Inc - Facebook* Serviços *Online* do Brasil

Uma suposta violação de tratamento de dados no ambiente digital, em especial o compartilhamento de dados e a falta de consentimento adequado, envolve a empresa *Meta Platforms Inc.*, representada no Brasil pela *Facebook* Serviços *Online* do Brasil, controladora dos aplicativos *Facebook, Messenger, WhatsApp* e *Instagram*, entre outras empresas.

O Instituto Brasileiro de Defesa do Consumidor (IDEC) tomou conhecimento de que a Meta, a partir de 26 de junho de 2024, passaria a utilizar dados pessoais públicos de seus usuários, coletados nas plataformas *Facebook* e *Instagram*, para treinamento indefinido de tecnologias de Inteligência Artificial (IDEC, 2024a).

Os dados pessoais seriam coletados sem qualquer especificação de finalidade e sem o consentimento dos usuários. Diante desse fato, o IDEC (2024b) denunciou a situação aos órgãos governamentais e requisitou a abertura de processo administrativo para investigar a mudança

na Política de Privacidade do *Facebook* e *Instagram*.

Em síntese, o IDEC alega na denúncia que a conduta da Meta de compartilhar dados para treinar IA generativa é abusiva, destacando, entre outros argumentos, que: não houve qualquer comunicação por parte da Meta sobre a mudança em sua política de privacidade para seus usuários brasileiros; faltam transparência e informações adequadas na comunicação da mudança da política de privacidade; há manipulação abusiva para dificultar o exercício do direito à oposição; não houve consentimento prévio dos consumidores; há falta de finalidade clara e legítima, ou seja, vinculação a finalidades legítimas, específicas e explícitas; não há legítimo interesse; e a prática é desproporcional em relação aos seus usuários (IDEC, 2024b).

Além disso, o IDEC requer que a empresa se abstenha de utilizar dados pessoais para treinamento de ferramentas de inteligência artificial generativa sem prévio consentimento e que seja determinada a adequação ao tratamento regular dos dados, de modo que a política de privacidade cumpra com os princípios da finalidade, adequação, necessidade e transparência. Ademais, requer que a empresa cesse o treinamento de ferramentas de IA generativa com dados pessoais dos consumidores, permitindo-o apenas com consentimento expresso, livre e informado dos titulares, ou de maneira restrita para fins de segurança, proibindo a utilização dos dados em benefício de seus próprios negócios (IDEC, 2024b).

O Conselho Diretor da Autoridade Nacional de Proteção de Dados Pessoais (ANPD), ao analisar a denúncia, proferiu o Despacho Decisório nº 20/2024/PR/ANPD com medidas preventivas, com efeitos até posterior decisão daquela autoridade, para determinar a imediata suspensão no Brasil (Brasil, 2024):

> (i) da vigência da nova política de privacidade da empresa, no que toca à parte relativa ao uso de dados pessoais para fins de treinamento de sistemas de IA generativa;
> (ii) do tratamento de dados pessoais dos titulares para essa finalidade em todos os Produtos da Meta, inclusive de pessoas não usuárias de suas plataformas, sob pena de multa diária de R$ 50.000,00 (cinquenta mil reais) por dia de descumprimento, em virtude do risco iminente de dano grave e irreparável ou de difícil reparação aos direitos fundamentais dos titulares afetados.

Ao proferir a decisão, a ANPD considerou a Nota Técnica nº 27/2024/FIS/CGF/ANPD, SEI nº 0129769, que apresentou três potenciais irregularidades: “a) ausência de hipótese legal adequada para a realização do tratamento; (b) falta de transparência na divulgação das novas informações aos titulares; e (c) limitação ao exercício de direitos dos titulares.” Além destas, no decorrer do voto 11, foi indicada a existência de outra suposta irregularidade, relativa ao (d)

tratamento de dados pessoais de crianças e adolescentes, em violação ao seu melhor interesse e sem as devidas salvaguardas (Brasil, 2024).

Em virtude da notificação, conforme informações obtidas nos sites governamentais, até 7 de julho de 2024, outros órgãos se manifestaram com pedidos de providências: o Conselho Administrativo de Defesa Econômica (CADE) instaurou um Procedimento Preparatório para que a Meta explique os questionamentos; a Secretaria Nacional do Consumidor (SENACON) solicitou esclarecimentos, exigindo que a Meta apresente: "a) O uso de dados de consumidores para treinamento de inteligência artificial; b) O propósito desse uso; c) O impacto do treinamento de IA nos consumidores; d) A política de informação adotada para o uso de dados; e) A existência de um canal de atendimento que facilite o exercício dos direitos dos consumidores" (IDEC, 2024c).

A SENACON ainda solicitou que a Meta comprove que sua política de privacidade cumpre com os princípios da finalidade, adequação, necessidade e transparência, indicando as bases legais aplicáveis para cada finalidade e os tipos de dados pessoais necessários. Além disso, o Ministério Público de Santa Catarina ingressou com uma ação civil pública contra a Meta para que a empresa paralise o treinamento de IA até que esteja de acordo com as leis brasileiras (IDEC, 2024c).

Nesse caso, supostamente ocorreram violações nos tratamentos de dados no ambiente digital, por provável infração à Lei Geral de Proteção de Dados Pessoais e a outras legislações relacionadas, como o Código de Defesa do Consumidor. As principais irregularidades identificadas incluem a falta de consentimento adequado dos titulares dos dados, falta de transparência, ausência de legítimo interesse por parte da empresa *Meta Platforms Inc.*, e a inadequação às finalidades declaradas para o uso dos dados pessoais coletados. Essas irregularidades, se confirmadas, comprometem os direitos dos consumidores e potencialmente violam princípios fundamentais de proteção de dados.

3.3 VIOLAÇÃO DO DIREITO À PRIVACIDADE NA INTERNET DAS COISAS

Conforme mencionado na seção 2.2, "Privacidade no Ambiente Digital – Conceitos e Características", a privacidade, que pode ser definida como o direito personalíssimo atribuído a toda pessoa de manter certos momentos, aspectos e dados relacionados à própria vida ao abrigo de invasões e divulgações não autorizadas, é considerada um direito fundamental, prevista no inciso X do art. 5º da Constituição Federal de 1988 e no Código Civil, no rol de Direitos da Personalidade e na Lei Geral de Proteção de Dados, inclusive estabelecendo que o

direito à privacidade deve ser observado desde a concepção do produto ou do serviço até a sua execução (art. 46 da LGPD).

O direito à privacidade abrange diversos aspectos, incluindo os direitos à intimidade, à honra, à imagem, à inviolabilidade do domicílio, ao sigilo de correspondência e das comunicações telegráficas, bem como à proteção dos dados das comunicações telefônicas. O art. 5º, X, da Constituição Federal de 1988 prescreve que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.

A violação do direito à intimidade na Internet das Coisas se manifesta através da invasão não autorizada da esfera íntima e pessoal dos usuários, mediante a coleta excessiva e não consentida de informações privadas, como hábitos, comportamentos e preferências, por meio de dispositivos conectados, expondo dados pessoais sensíveis sem o conhecimento ou permissão dos indivíduos afetados.

No que tange à violação do direito à honra na *IoT*, ela pode ocorrer por diversas vias. Uma delas é por meio do uso indevido de dados pessoais coletados por dispositivos conectados, expondo informações sensíveis, como opiniões, preferências políticas, orientações pessoais ou atividades privadas, sem consentimento do indivíduo. Ademais, a exposição não autorizada de informações pessoais em dispositivos *IoT*, como câmeras ou dispositivos de monitoramento, pode resultar em situações constrangedoras ou difamatórias. Ataques cibernéticos direcionados a dispositivos conectados também podem levar à divulgação de informações falsas ou comprometedoras sobre alguém, prejudicando sua reputação e honra.

Quando se trata da violação do direito à imagem na *IoT*, esta ocorre quando imagens pessoais são capturadas, armazenadas, divulgadas ou utilizadas sem o consentimento explícito da pessoa envolvida. Isso pode ser viabilizado por dispositivos como câmeras de vigilância, reconhecimento facial ou drones, que coletam imagens sem permissão. Além disso, a disseminação não autorizada de fotos ou vídeos em redes sociais, ou outros meios *online*, sem o consentimento da pessoa, também configura uma violação. A manipulação digital de imagens para criar conteúdo enganoso ou prejudicial à reputação de um indivíduo é outra forma de violação desse direito. Nesse sentido, ensina Viviane da Silva Coelho Vasques (2020, p. 255):

> A garantia de inviolabilidade à imagem significa impedir a utilização indevida e sem prévia autorização das características física ou projeção moral da pessoa em uma fotografia, filme, vídeo, entre outros. É direito da pessoa não ver sua imagem mercantilizada sem seu consentimento nem de ter a sua reputação atingida perante a sociedade.

A violação da inviolabilidade do domicílio na Internet das Coisas pode ocorrer por meio de dispositivos conectados que, de maneira não autorizada, invadem o espaço físico das pessoas. A presença de câmeras de vigilância, sensores e outros dispositivos inteligentes em residências ou locais de trabalho pode ser utilizada para monitorar e capturar dados sem o conhecimento ou consentimento dos moradores. Essa coleta indiscriminada de informações pessoais pode comprometer a privacidade e a segurança dos indivíduos, resultando em uma violação do direito à inviolabilidade do domicílio.

Além disso, vulnerabilidades na segurança desses dispositivos podem ensejar espaço para invasões cibernéticas, permitindo que terceiros acessem dados sensíveis e informações sobre o ambiente doméstico sem permissão. Caso situações como essas se verifiquem, poderão expor os moradores a potenciais ameaças, incluindo roubo de identidade, crimes cibernéticos e invasão da privacidade.

Nesse sentido, ensina Rosner (2016) que as atividades que envolvem informações de uma pessoa podem criar um risco maior de que a pessoa seja vítima de roubo de identidade ou fraude. Tais atividades aumentam as chances de a pessoa sofrer danos dignitários, bem como danos monetários ou físicos.

A inviolabilidade do domicílio é garantida pela Constituição Federal, no art. 5º, XI, ao estabelecer que a casa é asilo inviolável do indivíduo, não podendo ser violada sem o consentimento do morador, salvo em caso de flagrante delito ou desastre, ou por determinação judicial. Esse direito também é reforçado pelo Código Penal Brasileiro (Decreto-Lei nº 2.848/1940), em seu art. 150.

Quanto à violação do direito ao sigilo de correspondência e das comunicações telegráficas na *IoT*, essa pode ocorrer por meio de interceptação e monitoramento não autorizados das comunicações eletrônicas. Com o crescente uso de dispositivos conectados, como *Smartphones*, computadores e dispositivos de casa inteligente, há um aumento na troca de informações através de mensagens, e-mails, chamadas telefônicas e outras formas de comunicação digital. Contudo, caso essas comunicações não sejam adequadamente protegidas por medidas de segurança, podem estar sujeitas a interceptações e acessos indevidos por parte de terceiros mal-intencionados, violando o direito ao sigilo das comunicações. Ressalta-se que o sigilo de correspondência e das comunicações telegráficas é assegurado pelo art. 5º, XII, da Constituição Federal, que estabelece a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, exceto por ordem judicial, nas hipóteses e na forma que a lei estabelecer. Esse direito também é regulamentado pela Lei nº 9.296/1996, conhecida como Lei de Interceptação Telefônica.

No que concerne à violação do direito de proteção dos dados das comunicações telefônicas na *IoT*, essa também pode ocorrer de várias maneiras. Devido ao crescente uso de dispositivos conectados e aplicativos móveis, muitas informações pessoais e dados de comunicação são coletados, armazenados e compartilhados sem o devido consentimento dos usuários. Empresas e provedores de serviços podem coletar dados das chamadas telefônicas, como registros de chamadas, duração das ligações e até mesmo o conteúdo das conversas, sem que os usuários tenham ciência ou controle sobre essas práticas.

Existem ainda vulnerabilidades em aplicativos e redes que podem dar lugar para que terceiros não autorizados tenham acesso aos dados das comunicações telefônicas, comprometendo a privacidade e segurança dos usuários. A proteção dos dados das comunicações telefônicas é garantida pela Lei Geral de Telecomunicações (Lei nº 9.472/1997), que dispõe sobre a organização dos serviços de telecomunicações, estabelecendo normas para proteção e privacidade dos usuários desses serviços. Esses aspectos da privacidade são cruciais para preservar a dignidade e a segurança dos indivíduos em um cenário cada vez mais conectado e repleto de dispositivos inteligentes.

Na próxima seção, são discutidos os riscos inerentes ao tratamento de dados no contexto da Internet das Coisas, destacando-se os impactos para os indivíduos, as organizações e o ambiente econômico e social. Além disso, são apresentadas normas de segurança e prevenção aplicáveis a este contexto.

3.4 RISCOS SIGNIFICATIVOS PARA INDIVÍDUOS, ORGANIZAÇÕES E O AMBIENTE ECONÔMICO E SOCIAL - NORMAS DE SEGURANÇA E PREVENÇÃO

Conforme exposto ao longo da dissertação, o tratamento de dados pessoais, compreendido como toda operação realizada com esses dados, incluindo o tratamento abusivo, a proteção inadequada e o vazamento de dados, entre outras violações, pode trazer riscos à sociedade. Esses riscos decorrem da violação do direito à proteção de dados, bem como da violação dos direitos à privacidade, incluindo os direitos à intimidade, à honra, à imagem e à inviolabilidade do domicílio, e podem ser classificados como riscos para os indivíduos, para as organizações e para o ambiente econômico e social.

Entre os riscos para os titulares dos dados, destacam-se a exposição da privacidade e intimidade (dano reputacional), o roubo de identidade, a fraude financeira e a discriminação (Palhares; Prado; Vidigal, 2021, p. RB-5.71). A exposição da privacidade pode levar ao uso indevido de informações pessoais, enquanto o roubo de identidade e a fraude financeira podem

resultar em perdas econômicas significativas para as vítimas. A discriminação pode ocorrer quando dados pessoais são utilizados para excluir ou prejudicar indivíduos com base em características específicas, como etnia, gênero ou orientação sexual, acarretando prejuízos sociais e marginalização de grupos vulneráveis.

De acordo com os ensinamentos de Laura Schertel Mendes (2016), os riscos do tratamento de dados pessoais podem ser observados em diversos setores da sociedade, destacando-se os desafios apresentados nas relações de consumo. Os riscos da vigilância no mercado de consumo, resultantes do tratamento de dados, incluem a diminuição da autonomia do consumidor e o potencial para discriminação no mercado de consumo.

A autora complementa que a vigilância contínua dos comportamentos do consumidor por parte das empresas pode levar à perda de controle sobre suas informações que circulam na sociedade. Se o titular de dados não consegue determinar quais informações sobre si são conhecidas e utilizadas para a tomada de decisões que influenciam sua vida, sua capacidade de autodeterminação é reduzida. Em relação à discriminação, esta pode ocorrer caso lhe seja negado acesso a bens e serviços ou se suas oportunidades de vida forem diminuídas devido ao uso indiscriminado das informações armazenadas em bancos de dados (Mendes, 2016).

Para as organizações, os riscos decorrentes do tratamento inadequado de dados atingem principalmente a reputação das empresas. Empresas que não protegem adequadamente os dados de seus clientes podem sofrer danos significativos à sua reputação. A perda de confiança do consumidor pode resultar em uma diminuição de vendas e a perda de clientes. Adicionalmente, a reputação danificada pode dificultar a atração de novos negócios e parcerias. Necessário salientar que as empresas que não adotam medidas de segurança, conforme estipulado no art. 46[15] da Lei Geral de Proteção de Dados, ficam vulneráveis a ataques como: *Dumpster Diving:* obtenção de informações sensíveis descartadas inadequadamente, como documentos ou dispositivos eletrônicos; *Data Exfiltration:* remoção não autorizada de dados de um sistema ou rede por atacantes; *Shoulder Surfing:* observação direta ou indireta das informações digitadas ou exibidas em dispositivos eletrônicos; Engenharia Social: manipulação psicológica para obter informações confidenciais ou acesso a sistemas; *Spear Phishing:* e-mails fraudulentos personalizados para enganar indivíduos específicos e obter informações sensíveis; *Ransomware: malware* que criptografa dados e exige um resgate para liberar o acesso, entre

[15] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (Brasil, 2018).

outros (Donda, 2020, p. 98 - 103). Em todos esses tipos de ataques, os impactos podem levar a consequências financeiras significativas, danos à reputação, perda de confiança, sanções regulatórias e desafios legais, além de afetar a segurança e a privacidade dos indivíduos envolvidos.

Além disso, há as sanções legais e regulatórias, previstas nas leis que tratam sobre o tema, em especial no Capítulo VIII, da Fiscalização, Seção I, das Sanções Administrativas, da LGPD (Brasil, 2018), que impõem multas e outras sanções para organizações que não cumprem as normas de proteção de dados. As multas podem atingir valores expressivos, impactando financeiramente a empresa.

Há ainda custos de litígios, em decorrência de ações judiciais propostas pelos titulares dos dados contra a empresa, em razão da negligência na proteção de seus dados pessoais, resultando em custos legais significativos e possíveis indenizações. Nesse contexto, Ricardo Oliveira (2021) ensina: "a judicialização das demandas pode condenar o negócio à falência ou ao decréscimo significativo de desempenho." Além do mais, os processos judiciais podem trazer à tona práticas inadequadas de proteção de dados, exacerbando os danos reputacionais. Corroborando as informações acima, ensinam Hissa e Galamba (2019, p. RB-9.5) que "As consequências da não normatização e não adequação à LGPD são inúmeras: prejuízos à imagem e à reputação das empresas, além dos prejuízos financeiros, vez que haverá, além de multa, a publicização da infração e, em consequência, a perda de clientes e mercado."

De acordo com Fabio Correa Xavier (2021), o Relatório do Custo de uma Violação de Dados 2021 considerou quatro atividades relacionadas ao processo de identificação e mitigação de um incidente de segurança: **(I) detecção e escalonamento**, que envolve atividades forenses e de investigação, serviços de avaliação e auditoria, gerenciamento de crise e comunicação aos executivos e conselhos das organizações; **(II) perda de negócios**, que implica a perda de receita devido à indisponibilidade dos sistemas, custo da perda de clientes e da não aquisição de novos clientes; **(III) notificação**, que inclui atividades de notificação do incidente às autoridades e titulares dos dados; **(IV) custos de resposta após a violação**, que são medidas tomadas para reparação do incidente junto a autoridades de regulação e titulares, incluindo despesas legais, multas regulatórias, emissão de novos cartões, descontos em produtos e recuperação de imagem. Segundo o relatório, a **"perda de negócios"** é o maior custo de um incidente de segurança entre as quatro atividades, representando aproximadamente 38% do custo total.

Conforme o Relatório do Custo de uma Violação de Dados, produzido em 2023 em parceria entre o Instituto Ponemon e a IBM Security, em 2023 o custo médio de uma violação de dados no Brasil foi de US$ 1,22 milhões (IBM, 2023).

Também podem ser mencionados os riscos para o ambiente econômico e social, em consequência da erosão da confiança digital e do impacto na inovação. A proteção inadequada de dados pode levar a uma erosão geral da confiança no ambiente digital, afetando a disposição de indivíduos e empresas em utilizar serviços *online* e adotar novas tecnologias (Neotel, 2021).

Nos casos em que a proteção de dados envolve Infraestruturas Críticas Nacionais (ICN)[16], a inadequada proteção pode ter implicações para a segurança pública, expondo setores estratégicos a ataques cibernéticos, bem como trazendo transtornos e prejuízos ao Estado, à sociedade e ao meio ambiente. Tais infraestruturas incluem setores como energia, transporte e comunicações, em que a segurança dos dados é vital para a operação segura e contínua (Gimpel; Silva, 2024).

Assim, o tratamento e a proteção inadequada de dados pessoais no ambiente digital apresentam riscos significativos para indivíduos, organizações e o ambiente econômico e social. As legislações de proteção de dados, em especial a LGPD, visa mitigar esses riscos e garantir a proteção dos direitos fundamentais dos indivíduos, promovendo um ambiente digital mais seguro e respeitoso.

Nesse contexto, Frazão e Cueva (2022, p. RB-49.1) mencionam o que seja estar em conformidade:

> Estar em conformidade significa alterar toda a cultura da instituição no que tange ao tema, observando de forma específica os princípios da LGPD (especialmente a responsabilidade e a prestação de contas, a segurança, a prevenção, a transparência e a não discriminação), bem como capacitar todos os sujeitos para que atuem conforme as normas que apresentam relevância jurídica por força de lei ou contrato.
> A conformidade é caracterizada "pelo compromisso com a criação de um sistema complexo de políticas, de controles internos e de procedimentos, que demonstrem que a empresa está buscando 'garantir' que se mantenha em um estado de compliance."

Diante de possíveis riscos, a Lei Geral de Proteção de Dados impõe a adoção de medidas para diminuí-los ou eliminá-los, evitando sua materialização e os consequentes danos patrimoniais, morais, individuais ou coletivos. Assim, a LGPD estipula que os agentes de tratamento adotem medidas proativas para mitigar riscos, criando obrigações proporcionais ao grau de risco presente nas atividades de tratamento de dados. As obrigações previstas na lei incluem: o relatório de impacto à proteção de dados pessoais (art. 5º, XVII); a comunicação à ANPD e ao titular em caso de incidentes (art. 48, § 1º); o estabelecimento de boas práticas por

[16] Infraestruturas críticas nacionais referem-se a sistemas, instalações e serviços essenciais para o funcionamento de uma sociedade e a economia de um país. Essas infraestruturas são consideradas críticas devido à sua grande importância para a segurança, saúde, bem-estar e funcionamento contínuo de uma nação (Gimpel; Silva, 2024).

controladores e operadores (art. 50, § 1º); e o estabelecimento de políticas e salvaguardas adequadas (art. 50, § 2º, I, "d") (Palhares; Prado; Vidigal, 2021, p. RB-5.18).

A LGPD também adotou a aplicação do *Privacy by Design,* privacidade desde a concepção, que consiste na implementação de medidas preventivas desde os estágios iniciais das operações de tratamento de dados. Este conceito demanda uma postura proativa, focando na antecipação de eventos nocivos à privacidade (Palhares; Prado; Vidigal, 2021, p. RB-5.18).

Entre as normas de segurança[17] e prevenção[18] a serem adotadas, deve-se incluir a criptografia de dados, a instalação de *softwares* antivírus, políticas de senhas, a autenticação multifator, controle de acesso, além do monitoramento contínuo de sistemas e a criação de um plano de recuperação de desastre para não afetar as operações comerciais e a segurança (Donda, 2020, p. 65 a 74).

Devem ser realizados regularmente treinamentos e conscientização sobre proteção de dados com todos os funcionários, para assegurar que todos compreendam a importância e as práticas de segurança de dados. "Em sua maioria, os incidentes acontecem por conta do fator humano; por isso, o treinamento das pessoas é muito importante" (Kohls; Dutra; Welter, 2021, p. 157).

Auditorias regulares e avaliações de risco devem ser conduzidas para identificar e mitigar vulnerabilidades nos sistemas de informação (Donda, 2020, p. 76). Deve haver transparência[19] e comunicação clara com os titulares dos dados sobre como estes são coletados, usados e protegidos, fortalecendo a confiança e cumprindo os requisitos legais de consentimento informado. Além disso, devem ser estabelecidas políticas rigorosas de resposta a incidentes para lidar rapidamente com violações de dados, minimizando o impacto e prevenindo futuras ocorrências.

Nas palavras de José Fabio Rodrigues Maciel e Thaluana Alves da Penha (2023, p. 160), "a cultura de proteção de dados e governança caminham juntas, o que requer a incorporação de práticas seguras, capazes de evitarem riscos de exposições e, ao mesmo tempo, sanções administrativas."

---

[17] Art. 6º, VII, da LGPD: "segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;" (Brasil, 2018).

[18] Art. 6º, VIII, da LGPD: "prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;" (Brasil, 2018).

[19] Art. 6º, VI, da LGPD: "transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;" (Brasil, 2018).

Nas palavras de Calaza e Faleiros Júnior (2024), a regulação da Internet das Coisas apresenta grandes desafios. As características intrínsecas da *IoT*, especialmente a rapidez com que novas tecnologias são desenvolvidas, dificultam a criação de leis que acompanhem o cenário em tempo hábil. Além disso, a falta de padronização dos dispositivos pode complicar a formulação de normas aplicáveis a todos os produtos *IoT*. A criação de um ambiente colaborativo entre os diferentes atores envolvidos na produção e regulamentação dos dispositivos *IoT* também representa um desafio significativo, devido aos diversos interesses e perspectivas que precisam ser harmonizados.

Assim, as abordagens preventivas devem ser holísticas, integrando práticas de segurança robustas, transparência e colaboração entre todos os envolvidos para assegurar uma regulamentação eficaz e a proteção adequada dos dados pessoais.

CONCLUSÃO

Este estudo explorou os obstáculos relacionados à privacidade e à proteção de dados, especialmente no que tange à coleta e ao uso indevido, ou seja, no tratamento de dados pessoais advindos das Tecnologias da Informação e Comunicação, como a Internet das Coisas. Demonstrou-se a importância da proteção de dados pessoais na era da Sociedade da Informação, pois tais dados pessoais, transformados em informações, constituem o motor dessa era informacional.

Conforme explorado ao longo deste trabalho, a Internet e a Internet das Coisas modificaram significativamente o estilo de vida das pessoas, das organizações e da sociedade. A *IoT*, em conjunto com outras tecnologias, trouxe benefícios diretos aos seus usuários e à sociedade, permitindo a redução de custos, a otimização de processos e a maximização dos lucros para empresas. Os governos também se beneficiam com a tecnologia da *IoT*, melhorando processos, criando rotinas mais eficientes e tomando decisões mais assertivas com base nos dados coletados no ambiente da *IoT*.

No entanto, como demonstrado nos capítulos anteriores, todos esses benefícios vêm acompanhados de preocupações e riscos relacionados à proteção dos dados pessoais e à privacidade das pessoas. As consequências dos incidentes de violação de dados podem ser graves tanto para os usuários quanto para as empresas. Entre as consequências para os titulares dos dados estão os danos reputacionais, fraudes financeiras, discriminação e diminuição da autodeterminação. Para as empresas, as consequências incluem danos à reputação, perda de confiança, sanções regulatórias, multas e perdas financeiras. Há também riscos para o ambiente econômico e social, em decorrência da erosão da confiança digital e do impacto na inovação, além de riscos à segurança pública, especialmente quando a proteção de dados envolve infraestruturas críticas nacionais.

Esta dissertação explorou a Sociedade da Informação, a Internet, a *IoT*, as aplicações da *IoT* e os benefícios e riscos associados a essa tecnologia. Além disso, foram abordadas as legislações pertinentes à proteção de dados e à privacidade, com especial destaque para a Lei Geral de Proteção de Dados. A LGPD emerge como um marco regulatório essencial para assegurar a proteção dos direitos fundamentais de privacidade e proteção de dados pessoais, impondo normas rigorosas para a coleta, armazenamento e processamento de dados, e estabelecendo sanções para violações, complementando e fortalecendo o arcabouço legislativo sobre o tema.

A pesquisa destacou a necessidade de um equilíbrio entre inovação tecnológica e

proteção de dados. O avanço tecnológico, embora traga inúmeros benefícios, também aumenta a vulnerabilidade dos dados pessoais, exigindo uma regulamentação robusta e eficaz. A implementação de medidas de segurança cibernética, a conscientização dos usuários e a responsabilidade das empresas são fundamentais para mitigar os riscos associados à coleta e ao uso indevido de dados.

A dissertação sugeriu recomendações para melhorar a proteção de dados no ambiente digital. Entre elas, a adoção de melhores práticas de segurança por parte das empresas e a conscientização dos usuários sobre os riscos à privacidade. Empresas e governos têm a responsabilidade de implementar práticas robustas de proteção de dados, não apenas para cumprir com as legislações vigentes, como a LGPD, mas também para demonstrar um compromisso com a privacidade dos indivíduos.

O estudo concluiu que a proteção de dados pessoais é um imperativo na Sociedade da Informação. A privacidade e a segurança dos dados pessoais não são apenas questões técnicas, mas também são direitos humanos que devem ser preservados e protegidos. Em um mundo cada vez mais digitalizado e conectado, onde a coleta e o processamento de dados são constantes e onipresentes, a importância de salvaguardar esses direitos é fundamental para a manutenção da dignidade da pessoa humana.

Além disso, a proteção de dados pessoais é essencial para a confiança nas interações digitais. Usuários que se sentem seguros ao compartilhar seus dados estão mais propensos a participar de atividades *online*, contribuindo para o crescimento econômico e a inovação tecnológica. O desenvolvimento de uma cultura de privacidade é fundamental, incluindo a educação dos cidadãos sobre seus direitos de proteção de dados e sobre como proteger suas informações pessoais.

Também é necessário que as organizações adotem uma abordagem de privacidade por *design*, privacidade desde a concepção, integrando considerações de privacidade e segurança em todas as etapas do desenvolvimento de produtos e serviços. É importante ainda que as empresas e organizações adotem uma postura ativa de prevenção de danos, implementando medidas e padrões de qualidade e segurança adequados, com a finalidade de assegurar que a atividade de tratamento de dados seja realizada nos estritos limites legais.

Portanto, a proteção dos dados pessoais no ambiente digital, especificamente no contexto da Internet das Coisas, exige uma abordagem multifacetada que envolve avanços tecnológicos, regulamentações jurídicas eficazes, práticas empresariais responsáveis e uma cidadania digital informada. Somente esforços combinados em todos esses níveis garantem a privacidade e a segurança dos dados pessoais na era digital.

REFERÊNCIAS

ABES; IDC. **Estudo Mercado Brasileiro de Software: Panorama e Tendências 2024.** 2024. Disponível em: https://abes.com.br/dados-do-setor/. Acesso em: 28 jun. 2024.

AFONSO, Luiz Fernando. Internet e as Relações de Consumo: informação e responsabilidade. *In:* MARQUES, Claudia Lima; MIRAGEM, Bruno. **Diálogo das fontes**: novos estudos sobre a coordenação e aplicação das normas do direito brasileiro. São Paulo: Thomson Reuters Brasil, 2020.

ALECRIM, E.; MARQUES, A. **O que é *RFID*?** Saiba como funciona essa tecnologia de conexão. Tecnoblog, [*S.l.*], 2023. Disponível em: https://tecnoblog.net/responde/o-que-e-*RFID*-entenda-como-fun ciona-essa-tecnologia/. Acesso em: 2 de jun. de 2023.

ALMEIDA, P. S. **Indústria 4.0**: princípios básicos, aplicabilidade e implantação na área industrial. 1. Ed. São Paulo: Saraiva, 2019. Disponível em: https://integrada.minhabiblIoteca.com.br/#/books/9788536530451/. Acesso em: 11 jun. 2023.

ALVES, D. *et al.* **Internet das Coisas (*IOT*)**: segurança e privacidade de dados pessoais. 1. ed. Rio de Janeiro: Alta Books, 2021. 256 p.

AMAZON, A. **AWS *IoT* para a residência conectada**. AWS, Washington, 2023. *Online*. Disponível em: https://aws.*Amazon*.com/pt/*IoT*/solutions/connected-home/. Acesso em: 11 ago. 2023.

ANPD – Autoridade Nacional de Proteção De Dados. **Cartilha de Segurança para Internet**. Brasília: ANPD – Fascículo – Proteção De Dados, 2021. Disponível em: https://cartilha.cert.br/fasciculos/protecao-de-dados/fasciculo-protecao- de-dados.pdf. Acesso em: 12 ago. 2023.

ANPD – Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília: ANPD, 2021. Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 21 jan. 2024.

ARTIGO19; INTERNETLAB; LAPIN. **Cidades Inteligentes e Dados Pessoais: Recomendações e Boas Práticas.** São Paulo. 2022. *Online*. Disponível em: https://lapin.org.br/wp-content/uploads/2022/08/Cidades- Inteligentes-e-Dados-Pessoais-InternetLab-ARTIGO-19-e-LAPIN.pdf. Acesso em: 15 jul. 2023.

ASCENTY. **O que é conectividade?** Guia completo para empresas do futuro. 2024. Disponível em https://ascenty.com/blog/artigos/o-que-e-conectividade/#:~:text=Conectividade%20%C3%A9%20a%20capacidade%20de,locais%20e%20por%20diversos%20usu%C3%A1rios. Acesso em: 30 jun. 2024.

ASHER, C. **Será que sua *Smart* TV está te vigiando?** AVG, São Paulo, 2021. *Online*. Disponível em: https://www.avg.com/pt/signal/is-your-tv-watching-you. Acesso em: 21 jul. 2023.

ASHTON, K. *That "Internet of things" Things*. ***RFID Journal***, [*S.l.*], 2009. Disponível em: https://www.*RFID*journal.com/that-Internet-of-things-thing. Acesso em: 12 jun. 2023.

ASSESSORIA DE IMPRENSA. ***IoT*****:** 41,76 bilhões de dispositivos ativos conectados são previstos globalmente em 2023. Ind4.0, [S.l.], 2023. Disponível em: https://www.industria40.ind.br/noticias/23827-*IoT*-4176-bilhoes-dispositivos-ativos-conectados-na-previstos-globalmente-2023-diz-pesquisa. Acesso em 15 de jun. 2023

BARCELOS, M. S. **Um olhar no jornalismo do futuro a partir da Internet das Coisas (*IoT*) e Inteligência Artificial (AI)**: prospecções científicas e os desafios tecnológicos nas redações. 2019. 338 p. Tese (Doutorado em Jornalismo) - Universidade Federal de Santa Catarina, Florianópolis, 2019. Disponível em: https://repositorio.ufsc.br/handle/123456789/214828. Acesso em: 9 set. 2023.

BASSO, D. E. ***Big Data***. Curitiba: Contentus, 2020. Disponível em: https://plataforma.bvirtual.com.br/Leitor/Publicacao/186460/pdf/0?code=XPKzGFAZjXmh4xp7m8Xbla8Hs+Bbg5PZFzZqkYhNvB1KJV8apqGw6Xemp87AR4IQMinySRfRl/1kGtwmdgSvdA==. Acesso em: 29 jun. 2023.

BELLI, Lucas. Como implementar a LGPD por Meio da Avaliação de Impacto Sobre a Privacidade e Ética de Dados. *In:* DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR. Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de proteção de dados**. 3. ed. Rio de Janeiro: Forense, 2023, p. 393-422.

BELTRAMELLI NETO, Silvio; MELO, Maria Gabriela Vicente Henrique de. Quarta Revolução Industrial e os impactos da Era Digital na morfologia e na regulação do trabalho. **Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD)**, v. 14, n. 3, p. 539-558, set./dez., 2022. DOI: https://doi.org/10.4013/rechtd.2022.143.14. Disponível em: https://revistas.unisinos.br/index.php/RECHTD/article/view/21300. Acesso em: 27 maio 2024.

BNDES. **Estudo "Internet das Coisas: um plano de ação para o Brasil".** 2017. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-Internet-das-coisas-*IoT*/estudo-Internet-das-coisas-um-plano-de-acao-para-o-brasil. Acesso em: 18 maio 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/102ndia102árias102/102ndia102árias102.htm. Acesso em: 6 out. 2023.

BRASIL. **Decreto nº 9.854, de 25 de junho de 2019**. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. Brasília: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9854.htm. Acesso em: 5 set. 2023.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de

dados pessoais. Brasília: Presidência da República, 2022a. Disponível em: https://www12.senado.leg.br/noticias/materias/2022/02/10/promulgada-emenda-constitucional-de-protecao-de-dados. Acesso em: 30 de jul. 2023.

BRASIL. **Incidentes de segurança com dados pessoais**. Brasília, Autoridade Nacional de Proteção de Dados, 2022b. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/sema na-da-protecao-de-dados-2022/incidentes-de-seguranca-com-dados-pessoais. Acesso em: 12 set. 2023.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm#art118. Acesso em: 26 set. 2023.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011a**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 24 set. 2023.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011b**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 24 set. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 set. 2023.

BRASIL. **Lei nº 13.188, de 11 de novembro de 2015a**. Dispõe sobre o direito de resposta ou retificação do ofendido em matéria divulgada, publicada ou transmitida por veículo de comunicação social. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13188.htm. Acesso em: 12 abr. 2024.

BRASIL. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados. Conselho Diretor. **Despacho Decisório nº 20/2024/PR/ANPD.** Disponível em: https://www.in.gov.br/en/web/dou/-/despacho-decisorio-n-20/2024/pr/anpd-569297245. Acesso em: 7 jul. 2024.

BRASIL. Ministério das Relações Exteriores. **Brasil e Alemanha apresentam à ONU projeto de resolução sobre o direito à privacidade na Era Digital**. 1º nov. 2013. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/brasil-e-alemanha-apresentam-a-onu-projeto-de-resolucao-sobre-o-direito-a-privacidade-na-era-digital, Acesso em: 10 maio 2024.

BRASIL. **Promulgada emenda constitucional de proteção de dados**. Brasília: Senado Notícias, 2022c. Disponível em: https://www12.senado.leg.br/noti cias/103ndia103ár/2022/02/10/promulgada-emenda-constitucional-de-protecao-de-dados. Acesso em: 30 jul. 2023.

BRASIL. Superior Tribunal de Justiça. **Notícias**. Quarta Turma reafirma que direito de resposta não se confunde com publicação de sentença condenatória. 10 set. 2021a. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/10092021-Quarta-Turma-reafirma-que-direito-de-resposta-na-se-confunde-com-publicacao-de-sentenca-condenatoria.aspx#:~:text=Regulado%20atualmente%20pela%20Lei%2013.188,pela%20divulga%C3%A7%C3%A3o%20de%20not%C3%ADcia%20ofensiva. Acesso em: 9 abr. 2024.

BRASIL. Superior Tribunal de Justiça. **LGPD:** Um marco na regulamentação sobre dados pessoais no Brasil. 2020a. Disponível em: https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protecao-de-dados-pessoais-lgpd#:~:text=A. Acesso em: : 22 set. 2023.

BRASIL. Superior Tribunal de Justiça. **SÚMULA 550**: DIREITO DO CONSUMIDOR - SISTEMA CREDIT SCORING. Julgamento em 14 out. 2015b. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?pesquisaAmigavel=+%3Cb%3Ecredit+scoring%3C%2Fb%3E&b=SUMU&ordenacao=-%40NUM&numDocsPagina=10&i=1&O=&ref=&processo=&ementa=&materia=&situacao=&orgao=&data=&dtpb=&dtde=&operador=e&livre=credit+scoring. Acesso em: 24 maio 2024.

BRASIL. Supremo Tribunal Federal. **Referendo Na Medida Cautelar Na Ação Direta De Inconstitucionalidade 6.393/Distrito Federal.** Rel. Min. Rosa Weber. Julgamento: 7 maio 2020b. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358850. Acesso em: 21 jun. 2024.

BRASIL. **Vazamento de Dados.** Cartilha de Segurança para Internet. Brasília: ANPD – Fascículo, 2021b. Disponível em: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo- vazamento-de-dados.pdf. Acesso em: 12 ago. 2023.

BRASILEIRO, E. T. **Quarta Revolução Industrial e Direito do Trabalho**. Portugal: Grupo Almedina, 2022. Disponível em: https://integrada.minhabiblIoteca.com.br/reader/books/9786556276113/pageid/28. Acesso em: 10 set. 2023.

BURDOVA, C. Como impedir que sua *Smart* TV te espione. **Avast Academy**, [*S.l.*], 2021. *Online*. Disponível em: https://www.avast.com/pt-br/c-*Smart*-tv-spying-on-you. Acesso em: 21 jul. 2023.

CALAZA, Tales; FALEIROS JÚNIOR, José Luiz de Moura. Internet das Coisas e Generatividade: como tutelar os interesses coletivos sem limitar a inovação. *In:* SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio (Org.). **Proteção de dados:** temas controvertidos. Indaiatuba, SP: Foco, 2024. *E-book*. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 30 jun. 2024.

CARDOSO, Oscar Valente. **Inteligência artificial, direito e processo.** Belo Horizonte, MG: Dialética, 2024. *E-book*. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 07 jul. 2024.

CARREIRA, M. **8 Benefícios da Computação em Nuvem impacto e transformação digital**. Industria 4.0, [*S.l.*], 2022. *Online*. Disponível em: https://www.industria40.ind.br/artigo/22203-8-beneficios-computacao-nuvem-impacto-transformacao-digital. Acesso em: 1 ago. 2023.

CARSTENS, D. D. S.; FONSECA, E. **Gestão da Tecnologia e Inovação**. Curitiba: Intersaberes, 2019. Disponível em: https://plataforma.bvirtual.com.br/Leitor/Publicacao/173306/pdf/18?code=50puNd5YQnvcqmdcqQG8xGQrc17PH+Qs15UMfKUXukk1Jay2barFukFmjw/Ejl5m4ln9IjDxddgE1Qfx3u27jg==. Acesso em: 27 maio 2023.

CASTELLS, M. **A Galáxia da Internet**: Reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Editor Ltda, 2003.

CASTELLS, M. **A sociedade em Rede – A Era da Informação**: economia, sociedade e cultura. Trad. Roneide Venancio Majer. 6. ed. São Paulo: Paz e Terra, 1999. v. I.

CASTELLS, M. ***Communication Power***. *New York: Oxford University Press*, 2009.

CEARÁ. **A Lei do cadastro positivo e o código de defesa do consumidor**. Ceará: Ministério Público do Estado do Ceará, 2023. *Online*. Disponível em: http://www.mpce.mp.br/decon/duvidas/outras- duvidas/cadastro-positivo-de-consumidores/. Acesso em: 24 set. 2023.

CERTI. ***IIoT*****:** o que é e qual a importância para a Indústria 4.0. Certi, Florianópolis, 2023. *Online*. Disponível em: https://certi.org.br/blog/*IIoT*-o-que-e-e-qual-a-importancia-para-a-industria-4-0/. Acesso em: 16 set. 2023.

CHAVES, L. F. P.; VIDIGAL, P. **A LGPD revogou tacitamente dispositivos do Marco Civil da Internet**. Consultor Jurídico, Brasília, 2020. *Online*. Disponível em: https://www.conjur.com.br/2021-mar-29/chaves-vidigallgpd-revogou-tacitamente-dispositivos-mci. Acesso em: 24 set. 2023.

CISCO. A iniciativa Cidade inteligente de Barcelona orientada pela *IoT* reduz as contas de abastecimento de água, aumenta as receitas de estacionamento, cria empregos e muito mais. **Cisco**, [*S.l.*], 2014. *Online*. Disponível em: https://www.cisco.com/c/dam/m/pt_br/ioe/public_sector/pdfs/Jurisdictions/Barcelona_Jurisdiction_Profile_final.pdf. Acesso em: 5 jun. 2023.

CISOADVISOR. **INSS confirma exposição de dados de até 40 milhões de segurados.** 2024. Disponível em: https://www.cisoadvisor.com.br/inss-expos-dados-de-40-milhoes-de-segurados/ Acesso em: 24 jun. 2024.

CONHEÇA 3 Tecnologias que são tendências para a segurança pública. Byne, Florianópolis, 2023. Disponível em: https://www.byne.com.br/conheca-3-tecnologias-que-na-tendencias-para-a-seguranca-publica/. Acesso em: 17 set. 2023.

COSTA, Rosa Maria Cardoso Dalla. **História social dos meios de comunicação**. Curitiba: Intersaberes, 2020. Disponível em: https://plataforma.bvirtual.com.br/Leitor/Publicacao/

184989/pdf/0?code=xv4HD2/hJKhTH74Akq3Xswv3hBGteKGTPk2+lxDYhLxrRE/. Acesso em: 27 maio 2024.

CUNHA, H. **Internet das Coisas em favor da segurança**. Petrobrás Nossa Energia, [*S.l.*], 2019. Disponível em: https://nossaenergia.petrobras.com.br/energia/Internet-das-coisas-em-favor-da-seguranca/. Acesso em: 16 set. 2023.

CUNHA, J. I. C. D. **Usos das Tecnologias de Informação e Comunicação (TICs) nos circuitos curtos de comercialização de agricultores familiares**: o caso da rede Xique Xique de comercialização solidária no Rio Grande do Norte. 2022. 256 p. Tese (Doutorado em Sociologia) - Universidade Federal do Rio Grande do Sul. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/255660/ 001163866.pdf?sequence=1. Acesso em: 9 set. 2023.

DAVENPORT, T. H. ***Big Data*** **no trabalho**. Rio de Janeiro: Alta Books, 2014. Disponível em: https://integrada.minhabiblIoteca.com.br/reader/books/9786555206838/pageid/4. Acesso em: 31 jul. 2023.

DE LUCCA, Newton. MARTINS, Guilherme Magalhães**.** A Tutela Dos Dados Pessoais Sensíveis Na Lei Geral De Proteção De Dados. *In*: SCHREIBER, Anderson; MARTINS, Guilherme Magalhães; CARPENA, Heloisa (coord.). **Direitos fundamentais e sociedade tecnológica.** 1. ed. Indaiatuba, SP: Foco, 2022. *E-book*. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 1 jun. 2024.

DOCUSIGN. **O que são as violações de dados?** DocuSign, Califórnia, 2023. *Online*. Disponível em: https://www.docusign.com.br/blog/106ndia106ári-dados#:~:text=Os%20dados%20que%20ficam%20retidos,inviabilizar%20ª%20continuidade%20do%20neg%C3%B3cio. Acesso em: 18 set. 2023.

DONDA, Daniel. **Guia prático de implementação da LGPD**: conheça as estratégicas e soluções para adequar sua empresa em conformidade com a lei. São Paulo: Labrador, 2020. 144 p. Disponível em: https://plataforma.bvirtual.com.br/Leitor/ Publicacao/185745/pdf/0?code=mUOti0KdRoslIRAWOBbGs2BOELV/JfjeNdBR+ Acesso em: 22 jul. 2023.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. São Paulo: Revista dos Tribunais, 2021. Disponível em: https://next-proview-thomsonreuters-com.uninove.idm.oclc.org/launchapp/title/rt/monografias/215543393/v3/page/RB-2.5. Acessado em: 13 maio 2024.

DONEDA, Danilo. **Panorama Histórico da Proteção de dados Pessoais.** *In:* DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR. Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de proteção de dados.** 3. ed. Rio de Janeiro: Forense, 2023.

DONEDA, Danilo A. Proteção dos dados pessoais como um direito fundamental. **Revista Espaço Jurídico**, Espaço Jurídico Journal o Law, Editora Joaçaba, v. 12, n. 2, p. 91-108, 2011. Disponível em: https://periodicos.unoesc.edu.br/%20espacojuridico/article/view/1315/658, Acesso em: 5 ago. 2023.

ESPANHA. **Sobre a FTC**. Espanha: *Comisión Federal de Comercio*, 2023. Disponível em: https://www.ftc.gov/es. Acesso em: 22 jul. 2023.

ESTADÃO. *Amazon* pagará US$ 31 milhões por violação de privacidade causada pela assistente de voz *Alexa*. **Estadão**, São Paulo, maio 2023. Disponível em: https://www.estadao.com.br/link/*Amazon*-violacao-privacidade-multa-31-milhoes-*Alexa*-*Ring*-nprei/#:~:text=A%20*Amazon*%20concordou%20na%20quarta,gravados%20por%20seu%20popular%20assistente. Acesso em: 16 jul. 2023.

EUROPA. **O que é uma violação de dados e o que deve ser feito caso ocorra?** Comissão Europeia, [*S.l.*], 2023. *Online*. Disponível em: OqueÃľumaviolaÃğÃčodedadoseoquedeveserfeitocasoocorra? Acesso em: 21 jul. 2023.

FANTÁSTICO. Médicos operam coração de criança a 3 mil quilômetros de distância. **G1 Globo**, São Paulo, 2023. Disponível em: https://g1.globo.com/fantastico/noticia/2023/06/04/medicos-operam- coracao-de-crianca-a-3-mil-quilometros-de-distancia-video.ghtml. Acesso em: 6 jun. 2023.

FERNANDES, Gilberto L. Direito e ciência de dados: tendências e impactos da Quarta Revolução Industrial. *In*: PINTO, Henrique Alves; GUEDES, Jefferson Carús; CÉSAR, Joaquim Portes de Cerqueira (coord.). **Inteligência Artificial aplicada ao processo de tomada de decisões**. Belo Horizonte, São Paulo: D'Plácido, 2022.

FINOTO, L.; MUSETI, C. **O *Big Data* e a Lei Geral de Proteção de Dados**. São Paulo: Dialética, 2023.

FIORILLO, Celso A. P. **O Marco civil da internet e o meio ambiente digital na sociedade da informação** - Comentários à Lei n. 12.965/2014. 1. ed. São Paulo: Saraiva, 2015. [E-book]. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502627741/. Acesso em: 9 jul. 2024.

FIORILLO, C. A. P. **Princípios constitucionais do direito da Sociedade da Informação**: a tutelajurídica do meio ambiente digital. São Paulo: Saraiva, 2014. Disponível em: https://integrada.minhabiblIoteca.com.br/#/books/ 9788502230644/. Acesso em: 6 ago. 2023.

FOROUZAN, B. A.; MOSHARRAF, F. **Redes de Computadores**: uma abordagem Top-down. 1. ed. Porto Alegre: AMGH, 2013.

FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e Políticas de Proteção de Dados** Editora: Revista dos Tribunais, 2022. Disponível em: https://next-proview-thomsonreuters-com.uninove.idm.oclc.org/launchapp/title/rt/monografias/278686705/v1/page/RB-49.1%20 Acesso em: 2 de jun. 2024.

FRAZÃO, Ana. Fundamentos da Proteção dos Dados Pessoais – Noções Introdutórias para a Compreensão da Importância da Lei Geral de Proteção de Dados. *In:* TEPEDINO, Gustavo; OLIVA, Milena Donato; FRAZÃO, Ana. **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2020. Disponível em

https://next-proview-thomsonreuters-com.uninove.idm.oclc.org/launchapp/title/rt/monografias/195107452/v2/page/RB-1.2. Acesso em: 28 jun. 2024.

GAMBA, João Roberto Gorini. **Democracia e tecnologia:** impactos da quarta revolução industrial. Rio de Janeiro: Lumen Juris, 2020.

GARRIDO, P. P. **Proteção de dados pessoais**: comentários a Lei n.º 13.709/2018 (LGPD). 4. ed. São Paulo: Saraiva, 2023. Disponível em: https://integrada.minhabiblIoteca.com.br/#/books/9786555599480/. Acesso em: 5 ago. 2023.

GIMPEL, Matheus; SILVA, Tatiane. **A defesa cibernética e as infraestruturas críticas nacionais.** Cybersecurity, Publicações. 10 maio 2024. Disponível em https://bipbrasil.com.br/a-defesa-cibernetica-e-as-infraestruturas-criticas-nacionais/ Acesso em: 27 jun. 2024.

HISSA, C. B.; GALAMBA, P. H. do N. O impacto da LGPD na aplicação das normas de compliance. *In:* LIMA, Ana Paula M. Canto; HISSA, Carmina Bezerra; SALDANHA, Paloma Mendes (Coord.) **Direito Digital.** São Paulo: Editora Revista dos Tribunais, 2019. Disponível em: https://next-proview.thomsonreuters.com/launchapp/title/rt/monografias/202761861/v1/page/1. Acesso em: 26 jun. 2024.

IBGE – INSTITUTO BRASILEIRO DE ESTATÍSTICA E GEOGRAFIA. **Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal**. Rio de Janeiro: IBGE, 2021. Disponível em: https://bibl*IoT*eca.ibge.gov.br/visualizacao/livros/liv101963informativo.pdf. Acesso em: 8 set. 2023.

IBGE – INSTITUTO BRASILEIRO DE ESTATÍSTICA E GEOGRAFIA. **Em 2022, streaming estava presente em 43,4% dos domicílios com TV.** Agência de Notícias, Rio de Janeiro, 2022. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38306-em-2022-streaming-estava-presente-em-43-4-dos-domicilios-com-tv#:~:text=A%20Internet%20era%20utilizada%20em,que%20se%20aproxima%20da%20universaliza%C3%A7%C3%A3. Acesso em: 31 mar. 2024.

IBM. ***Security****: Cost of a Data Breach Report 2023*. 2023. Disponível em: https://www.ibm.com/account/reg/signup?formid=urx-52258. Acesso em: 27 jun. de 2024.

IDEALI, W. **Conectividade em Automação e *IoT***: protocolos I2C, SPI, USB, TCP-IP entre outros. Funcionalidade e interligação para automação e *IoT*. Rio de Janeiro: Alta Books, 2021. Disponível em: https://integrada.minhabiblIoteca.com.br/#/books/9786555202564. Acesso em: 10 set. 2023.

IDEC. **Idec notifica órgãos governamentais para que suspendam o uso de dados dos usuários para treinamento de IA pela Meta.** 2024a. Disponível em: https://idec.org.br/release/idec-notifica-orgaos-governamentais-para-que-suspendam-o-uso-de-dados-dos-usuarios-para. Acesso em: 7 jul. 2024.

IDEC. **Utilização compulsória de dados de consumidores para treinamento de inteligência artificial (IA) das plataformas da Meta.** 2024b. Disponível em: https://idec.org.br/sites/default/files/notificacao_idec_-_meta_ia_generativa_26.06.2024.pdf. Acesso em: 7 jul. 2024.

IDEC. **Idec atua contra o uso de dados pessoais de usuários em treinamento de IA da Meta**. 2024c. Disponível em: https://idec.org.br/release/idec-notifica-orgaos-governamentais-para-que-suspendam-o-uso-de-dados-dos-usuarios-para. Acesso em: 7 jul. 2024.

ITFORUM. **Internet das Coisas para gestão de ativos é a aposta da Infor para logística**. ItForum, [*S.l.*], 2018. *Online*. Disponível em: https://itforum.com.br/noticias/Internet-das-coisas-para-gestao- de-ativos-e-aposta-da-infor-para-logistica/. Acesso em : 16 set. 2023.

JACKSON, K. L.; GOESSLING, S. **Architecting Cloud Computing Solutions**. Birmingham: Packt Publishing, 2018. 378 p. Disponível em: https://learning-oreilly-com.uninove.idm.oclc.org/library/view/architecting-cloud-computing/9781788472425/073af6c1-e840-452ª-82c4-143fdab26e24.xhtml. Acesso em: 30 jun. 2023.

KOHLS, Cleize; DUTRA, Luiz Henrique; WELTER, Sandro. **LGPD**: da teoria à implementação nas empresas. 1. ed. São Paulo: Rideel, 2021. *E-book*. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 2 jun. 2024.

KUROSE, J.; ROSS, K. **Redes de Computadores e a Internet**: uma abordagem *top-down*. 5. Ed. São Paulo: *Pearson Education* do Brasil, 2009. 644 p.

LAUTERJUNG, Bruno. Brasil investiu quase 50 bilhões de dólares em tecnologia no último ano. **Tiinside.** 11 abr. 2024. Disponível em: https://tiinside.com.br/11/04/2024/brasil-investe-quase-50-bilhoes-de-dolares-em-tecnologia-no-ultimo-ano/. Acesso em: 27 jun. 2024.

LATTO, N. **O que é a Internet das Coisas (*IoT*)?** Avast Academy, [*S.l.*], 2019. *Online*. Disponível em: https://www.avast.com/pt-br/c-what-is-the-Internet-of-things. Acesso em: 21 jul. 2023.

LEMOS, Ronaldo; BRANCO, Sérgio. *PRIVACY BY DESIGN*: Conceito, Fundamentos e aplicabilidade na LGPD. *In:* DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de proteção de dados.** 3. ed. Rio de Janeiro: Forense, 2023. p. 449-460.

LIMA, C. R. P. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020. Disponível em: https://integrada.minhabiblIoteca.com.br/#/books/9788584936397/. Acesso em: 14 out. 2023.

LINS, T. Internet das Coisas: coletando dados na *IOT*. Laboratório Mobilis – UFOP, Ouro Preto, 2015. Disponível em: http://www2.decom.ufop.br/imobilis/*IoT*-coletando-dados/. Acesso em : 2 set. 2023.

LUCENA, André. **Há 10 anos, Edward Snowden revelou um mundo sitiado pela espionagem americana.** 6 jun. 2023. Disponível em:

https://www.cartacapital.com.br/mundo/ha-10-anos-edward-snowden-revelou-um-mundo-sitiado-pela-espionagem-americana/. Acesso em: 5 jul. 2024.

MACHADO, B. '*Alexa*, pagar multas': *Amazon* se prepara para autuações multimilionárias por violação de privacidade. **Multiverso notícias**, Goiânia, 2023. Disponível em: https://multiversonoticias.com.br/110ndia110ár-privacidade-*Amazon*-se-prepara-para-autuacoes-multi 110ndia110árias/. Acesso em: 22 jul. 2023.

MACIEL, José Fabio Rodrigues; PENHA, Thaluana Alves da Penha. Práticas ESG e o Tribunal de Contas do Município de São Paulo. *In:* TUMA, Eduardo (Coord.). **Função Social, Competência, ESG e Governança:** estudos de casos a partir do TCM-SP de acordo com a Lei n. 14.133, de 2021 (nova Lei de Licitações e Contratos Públicos)**.** Disponível em: https://integrada.minhabiblIoteca.com.br/#/books/9786556278995/. Acesso em: 8 jul. 2024.

MAGRANI, E. **A Internet das Coisas**. São Paulo: FGV, 2018.

MAGRANI, E. **Entre dados e robôs**: Ética e Privacidade na Era da Hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MAIMONE, F. H. C. P. **Responsabilidade Civil na LGPD**: Efetividade na Proteção de Dados Pessoais. Indaiatuba: Foco, 2022.

MALDONADO, Viviane. Nóbrega; BLUM, Renato. Opice. **Lei Geral de Proteção de Dados Pessoais comentada**. São Paulo: Revista dos Tribunais, 2022.

MARINELI, M. R. **Privacidade e Redes Sociais virtuais**: sob égide da lei 12.965/2014 – Marco Civil da Internet e da Lei 13.7039/2018 – Lei Geral de Proteção de Dados Pessoais. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MARQUES, Claudia Lima. **Contratos no Código de Defesa do Consumidor:** o novo regime das relações contratuais. 9. ed. São Paulo: Revista dos Tribunais, 2019.

MARTINS, S. P. **Instituições de Direito Público e Privado**. 14. ed. São Paulo: Saraiva, 2014. Acesso em: 14 set. 2023.

MASCHIETTO, L. G. *et al.* **Arquitetura e Infraestrutura de *IoT***. Porto Alegre: Grupo A, 2021.

MATTHIEU, C. Importance of Secure Cross-Protocol *IoT* Communications. **Citrix**, Fort Lauderdale, 2017. *Online*. Disponível em : https ://www.citrix.com/blogs/2017/02/28/importance-of-secure-cross- protocol–*IoT*-communications/. Acesso em: 11 jun. 2023.

MENDES, Laura Schertel, **A Vulnerabilidade do Consumidor quanto ao Tratamento de Dados Pessoais**: *In:* GSELL, Beate; MARQUES, Claudia Lima (Org.). São Paulo: Revista dos Tribunais - **Novas Tendências do Direito do Consumidor** – Rede Alemanha-Brasil de Pesquisas em Direito do Consumidor, 2016. Disponível em: https://next-proview.thomsonreuters.com/launchapp/title/rt/monografias/109619789/v1/document/110227747/anchor/a-110226895. Acesso em: 22 jun. 2024.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares. Proteção de Dados para Além do Consentimento: tendências de materialização. *In:* DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR. Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de proteção de dados.** 3. ed. Rio de Janeiro: Forense, 2023.

MENDES, Laura Schertel; MATTIUZZO, Marcela. FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à Luz da Lei Geral de Proteção de Dados. *In:* DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR. Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de proteção de dados.** 3. ed. Rio de Janeiro: Forense, 2023.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014 (Série IDP). Disponível em: https://integrada.minhabiblIoteca.com.br/#/books/9788502218987/. Acesso em: 30 jul. 2023.

MICHAELIS. **Dicionário Brasileiro da Língua Portuguesa**. 2023. *Online*. Disponível em: https://michaelis.uol.com.br/. Acesso em: 27 maio 2023.

MICROSOFT. Principais benefícios da Computação em Nuvem. **Azure**, [*S.l.*], 2023. *Online*. Disponível em: https://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/what-is-cloud-computing. Acesso em: 1º ago. 2023.

MIGLIOR, S. Tecnologias habilitadoras para cidades seguras. **Revista Segurança Eletrônica**, São Paulo, 2023. Disponível em: https://revistasegurancaeletronica.com.br/tecnologias-habilitadoras-para-cidades-seguras/. Acesso em: 17 set. 2023.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. *In*: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coord.). **Responsabilidade civil e novas tecnologias**. 1. ed. Indaiatuba: Foco, 2020b. *E-book*. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 09 jul. 2024.

MIRAGEM, Bruno. **Curso de Direito do Consumidor.** São Paulo: Revista dos Tribunais, 2020a. Disponível em: https://next-proview-thomsonreuters-com.uninove.idm.oclc.org/launchapp/title/rt/monografias/75937820/v8/page/RB-1.34. Acesso em: 9 jul. 2024.

MORAIS, I. S. de *et al.* **Introdução a *Big Data* e Internet das Coisas**. Porto Alegre: SAGAH, 2018. 167 p. Disponível em: https://integrada.minhabiblIoteca.com.br/reader/books/9788595027640/pageid/2. Acesso em: 26 maio 2023.

MUCELIN, Guilherme; **Diálogo das fontes e direito digital.** *In:* MARQUES, Claudia Lima; MIRAGEM, Bruno. **Diálogo das fontes**: novos estudos sobre a coordenação e aplicação das normas do direito brasileiro. São Paulo: Thomson Reuters Brasil, 2020.

NAZARENO, C.; PINHEIRO, G. P (org.). **Legislação sobre acesso à informação, proteção de dados pessoais e Internet**. 2. ed. Brasília: Câmara dos Deputados, 2021. Disponível em: https://livraria.camara.leg.br/LAI-2ed. Acesso em: 24 set. 2023.

NEOTEL. **Erosão da confiança digital**: os consumidores querem mais proteção de informações pessoais. 2021. Disponível em https://blog.neotel.com.br/sem-categoria/erosao-da-confianca-digital-os-consumidores-querem-mais-protecao-de-informacoes-pessoais/. Acesso em: 2 jun. 2024.

OLIVEIRA, Ricardo. **LGPD**: Como evitar as sanções administrativas. São Paulo: Saraiva, 2021. *E-book.* Disponível em: https://integrada.minhabiblIoteca.com.br/#/books/9786553623262/. Acesso em: 27 jun. 2024.

O QUE É A Internet das Coisas (*IoT*)? AWS, Washington, 2023. Disponível em: https://aws.*Amazon*.com/pt/what-is/*IoT*/. Acesso em: 24 set. 2023.

O QUE É O NIST Cybersecurity Framework? IBM, New York, 2023. Disponível em: https://www.ibm.com/br-pt/topics/nist Acesso em: 1º ago. 2023.

ORACLE. **O que é *IoT*?**. Oracle, Austin, 2022. Disponível em: https://www.oracle.com/br/Internet-of-things/what-is-*IoT*/. Acesso em: 16 set. 2023.

ORACLE. **Quais setores podem se beneficiar da *IoT*?** Oracle, Austin, 2023, *Online*. Disponível em: https://www.oracle.com/br/Internet-of-things/what-is-*IoT*/#industries-*IoT*. Acesso em: 16 set. 2023.

PALHARES, Felipe; PRADO, Luís Fernando; VIDIGAL, Paulo. **Compliance Digital e LGPD**. São Paulo: Editora: Thomson Reuters Brasil, 2021.

PALHOÇA. **Prefeitura de palhoça instala sensores em contentores de lixo**. Rede Cidade Digital, Palhoça, 2022. Disponível em: https://portalpalhoca.com.br/noticias/comunidade/prefeitura-de-palhoca-instala-sensores-em-contentores- de-lixo. Acesso: em 17 set. 2023.

PENTEADO, Andriele. **Interconexões:** educação e sociedade na Era Digital. São Paulo: Dialética, 2023.

PRIBERAM. **Dicionário Priberam da Língua Portuguesa**. 2008–2021. Disponível em: https://dicionario.priberam.org/metadados. Acesso em: 27/05/2023.

RAIS, Diogo (Coord.). **Fake News**: A conexão entre a desinformação e o direito. 3. ed. São Paulo: Thomson Reuters Brasil, 2022.

RING. 2023. Disponível em: https://latam-es.*Ring*.com/products/112ndia-doorbell-pro-2. Acesso em: 22 jul. 2023.

RIO DE JANEIRO. **Lei Estadual nº 824, de 28 de dezembro de 1984.** Assegura o direito de obtenção de informações pessoais contidas em banco de dados operando no Estado do Rio de Janeiro e dá outras providencias. Disponível em: http://alerjln1.alerj.rj.gov.br/CONTLEI.NSF/f25571cac4a61011032564fe0052c89c/664ba2b6d6098738032565600058805 5?OpenDocument. Acesso em: 15 mai. 2024.

RIO GRANDE DO SUL. Tribunal de Justiça do Rio Grande do Sul. **TJRS conclui migração do *eproc* para a Nuvem.** 27 maio 2024. Disponível em: https://www.tjrs.jus.br/novo/eproc/noticias/?idNoticia=138207. Acesso em: 30 jun. 2024.

RODRIGUES, Ricardo Batista. **Novas Tecnologias da Informação e da Comunicação**. Recife: IFPE, 2016. Disponível em: https://www.ufsm.br/app/uploads/sites/413/2018/12/arte_tecnologias_informacao_comunicacao.pdf. Acesso em: 9 maio 2024.

ROSNER, G. Privacy and the Internet *of things*. O'Reilly Media, Farnham, 2016. Disponível em: https://learning.oreilly.com/library/view/privacy-and-the/9781492042822/ch01ch02.html. Acesso em: 26 de jul. 2023.

ROUNTREE, D. ; CASTRILLO, I. **The basics of cloud computing** : understanding the fundamentals of cloud computing in theory and practice. 1. Ed. Amsterdam: Syngress na imprint of Elsevier, 2014.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O Direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados. *In:* DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR. Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de proteção de dados.** 3. ed. Rio de Janeiro: Forense, 2023.

SANTOS, Marcelo Henrique dos. **Introdução à Inteligência Artificial**. São Paulo: Saraiva, 2021. *E-book.* Disponível em: https://integrada.minhabiblIoteca.com.br/#/books/9786559031245/. Acesso em: 10 maio 2024.

SÃO PAULO. **Lei Estadual nº 5.702, de 5 de junho de 1987.** Concede ao cidadão o direito de acesso às informações nominais sobre sua pessoa. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/lei/1987/lei-5702-05.06.1987.html#:~:text=Artigo%201%C2%BA%20%2D%20Qualquer%20cidad%C3%A3o%20ter%C3%A1,Estado%2C%20inclusive%20em%20fich%C3%A1rios%20policiais. Acesso em: 15 maio 2024.

SÃO PAULO. **Prefeito assina contrato para o início do *Smart* Sampa, maior programa de videomonitoramento da cidade com até 40 mil câmeras**. São Paulo: Secretaria Especial de Comunicação, 2023a. *Online*. Disponível em: https://www.capital.sp.gov.br/noticia/prefeito-assina-contrato-para-o-inicio-do-*Smart*-sampa-maior-programa-de-videomonitoramento-da-cidade-com-ate-40-mil-cameras-2. Acesso em: 18 set. 2023.

SÃO PAULO. **TJSP mantém proibição de coleta de dados pela Via Quatro**. São Paulo: Tribunal de Justiça do Estado de São Paulo, 2023b. Disponível em: https://www.tjsp.jus.br/Noticias/Noticia?codigoNoticia=91605&pagina=1. Acesso em: 15 jul. 2023.

SÃO PAULO. Tribunal de Justiça de São Paulo (27ª Câmara de Direito Privado). **Apelação Cível 1000331-24.2021.8.26.0003**. Rel.: Des. Alfredo Attié. Julgamento em: 16 de novembro

de 2021. Disponível em: https://jurisprudencia.s3.amazonaws.com/TJ-SP/attachments/TJ-SP_AC_10003312420218260003_ea24e.pdf?AWSAccessKeyId=AKIARMMD5JEAO67SMCVA&Expires=1721239696&Signature=z1OppwXQYY%2FKpczF15jr2BZlYOQ%3D. Acesso em: 10 jun. 2024.

SAP. **O que é a Internet das Coisas Industrial (*IIoT*)?** SAP, [*S.l.*], 2023. *Online*. Disponível em: https://www.sap.com/brazil/products/scm/industry-4-0/what-is-*IIoT*.html. Acesso em: 17 set. 2023.

SARLET, Inglo Wolfgang. Fundamentos Constitucionais: o direito fundamental à proteção de dados. *In:* DONEDA. Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de proteção de dados.** 3. ed. Rio de Janeiro: Forense, 2023.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SENADO FEDERAL. **Projeto de Lei n° 2338, de 2023.** *Online*. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1714508324684&disposition=inline. Acesso em: 5 maio 2023.

SENADO FEDERAL. **Relatório Final dos trabalhos da Comissão de Juristas responsável pela revisão e atualização do Código Civil, 2024, Livro VI, do Direito Civil Digital.** *Online*. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento/download/68cc5c01-1f3e-491ª-836ª-7f376cfb95da. Acesso em: 17 maio 2024.

SILVA, J. J. **Casa Inteligente e Internet das Coisas (*IOT*)**: Sustentabilidade, Economia, Conforto e Segurança. São Paulo: kindle Literando, 2021.

SOLOVE, D. J. A Taxonomy of Privacy. **University of Pennsylvania Law Review**, Pennsylvania, v. 154, n. 477, 2006. Disponível em: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1376&context=penn_law_review. Acesso em: 29 de jul. 2023.

SOUSA NETO, M. V. **Computação em Nuvem**. Rio de Janeiro: Brasport, 2015. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 17 set. 2023.

SOUZA JUNIOR, E. Desmitificando a Internet das Coisas (*IoT*). **ItForum**, [*S.l.*], 2021. Disponível em: https://itforum.com.br/colunas/desmitificando-a-Internet-das-coisas-*IoT*-conceitos-basicos/. Acesso em: 4 jun. 2023.

TAKAHASHI, T (org.). **Sociedade da Informação no Brasil**: Livro Verde. Brasília: Ministério da Ciência e Tecnologia, 2000.

TAKASHI, V.; MORAES, A. de. **Segurança em *IoT***: Entendendo os riscos e ameaças em *IoT*. 1. Ed. Rio de Janeiro: Alta Books, 2021.

TAURION, C. ***Big Data***. Rio de Janeiro: Brasport, 2013.

TELEMEDICINA e Internet das Coisas conectam salas cirúrgicas para procedimentos cardíacos em crianças. **Portal Hospitais Brasil**, São Paulo, 2023. Disponível em: https://portalhospitaisbrasil.com.br/telemedicina-e-Internet-das-coisas-conectam-salas-cirurgicas-para-procedimentos-cardiacos-em-criancas/. Acesso em: 10 jun. 2023.

TELLES, A.; KOLBE JUNIOR, A. ***Smart IoT***: a revolução da Internet das Coisas para negócios inovadores. Curitiba: Intersaberes, 2022. 238 p. Disponível em: https://plataforma.bvirtual.com.br/Leitor/Publicacao/201652/pdf/0?code=O11UXHg9OcxqC+C+lvqqdbwqhEX+vwV+Eh7SgBXjN/GezkSh1Qac4JtMwkETbg12MeR1HXX1uCBam/voiS1ucA==. Acesso em: 10 jun. 2023.

UFRJ – UNIVERSIDADE FEDERAL DO RIO DE JANEIRO. **Incidentes de Segurança da Informação**. Security, Rio de Janeiro, 2023. *Online*. Disponível em: https://www.security.ufrj.br/denuncie-um-incidente/. Acesso em: 13 de ago. 2023.

VASQUES, V. S. C. Considerações sobre a proteção de dados pessoais sensíveis no ambiente virtual. *In*: LÓSSIO, C. J. B.; NASCIMENTO, L.; TREMEL, R (org.). **Cibernética Jurídica**: Estudos sobre Direito Digital. Campina Grande: EDUEPB, 2020, p. 252-261.

VIOLA, Mario Viola; TEFFÉ, Chiara Spadaccini. Tratamento de Dados Pessoais na LGPD: Estudos cobre as bases legais dos artigos 7º e 11. *In:* DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR. Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de proteção de dados.** 3. ed. Rio de Janeiro: Forense, 2023.

XAVIER: Fabio Correa. Custo de incidentes de segurança aumentam 10% em 2021 e alcançam o maior valor em 17 anos. 27 dez. 2021. **MIT Technology Review Brasil**. Disponível em: https://mittechreview.com.br/custo-de-incidentes-de-seguranca-aumentam-10-em-2021-e-alcancam-o-maior-valor-em-17-anos/#:~:text=Assim%2C%20em%202021%2C%20o%20custo,que%20a%20pesquisa%20%C3%A9%20realizada. Acesso em: 24 jun. 2024.

XP EDUCAÇÃO. Como funciona a *Alexa*? Tudo sobre a assistente de voz da *Amazon*. **Blog XP Educação**, [*S.l.*], 2022. Disponível em: https://blog.xpeducacao.com.br/como-funciona-*Alexa*/#:~:text=A%20*Alexa*%20funciona%20por%20meio,a%20*Alexa*%20processa%20ª%20solicita%C3%A7%C3%A3o. Acesso em: 22 jul. 2023.