**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS**
**ESCOLA POLITÉCNICA E DE ARTES**
**GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO**

# RESPONSABILIDADE CIVIL E PENAL DOS PROFISSIONAIS DE TI

PAULO HENRIQUE DE TOLEDO CARDOSO

GOIÂNIA
2025

PAULO HENRIQUE DE TOLEDO CARDOSO

# RESPONSABILIDADE CIVIL E PENAL DOS PROFISSIONAIS DE TI

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, como parte dos requisitos para obtenção do título de Bacharel em Engenharia de Computação.

Orientadora:
Profª. Dra. Solange da Silva

Banca Examinadora:
Profª. Ma. Mirian Sandra R. Gusmão,
Prof. Dr. Sibelius Lellis Vieira

GOIÂNIA
2025

PAULO HENRIQUE DE TOLEDO CARDOSO

**RESPONSABILIDADE CIVIL E PENAL DOS PROFISSIONAIS DE TI**

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Engenharia de Computação, em: 04/12/2025.

_____

Orientadora: Profª. Drª. Solange da Silva

_____

Examinadora: Profª. Ma. Mirian Sandra Rosa Gusmão

_____

Examinador: Prof. Dr Sibelius Lellis Vieira

GOIÂNIA

2025

## AGRADECIMENTOS

Primeiramente, expressar minha gratidão a Deus, por me abençoar com as oportunidades de cursar e concluir na Pontifícia Universidade Católica de Goiás os cursos de graduação em Engenharia Civil, Direito e Engenharia de Computação, conhecimento de grande relevância e importância.

Deixar um agradecimento especial à minha esposa Adma Toledo, grande incentivadora, que tanto somou com seu companheirismo e paciência.

Agradeço a nossos filhos, nossa família, minha razão, para ser diligente e determinado às graduações e pós graduações.

Agradeço de forma especial à minha orientadora, Professora Drª Solange, pela valiosa orientação, pelo rigor técnico e pela respeitável paciência, bem como à Profª. Ma. Mirian Sandra Rosa Gusmão e ao Professor Dr. Sibelius Lellis Vieira, pelas pertinentes e relevantes sugestões, que tanto contribuíram para o aprimoramento deste trabalho.

Aos muitos colegas e amigos, agradeço pela contribuição e parcerias produtivas.

Estendo minha gratidão aos professores que contribuíram significativamente para o meu crescimento acadêmico e pessoal.

Por fim, agradeço a todos que, direta ou indiretamente, fizeram parte deste processo. Este trabalho é o reflexo do esforço de todos aqueles que me apoiaram. A cada um de vocês agradeço terem feito parte dessa caminhada ricamente produtiva.

## RESUMO

O objetivo geral deste trabalho é identificar as responsabilidades civis e penais dos profissionais de TI. Ao longo do trabalho, buscou-se mapear os principais desafios enfrentados pelos profissionais da área, consequentes responsabilidades civis e penais, ante a observância de legislações como a Lei Federal n.º 13.709 – Lei Geral de Proteção de Dados LGPD, Lei Federal n.º 12.737 - Lei Carolina Dieckmann, Lei Federal n.º 12.965 – Marco Civil da Internet, Decreto-Lei Federal n.º 2.848 – Código Penal, Lei Federal n.º 10.406 – Código Civil. A pesquisa revelou que a inobservância do arcabouço legal inerente, redunda em penalidades severas, danos financeiros e impactos reputacionais, por vezes até irreversíveis para empresas e profissionais de TI. Diante disso, ficou evidente a importância de um *compliance* sólido e de políticas internas bem definidas para mitigar riscos. A implementação de boas práticas de segurança digital, aliada à capacitação contínua dos profissionais de TI, desponta como um fator crítico para garantir conformidade e minimizar impactos negativos de eventuais consequências jurídicas. Foi identificado a necessidade de implantação de uma cultura diligente de conformidade legal. Além disso, a análise jurisprudencial demonstrou que a interpretação da legislação atinente, tem se tornado cada vez mais rigorosa, reforçando a urgência da adequação às exigências jurídicas pertinentes. Portanto, conclui-se, portanto, que o papel do profissional de Tecnologia da Informação ultrapassa o domínio estritamente técnico e exige a internalização das responsabilidades civis e penais que permeiam o desenvolvimento e a operação de sistemas e serviços digitais. O êxito nessa atuação pressupõe não apenas o uso de soluções tecnológicas avançadas, mas também uma postura preventiva e estratégica, orientada pela legislação vigente, pela governança de dados e pelo *compliance* digital, de modo a assegurar conformidade normativa e sustentação jurídica à atividade profissional em TI.



Palavras Chaves: Tecnologia da Informação. Compliance. Aspectos Jurídicos. Profissional de TI.

**ABSTRACT**

The general objective of this work is to identify the civil and criminal liabilities of Information Technology (IT) professionals. Throughout the work, we sought to map the main challenges faced by professionals in the area, resulting civil and criminal liabilities, in view of compliance with legislation such as Federal Law No. 13,709 - General Data Protection Law LGPD, Federal Law No. 12,737 - Carolina Dieckmann Law, Federal Law No. 12,965 - Internet Civil Framework, Federal Decree-Law No. 2,848 - Penal Code, Federal Law No. 10,406 - Civil Code. The research revealed that failure to observe the inherent legal framework results in severe penalties, financial damages and reputational impacts, sometimes even irreversible for companies and IT professionals. In view of this, the importance of solid compliance and well-defined internal policies to mitigate risks became evident. The implementation of good digital security practices, combined with ongoing training of IT professionals, is emerging as a critical factor in ensuring compliance and minimizing the negative impacts of potential legal consequences. The need to implement a diligent culture of legal compliance was identified. In addition, the analysis of case law demonstrated that the interpretation of the relevant legislation has become increasingly rigorous, reinforcing the urgency of adapting to the relevant legal requirements. Therefore, It can be concluded, therefore, that the role of the Information Technology professional goes beyond the strictly technical domain and requires the internalization of the civil and criminal responsibilities that permeate the development and operation of digital systems and services. Success in this role presupposes not only the use of advanced technological solutions, but also a preventive and strategic approach, guided by current legislation, data governance, and digital compliance, in order to ensure regulatory conformity and legal support for professional activity in IT.

Keywords: Information Technology. Compliance. Legal Aspects. IT Professional.

## LISTA DE ABREVIATURAS E SIGLAS:

| | |
|---|---|
| ABNT | Associação Brasileira de Normas Técnicas |
| AES | Padrão Avançado de Criptografia |
| API | Interface de Programação de Aplicações |
| AJAX | *JavaScript* e *XML* Assíncronos |
| BYOD | Traga Seu Próprio Dispositivo |
| CC | Código Civil |
| CDC | Código de Defesa do Consumidor |
| CDN | Rede de Distribuição de Conteúdo |
| CERT | Equipe de Resposta a Incidentes de Segurança Cibernética |
| CGI.br | Comitê Gestor da Internet no Brasil |
| CI/CD | Integração Contínua / Entrega Contínua |
| CIO | Diretor de Tecnologia da Informação |
| CISO | Diretor de Segurança da Informação |
| CMS | Sistema de Gerenciamento de Conteúdo |
| CNJ | Conselho Nacional de Justiça |
| CP | Código Penal |
| CPP | Código de Processo Penal |
| CPC | Código de Processo Civil |
| CSS | Folhas de Estilo em Cascata |
| DLP | Prevenção contra Perda de Dados |
| DNS | Sistema de Nomes de Domínio |
| DPIA | Avaliação de Impacto sobre a Proteção de Dados |
| ERP | Planejamento de Recursos Empresariais |
| GDPR | Regulamento Geral de Proteção de Dados (União Europeia) |

| | |
|---|---|
| HTTP | Protocolo de Transferência de Hipertexto |
| IAM | Gerenciamento de Identidade e Acesso |
| ISO/IEC | Organização Internacional de Padronização |
| 27001 | Norma Internacional de Segurança da Informação |
| ITIL | Biblioteca de Infraestrutura de Tecnologia da Informação |
| JWT | *Token* da *Web* em *JSON* |
| LAN | Rede de Área Local |
| LGPD | Lei Geral de Proteção de Dados |
| MCI | Marco Civil da Internet |
| MFA | Autenticação Multifator |
| MP | Medida Provisória |
| NIST | Instituto Nacional de Padrões e Tecnologia (EUA) |
| PaaS | Plataforma como Serviço |
| REST | Transferência Representacional de Estado |
| SaaS | Software como Serviço |
| SDN | Rede Definida por Software |
| SIEM | Gerenciamento de Informações e Eventos de Segurança |
| SOC | Centro de Operações de Segurança |
| SPA | Aplicação de Página Única |
| STF | Supremo Tribunal Federal |
| STJ | Superior Tribunal de Justiça |
| TI | Tecnologia da Informação |
| VPN | Rede Privada Virtual |
| WWW | Rede Mundial de Computadores |

**SUMÁRIO**

## 1. INTRODUÇÃO:

Nas últimas décadas, observa-se uma mudança substancial na atuação profissional na área de Tecnologia da Informação (TI), marcada pela crescente centralidade dos dados e dos sistemas digitais nas relações sociais, econômicas e institucionais. Esse cenário foi acompanhado pela criação de leis federais que instituem princípios, parâmetros normativos e obrigações específicas para o tratamento de informações, incidindo diretamente sobre a prática profissional do especialista em TI.

A inobservância dessas normas não apenas compromete a segurança e a confiabilidade dos sistemas, como também pode acarretar severas consequências jurídicas, tanto na esfera civil quanto na penal, impactando indivíduos, organizações e o próprio Estado.

O tratamento rotineiro de grandes volumes de informações de pessoas físicas e jurídicas expõe o profissional de TI a um ambiente regulatório complexo, no qual decisões técnicas produzem efeitos jurídicos relevantes. Dados pessoais, registros sensíveis, códigos-fonte, bases de clientes, logs de acesso e conteúdos digitais, quando manipulados de forma inadequada, podem configurar violações a direitos de personalidade, à privacidade, à proteção de dados e à propriedade intelectual.

Nesse contexto, fenômenos como uso indevido de dados em campanhas direcionadas, ataques cibernéticos, vazamento de credenciais e fraudes digitais evidenciam que a dimensão ética e jurídica se tornou indissociável da atividade técnica em TI.

No âmbito da sociedade da informação, dados podem ser utilizados para alimentar sistemas de *machine learning*, otimizar processos por meio de soluções de *Big Data* ou sustentar modelos de negócio intensivos em informação. Ao mesmo tempo, o mesmo

ecossistema tecnológico permite práticas lesivas, como roubo de identidades, comercialização indevida de bases de dados, manipulação de reputações e cometimento de crimes cibernéticos.

Tal cenário reforça a necessidade de que o profissional de TI compreenda não apenas as arquiteturas técnicas e as boas práticas de segurança, mas também o arcabouço normativo que rege o tratamento de dados, o funcionamento da *internet* e a responsabilização civil e penal por condutas ilícitas no ambiente digital.

Justifica-se, portanto, o estudo do tema da responsabilidade civil e penal dos profissionais de TI, uma vez que esses agentes, ao desenvolverem sistemas, administrarem infraestruturas tecnológicas ou prestarem serviços especializados, estão diariamente expostos a riscos jurídicos e econômicos decorrentes de eventuais falhas técnicas, omissões ou decisões incompatíveis com a legislação vigente.

A pesquisa contribui para a conscientização e para a atuação mais diligente e respaldada dos profissionais da área, oferecendo-lhes uma visão integrada entre Engenharia de Computação, Métodologia Científica e Direito, alinhada às demandas contemporâneas de *compliance* digital, governança de dados e segurança da informação.

Diante desse contexto, este trabalho busca responder à seguinte questão de pesquisa: como o profissional de TI pode atuar, no exercício de suas atividades técnicas e empresariais, de forma a evitar falhas jurídicas que possam resultar em condenações civis e penais e em penalidades econômicas relevantes?

O objetivo geral consiste em identificar quais são os principais desafios jurídicos enfrentados pelos profissionais de TI e de que maneira eles podem estruturar sua prática para reduzir a exposição a riscos legais.

Os objetivos específicos, propõe-se:

a) A mapear os principais desafios legais relacionados à proteção de dados e à privacidade;
b) A investigar os riscos jurídicos associados ao desenvolvimento de *softwares*, aos contratos de tecnologia e à propriedade intelectual;
c) A analisar casos concretos de litígios envolvendo profissionais de TI, a fim de compreender os fatores que conduzem à responsabilização judicial;
d) A estudar os desafios inerentes à implementação de medidas de *compliance* digital e de segurança da informação nas organizações.

Quanto aos aspectos Métodológicos, trata-se de uma pesquisa de natureza exploratória e descritiva, desenvolvida por meio de procedimentos bibliográficos e documentais. São utilizados como fontes principais doutrina especializada, legislação (como a Lei Geral de Proteção de Dados, o Marco Civil da Internet, a Lei dos Crimes Cibernéticos, o Código Civil e o Código Penal), bem como decisões jurisprudenciais dos tribunais superiores, em especial do Superior Tribunal de Justiça (STJ) e do Supremo Tribunal Federal (STF).

A partir da revisão bibliográfica, da análise normativa e do exame de casos selecionados, procede-se à sistematização dos dados, permitindo a construção de uma base teórico-prática capaz de sustentar as reflexões desenvolvidas ao longo dos capítulos.

Esta monografia está organizada da seguinte maneira:

O **Capítulo 2** apresenta o referencial teórico, estruturado em conceitos e definições essenciais – tais como Tecnologia da Informação, desenvolvimento *web*, *Big Data*, segurança da informação, aspectos jurídicos da área de TI, proteção de dados, propriedade intelectual, responsabilidade civil e penal, contratos e acordos de nível de

serviço (SLAs) e *compliance* –, além de discutir trabalhos relacionados que situam o estado da arte na interface entre Direito e Tecnologia.

O **Capítulo 3** descreve o método de pesquisa, explicitando sua natureza exploratória e descritiva, os procedimentos bibliográficos e documentais adotados, as etapas de revisão da literatura, análise legislativa, levantamento jurisprudencial, estudos de caso e sistematização dos dados.

O **Capítulo 4** examina em profundidade a Lei Geral de Proteção de Dados (LGPD), abordando seu conceito, finalidade, âmbito de aplicação, princípios, bases legais, direitos dos titulares e responsabilidades dos agentes de tratamento, com especial atenção às implicações práticas para a atuação do profissional de TI.

O **Capítulo 5** trata do Marco Civil da Internet, contextualizando historicamente sua criação, apresentando seus princípios, direitos e garantias, bem como o regime de responsabilidade civil dos provedores e a interseção com a LGPD.

O **Capítulo 6** analisa a Lei dos Crimes Cibernéticos – Lei Carolina Dieckmann –, ressaltando o contexto histórico de sua aprovação, as principais alterações introduzidas no Código Penal, a tipificação da invasão de dispositivo informático, a interrupção de serviços telemáticos, a falsificação de cartões e os desafios investigativos contemporâneos.

O **Capítulo 7** discute as responsabilidades civis dos profissionais de TI, à luz dos fundamentos normativos da responsabilidade subjetiva e objetiva, da responsabilidade prevista na LGPD, das obrigações contratuais em serviços de tecnologia, dos seguros de riscos cibernéticos e das boas práticas de *compliance* voltadas à mitigação de danos.

O **Capítulo 8** aprofunda as responsabilidades penais dos profissionais de TI, examinando os pressupostos constitucionais e penais, os crimes informáticos tipificados, a responsabilidade do administrador de sistemas e do desenvolvedor de software, bem como as excludentes de ilicitude, a delegação de responsabilidades no contexto empresarial e o papel do *compliance* penal na redução de riscos.

O **Capítulo 9** apresenta e analisa decisões selecionadas do Superior Tribunal de Justiça em matéria de tecnologia da informação, contemplando temas como desenvolvimento *web* e direito autoral, LGPD, Marco Civil da Internet, Lei Carolina Dieckmann e responsabilidade civil e penal de agentes ligados à TI, com o intuito de evidenciar como o entendimento jurisprudencial tem se consolidado.

O **Capítulo 10** reúne as conclusões do trabalho, sintetizando os principais achados, indicando limitações e sugerindo possíveis desdobramentos para pesquisas futuras e para a prática profissional dos engenheiros da computação e demais profissionais de TI.

## 2. REFERENCIAL TEÓRICO:

Este capítulo é constituído de duas partes: uma refere-se aos Conceitos e Definições e a outra inerente aos Trabalhos Relacionados.

### 2.1. CONCEITOS E DEFINIÇÕES:

Este capítulo aborda os principais conceitos e definições, que norteiam as discussões que envolvem profissionais de TI e suas responsabilidades civis e penais.

### 2.1.1. Tecnologia da Informação:

A área de TI engloba o conjunto inter-relacionado de métodos, técnicas e instrumentos necessários e suficientes ao tratamento, armazenamento, processamento e disseminação de dados e informações. A área de TI compreende os recursos de hardware, software, redes de comunicação e processos operacionais que, de forma integrada, viabilizam o gerenciamento eficiente das informações e o suporte às atividades organizacionais e decisórias.

No cenário vigente, a TI é de vital importância à evolução tecnológica por que passam os profissionais, empresas e governos, contribuindo desde a automação de tarefas até a criação de *softwares* e novos modelos de negócios, cada vez mais intuitivos e de grande relevância social e econômica.

Na atualidade a atuação do profissional de TI é por demais ampla, necessária e complexa, vez que ele se afetará ambientes disciplinados por costumes nem sempre em singularidade às normas e leis, que regem o que é permitido ou não em sua atuação profissional, empresarial e econômica.

Nesse contexto, verifica-se que muitos profissionais de Tecnologia da Informação não receberam, em sua formação inicial, preparação jurídica suficientemente atualizada para enfrentar as exigências técnicas em conformidade com os deveres civis e penais que incidem sobre sua atuação. Isso se agrava pelo fato de que normas, legislações e padrões técnicos se encontram em permanente evolução, acompanhando o ritmo acelerado do avanço tecnológico e seus impactos culturais, sociais e econômicos. Diante dessa realidade, torna-se imprescindível que o profissional de TI adote uma postura diligente de atualização contínua, incorporando conhecimentos jurídicos relevantes à sua prática, de modo a alinhar competência técnica, segurança da informação e responsabilidade legal.

É necessário que os profissionais de TI atuem em conformidade com os direitos e garantias fundamentais previstos na Constituição Federal e na legislação, especialmente aqueles relacionados à proteção da imagem, à privacidade, à segurança dos dados e à propriedade intelectual. O respeito a esses princípios é indispensável à prática ética e responsável das atividades tecnológicas, considerando que o manuseio inadequado de informações sensíveis pode comprometer indivíduos, instituições e o próprio Estado.

A negligência ou o descumprimento das normas jurídicas aplicáveis pode acarretar sérias consequências, incluindo sanções civis, administrativas e penais, conforme previsto na legislação vigente.

### 2.1.2. Desenvolvimento *Web*:

Em concepção, consiste na criação e manutenção de sites, aplicativos e serviços online na rede mundial de computadores, que são acessados e utilizados através de navegadores ou plataformas inerentes.

Com a expansão do alcance corporativo da Internet e das redes sociais, esse processo tornou-se parte essencial da estratégia de atuação profissional, empresarial e governamental.

Novas soluções tecnológicas, como *frameworks* de desenvolvimento, *APIs* e arquiteturas baseadas em microserviços, ampliam a complexidade e a escala dos projetos e efeitos, exigindo maior conhecimento atualizado e atenção a questões de desempenho, segurança e conformidade jurídica.

### 2.1.3. *Big Data*:

Diz respeito ao conjunto de soluções técnicas necessárias ao trabalho com consideráveis volumes de dados, que variam em formato, complexidade e velocidade de produção. O objetivo é assimilar *insights* importantes, que irão subsidiar a tomada de decisões necessárias e relevantes.

A trabalho e utilização de dados em grande proporção demanda procedimentos criteriosos e rigorosos de segurança, privacidade e governança de TI, visando evitar uso indevido de informações e não infringir leis que protegem a privacidade dos indivíduos, estratégias corporativas e consequentemente a atuação do profissional de TI.

### 2.1.4. Segurança da Informação:

A segurança da informação compreende práticas e protocolos necessários à proteção de dados contra utilização, interceptação, alterações e destruição, não autorizados. Ela se embasa em três aspectos, quais sejam:

- **Confidencialidade**: permite que a informação seja acessada apenas por pessoas que estejam autorizadas.

- **Integridade**: favorece a precisão e a consistência das informações ao longo de todo o seu ciclo de vida útil.

- **Disponibilidade**: faz com que os dados estejam acessíveis a quem precisar, no momento necessário.

Para tanto é essencial definir autorizações de acesso específicas e precisas, através de controles, tais como: autenticação, criptografia, segregação de funções e monitoramento de atividades.

Os sistemas devem operar em conformidade com a LGPD, visando evitar danos legais, financeiros e reputacionais às organizações e aos profissionais de TI.

### 2.1.5. Aspectos Jurídicos Relacionados à Área de TI:

A relevância e abrangência da TI no progresso e desenvolvimento econômico, cultural e social, torna necessário um constante aprimoramento e aplicação tempestiva de leis que respaldam a proteção de dados, o respeito à honra e à imagem, possibilitando segurança e usabilidade.

### 2.1.6. Proteção de Dados e Privacidade:

A LGPD necessariamente estabeleceu parâmetros obrigacionais à profissionais de TI, autônomos ou empresariais, assim como às empresas públicas e privadas, quanto à coleta, ao armazenamento, ao tratamento e ao compartilhamento de dados pessoais. Errar em observar essas obrigações resultarão em processos: administrativos e judiciais, que resultarão na responsabilização civil e penal dos que derem causa ao evento danoso.

### 2.1.7. Propriedade Intelectual e Direitos Autorais:

O planejamento, criação e desenvolvimento de soluções técnicas necessárias, tais como: aplicativos, softwares, sites e os mais diversos serviços, na rede mundial de computadores, envolvem a utilização de bancos de dados, que estão protegidos por direitos e garantias fundamentais de cada indivíduo e/ou empresa.

O não respeito à legislação inerente à propriedade intelectual, por exemplo (como plágio ou uso indevido de conteúdo) acarretará na responsabilização civil e penal.

### 2.1.8. Responsabilidade Civil e Penal:

Os profissionais de TI, estão rotineiramente expostos e sujeitos à responsabilização civil e criminal, quando comprovada a responsabilidade por incidentes que resultarem no vazamento e utilização indevida de dados e imagens, protegidos por lei.

### 2.1.9. Contratos e Acordos de Nível de Serviço (SLAs):

Contratos de desenvolvimento, terceirização de serviços e acordos de nível de serviço, dentro do escopo de atuação profissional e empresarial na área de TI, precisam fixar obrigações e responsabilidades civis e criminais entre as partes envolvidas e interessadas de forma clara e sucinta.

Devem ser confeccionados com especial atenção ao objetivo do projeto, considerando às garantias de segurança e às cláusulas de confidencialidade para evitar as severas consequências jurídicas.

### 2.1.10. *Compliance* no Contexto da Tecnologia da Informação:

O termo *Compliance* refere-se à implantação da cultura que visa a conformidade e respeito por parte de profissionais e empresas em relação às normas e à legislação atinente.

Desse modo resulta em um sistema de governança que se dedica a essa conformidade de forma culturalmente contínua, através de políticas e controles internos, diligente gestão de riscos, específicos treinamentos, realização de auditorias necessárias, criação de um eficiente canal de denúncias e respostas.

Na área de TI, a governança e a auditoria são de relevante prioridade e atenção, vez que ajudam a manter o uso adequado e seguro das tecnologias, reduzindo o risco de consequências jurídicas, que podem resultar em impactos financeiros.

## 2.2. TRABALHOS RELACIONADOS:

Esta seção apresenta alguns trabalhos relacionados ao tema em estudo.

### 2.2.1. Marco Civil da Internet: A Neutralidade de Rede na Perspectiva das Telecomunicações

A dissertação de Franco (2024) tem como objetivo analisar o tema da neutralidade de rede, face às recentes discussões que culminaram na aprovação do Marco Civil da Internet (Lei Federal n. 12.965/2014), em especial sob o enfoque das telecomunicações.

Sua pesquisa demonstra que neutralidade de rede é uma condição técnica de configuração de rede relacionada ao modo pelo qual as informações trafegarão na Internet, permitindo que, de forma neutra, cada camada (física, lógica e de aplicações) possa operar sem interferência da outra.

O estudo se divide nas seguintes etapas: Contextualizando a Internet e as Telecomunicações; Contextualizando a Neutralidade de Rede; Examinando os Principais Argumentos Contrários à Neutralidade de Rede; Examinando os Principais Argumentos Favoráveis à Neutralidade; O Tema no Direito Comparado; Críticas à Experiência Brasileira sobre Neutralidade;

O autor conclui que embora o enfoque dado ao debate sobre a neutralidade de rede no (MCI) tenha contornos legais e políticos, o problema da discriminação no tráfego dos pacotes é de natureza técnica (impossibilidade de conferir tratamento indiscriminado

a toda e qualquer aplicação e pacote) e reflete questões econômicas para as quais não é possível se estabelecer, nesse momento, um consenso ou uma solução.

Existem consistentes fundamentos para sustentar a adoção ou não da neutralidade, a partir da visão de distintos doutrinadores e expoentes que foram abordados na presente pesquisa.

### 2.2.2. *Compliance* Digital e Segurança da Informação: Desafios Impostos pela LGPD

A dissertação de Ronha (2011) tem como objetivo estudar o *compliance* digital, a segurança da informação e a capacidade dessas ferramentas em propiciar segurança para os dados que são tratados e que trafegam pela Internet.

Almeja analisar como as referidas políticas podem ser implementadas nas empresas com o intuito de atingirem seus objetivos e legítimos interesses e se a junção dessas duas governanças poderá cumprir os desafios impostos pela LGPD - Lei Federal n. 13.709/2018.

A pesquisa demonstra como o direito e o *compliance* devem ser enxergados de uma forma multidisciplinar como tentativa para garantir a proteção dos dados. Dentre os fatores identificados sobressai o fato de que quando falamos de dados, estes podem ser trabalhados em qualquer seara, em qualquer ciência do conhecimento e da esfera profissional.

Seu vazamento pode ocorrer por meio de tratamento incorreto, de finalidade distinta do proposto, pela pulverização da informação na grande rede sem o consentimento expresso do titular do dado, dentre outras formas.

O tema não afeta somente o universo tecnológico ou o cumprimento de uma lei, mas toda origem e cadeia que permeia o dado.

O estudo se divide nas seguintes etapas: Proteção Jurídica da Privacidade e dos Dados; Governança: *Compliance* Digital e Segurança da Informação na Proteção da Privacidade e dos Dados; Adequação das Empresas ao novo modelo de Governança e a Multidisciplinaridade para garantir uma melhor governança do *Compliance* Digital.

O autor concluiu que com base nas informações coletadas, foi constatado que: a nova governança deverá ser incorporada pela sociedade empresária atentando-se aos princípios legais e direitos e garantias fundamentais, quais sejam, o respeito à privacidade e aos dados como condições inerentes à existência humana.

### 2.2.3. A Responsabilização das Plataformas Digitais sobre o Conteúdo Postado por Terceiros

A dissertação de Marchioni (2023), explica que o rápido desenvolvimento e popularização das tecnologias de comunicação digital, que partiu de computadores-robustos e fixos, mídias físicas para transmissão de conteúdo entre terminais e bandas de Internet bastante limitadas para *smartphones* com acesso a uma rede veloz de Internet capaz de conectar todas as localidades do mundo em tempo real, em apenas alguns anos, resultou em uma reorganização da estrutura da comunicação social.

Quanto à regulamentação da comunicação digital, tem-se que, no Brasil, a isenção de responsabilidade das plataformas digitais sobre o conteúdo postado por terceiros, instituída pelo Marco Civil da Internet, foi inspirada por normativas de outros países, notadamente dos Estados Unidos, e na perspectiva tradicional de proteção ao princípio constitucional da liberdade de expressão.

O estudo se divide nas seguintes etapas: Comunicação Digital, Capitalismo de Vigilância e Epistemologia Tribal; Democracia, Liberdade de Expressão e Governança dos Discursos nas Mídias Digitais; Mapeamento de Arranjo Jurídico Institucional: A Regulamentação da Comunicação Digital no Brasil a partir do Marco Civil da Internet.

O autor concluiu que as alterações recentes na legislação internacional e na postura das plataformas, entretanto, tem resultado em novas políticas no combate à disseminação de discurso de ódio, em um processo que passa por ações institucionais propriamente ditas, como os Programas do Tribunal Superior Eleitoral estudados nessa dissertação, ou na discussão do chamado Projeto de Lei das *Fake News*, e, principalmente, na ação das plataformas ao exercer governança privada dos discursos, modificando o panorama instituído pelo Marco Civil da Internet.

### 2.2.4. Provedores de Aplicação, Direitos Fundamentais e Responsabilidade Civil por Conteúdo de Terceiros

Explica que prestadores de serviços na Internet se tornaram agentes de grande relevância para a sociedade contemporânea, acarretando reflexos diretos à direitos fundamentais previstos na Constituição Federal de 1988.

O trabalho buscou analisar a unicidade do regime de responsabilidade civil de provedores de aplicação, termo guarda-chuva adotado no Marco Civil da Internet.

O dispositivo prevê que a responsabilidade civil por conteúdo de terceiros é condicionada pelo descumprimento a uma ordem judicial, o que faz com que a liberdade de expressão de usuários seja protegida, ainda que, em algumas situações, em detrimento de direitos de personalidade, como a privacidade e a honra.

A análise abordou primeiramente os conceitos do objeto de estudo, sucedido por uma comparação entre modelos de negócios de provedores de aplicação.

No segundo capítulo, a partir de consulta bibliográfica, normativa e jurisprudencial, foi realizada ampla análise sistematizada de jurisprudências do Superior Tribunal de Justiça (STJ) e de casos singulares para verificar a forma com que foram decididos litígios relacionados à responsabilidade civil de provedores de aplicação por conteúdo de terceiros.

Observou-se a forma com que o Tribunal decidiu diante de aparentes conflitos normativos e dificuldade de aplicação do artigo 19, em virtude do modelo de negócio do provedor de aplicação.

Por fim, no último capítulo do trabalho, voltou-se olhares ao Tema 987, do Supremo Tribunal Federal, no qual julga-se a constitucionalidade do artigo 19 do Marco Civil da Internet.

Concluiu pela necessidade de complexificação do regime de responsabilidade de provedores de aplicação por conteúdo de terceiros, já que o termo provedores de aplicação agrega muitos modelos de negócio e acarretam impactos e riscos distintos à sociedade.

### 2.2.5. Direitos Autorais, Informação e Tecnologia: Impasses e Potencialidades

Biscalchin e Almeida (2011) explicam que no contexto dos Direitos autorais, informação e tecnologia, o estudo realizado, chama a multidisciplinaridade para desvelar sua complexidade e para compreender como a era digital mobiliza novas formas de lidar com a propriedade intelectual, transpondo os limites da Ciência da Informação e enveredando pelos conceitos-chave de uma série de outras disciplinas que perpassam essa questão.

É feita uma revisão do conceito de autoria revendo aspectos legais do direito autoral e sua relação com a Internet. Realiza-se uma breve reflexão sobre como as publicações em periódicos de Ciência da Informação tratam novas possibilidades para o direito emergente das mudanças de paradigmas provocados pela tecnologia.

O estudo se divide nas seguintes etapas: Aspectos legais da autoria e sua relação com a Internet, Trocas sociais, cultura e capitalismo informacional, o digital como catalizador das discussões, interesses e soluções, as alternativas ao *Copyright*.

Os autores concluíram que com base nas informações coletadas, foi constatado que, ainda que timidamente, a Ciência da Informação está sintonizada no movimento das forças sociais, em lugar de atrelar-se a interesses previamente definidos de grupos ou instituições.

**3 - MÉTODO:**

Este trabalho, quanto à natureza da pesquisa é um resumo de assunto, no qual se busca apenas sistematizar uma área de conhecimento, usualmente indicando sua evolução histórica e estado da arte (Waslawick, 2014, p.29).

Segundo seus objetivos a pesquisa exploratória é aquela em que o autor não tem necessariamente uma hipótese ou objetivo definido em mente. Ela pode ser considerada, muitas vezes, como o primeiro estágio de um processo de pesquisa mais longo.

Na pesquisa exploratória, o autor vai examinar um conjunto de fenômenos, buscando anomalias que não sejam ainda conhecidas e que possam ser, então, a base para uma pesquisa mais elaborada (Waslawick, 2014, p.30).

Segundo aos procedimentos técnicos, esta pesquisa é bibliográfica e documental. A pesquisa bibliográfica, como qualquer outra, desenvolve ao longo de uma série de etapas. Seu número, assim como seu encadeamento, depende de muitos fatores, tais como a natureza do problema, o nível de conhecimentos que o pesquisador dispõe sobre o assunto, o grau de precisão que se pretende conferir à pesquisa etc. A pesquisa documental, apresenta muitos pontos de semelhança com a pesquisa bibliográfica (Gil, 2021, p.29).

Toda pesquisa científica é considerada bibliográfica em sua concepção face a necessidade de levantamento teórico necessário e suficiente à fundamentação do trabalho científico (Gil, 2021, p.43).

O passo a passo da pesquisa bibliográfica:

a) Escolha do tema: Responsabilidade Civil e Penal dos Profissionais de TI;

b) Levantamento bibliográfico preliminar: levantamento bibliográfico de acordo com área de interesse com intuito de familiarização com o tema e facilitação na definição do problema de pesquisa;

c) Formulação do problema: Ante à realidade jurídica, como o profissional de TI podem desempenhar suas atividades técnicas e empresariais, sem serem afetados pelas severas consequências civis e penais?

d) Identificação das fontes: Fontes em artigos científicos disponíveis na plataforma Capes e *Google academy*; Livros sobre o tema obtidos em acervo pessoal; Jurisprudências do Superior Tribunal de Justiça e do Supremo Tribunal Federal. Tais fontes propiciaram a formulação do problema de pesquisa e a elucidação dos processos envolvidos acerca do tema;

e) Leitura do material: identificação de pontos chaves correlacionadas ao tema de pesquisa;

f) Fichamento: produzido a partir do material bibliográfico selecionado afim guardar inferências importantes acerca do tema;

l) Redação do relatório: Escrita do TCC1.

A pesquisa documental, como já foi visto, apresenta muitos pontos de semelhança com a pesquisa bibliográfica. De modo geral, é possível identificar as seguintes etapas na pesquisa documental (Gil, 2021, p.59):

O passo a passo da pesquisa documental:

a) Formulação do problema: Ante à realidade jurídica, como o profissional de TI podem desempenhar suas atividades técnicas e empresariais, sem serem afetados pelas severas consequências civis e penais?
b) Identificacao das Fontes: foi buscado artigos científicos disponíveis na plataforma Capes e Google *academy*; Livros sobre o tema obtidos em acervo pessoal; Jurisprudências do Superior Tribunal de Justiça e do Supremo Tribunal Federal. Tais fontes propiciaram a formulação do problema de pesquisa e a elucidação dos processos envolvidos acerca do temos.

c) Redação do relatório e Escrita do TCC.

### 3.1. ETAPAS:

#### 3.1.1. Revisão Bibliográfica:

A revisão bibliográfica é a etapa inicial deste estudo, vez que privilegiou a investigação de publicações científicas relevantes, livros de temática especializada e artigos de periódicos, visando contribuir de forma coerente com os aprofundados estudos em relação ao tema proposto.

Para tanto, procedeu-se à organização sistemática dos principais conceitos e definições e teorias com foco na atualidade, observando-se a relevância temática das fontes escolhidas, assim como a diversidade de abordagens teóricas que contribuem para o escopo trabalhado.

#### 3.1.2. Análise da legislação vigente:

Para compreender o cenário jurídico em que se insere o objeto de estudo, realizou-se uma análise criteriosa da legislação vigente, quais sejam:

- Lei Federal n.º 13.709 de 2018 – Lei Geral de Proteção de Dados;
- Lei Federal n.º 12.965 de 2014 – Marco Civil da Internet;
- Lei Federal n.º 12.737 de 2012 – Tipificação Criminal de Delitos Informáticos Lei Carolina Dieckmann;
- Decreto-Lei Federal n.º 2.848 de 1940 – Código Penal;
- Lei Federal n.º 10.406 de 2002 – Código Civil;

Essa análise priorizou importantes alterações e adequações recentes na legislação e jurisprudência encontrada, que podem contribuir diretamente com a aplicabilidade do direito no que diz respeito à atuação profissional de TI, tornando possível compreender tendências e enquadramentos jurídicos, bem como as repercussões práticas, tanto de forma autônoma, quanto empresarial.

### 3.1.3. Entendimento jurisprudencial atinente:

O entendimento jurisprudencial pertinente ao tema escolhido, foi averiguado por meio de pesquisa em tribunais de diferentes instâncias, com destaque para as decisões do Superior Tribunal de Justiça e do Supremo Tribunal Federal, que servem de referência para a consolidação de teses jurídicas a serem seguidas no judiciário.

A escolha dos julgados foi baseada em critérios de relevância, atualidade e pertinência temática, o que possibilitou a formação de um panorama consistente acerca da realidade judicial em questão.

### 3.1.4. Compreensão das doutrinas dominantes:

O estudo das doutrinas dominantes, ou seja, bibliografia abrangente e relevante, envolveu a identificação das principais correntes de pensamento jurídico, que norteiam a matéria em questão, contemplando autores informados no início desse capítulo.

Por meio desse mapeamento doutrinário, buscou-se reconhecer os fundamentos teóricos mais significativos, bem como as perspectivas relevantes, que poderiam contribuir para a discussão proposta.

Esse movimento de articulação teórica possibilitou a construção de uma base conceitual sólida, sobre a qual se alicerçou a interpretação dos dados empíricos e a formulação de hipóteses e elucidação no contexto relevante.

### 3.1.5. Estudo de caso:

A estudo de caso concentrou-se na análise de um contrato de prestação de serviços, que quase foi assinado por um colega do curso de graduação, cujo qual tinha várias armadilhas jurídicas, várias ilegalidades, absurda discrepância de obrigações: quase 40 para o contratado e só 1 para o contratante.

A realização de estudo de caso foi fundamental para ilustrar, de forma concreta, as interfaces entre os aspectos técnicos da Engenharia de Computação e as consequências jurídicas da atuação profissional em Tecnologia da Informação.

Optou-se por um estudo de caso de natureza qualitativa, de caráter descritivo-explicativo, centrado na análise do contrato de prestação de serviços técnicos especializados em TI.

Esse documento foi selecionado por representar de maneira típica a prática contratual corrente no mercado, permitindo examinar, em contexto real, como se dá a alocação de riscos e deveres entre as partes e em que medida tal distribuição se harmoniza com os princípios da boa-fé objetiva, da função social do contrato e do equilíbrio contratual previstos no Código Civil, bem como com os deveres de segurança, confidencialidade e conformidade que recaem sobre o profissional de TI.

Em especial, verificou-se nesse contrato uma discrepância significativa entre as quase quarenta obrigações expressamente impostas ao contratado, envolvendo responsabilidades técnicas, prazos, garantias, confidencialidade, disponibilidade e solução de incidentes, enquanto que a única obrigação atribuída ao contratante, basicamente limitada ao pagamento dos serviços e ao fornecimento de informações mínimas.

Essa assimetria de deveres foi tratada, metodologicamente, como categoria analítica central, por evidenciar um potencial desequilíbrio na distribuição de riscos e responsabilidades, capaz de ampliar a exposição do profissional de TI a litígios civis e, em determinadas circunstâncias, a imputações penais.

A partir da leitura integral das cláusulas, procedeu-se à categorização das obrigações por temática (obrigações técnicas, de segurança da informação, de sigilo, de suporte e atendimento, deveres de colaboração do contratante etc.) e à confrontação dessas categorias com a legislação, a doutrina e a jurisprudência estudadas.

Esse procedimento permitiu utilizar o estudo de caso não apenas como ilustração empírica, mas como instrumento metodológico para demonstrar, de forma aplicada, como contratos desequilibrados podem reforçar o risco jurídico do profissional de TI e indicar a necessidade de uma atuação mais consciente, preventiva e alinhada às boas práticas de elaboração, negociação e revisão contratual.

### 3.1.6. Análise documental:

Na análise documental, recorreu-se a registros oficiais e dados estatísticos disponibilizados por órgãos públicos e entidades privadas.

Para tanto procedeu-se à seleção e avaliação criteriosa dos documentos, considerando aspectos como autenticidade, representatividade e fidedignidade, de modo a garantir que a interpretação resultante se alicerçasse em fontes consistentes.

### 3.1.7. Sistematização de dados:

A etapa de sistematização de dados consistiu na consolidação de todas as informações coletadas ao longo das fases anteriores, sejam elas de natureza bibliográfica, legislativa, jurisprudencial ou documental.

Buscou-se agrupar as informações segundo critérios de relevância e pertinência temática, culminando em um processo de interpretação que levou em conta tanto os referenciais teóricos estudados quanto as evidências empíricas colhidas.

Os resultados dessa sistematização embasam as reflexões desenvolvidas nos capítulos subsequentes, fornecendo subsídios sólidos para o trabalho proposto.

## 4. A LEI GERAL DE PROTEÇÃO DE DADOS:

A consolidação da economia digital transformou dados pessoais no principal ativo das relações de consumo, impulsionando riscos para a autodeterminação informativa.

Diante disso, a LGPD estabelece no Brasil um regime de proteção à privacidade que se articula com normas setoriais e com o Marco Civil da Internet, consolidando a proteção de dados como direito fundamental.

Para entender a LGPD, partimos do ambiente atual: sistemas distribuídos, dados em nuvem e integrações via *APIs*. O ganho de eficiência e novos serviços é inegável, mas o processamento extensivo de dados pessoais sem salvaguardas adequadas resulta em violações de privacidade — exatamente o problema que a lei busca endereçar.

Com frequência, pesquisamos um produto ou serviço na Internet e, pouco tempo depois, começamos a receber diversas ofertas de empresas relacionadas ao que foi buscado. Da mesma forma, não é novidade que, após uma simples conversa sobre determinado interesse, ao acessar o *Google*, surge imediatamente uma publicidade oferecendo exatamente aquilo que havia sido mencionado.

> Os aposentados recebem ligações de financeiras oferecendo empréstimo consignado antes mesmo de saber que a aposentadoria havia sido deferida. O

> *Google* e o *Facebook* já assumiram que filtram algumas palavras para oferecer produtos e serviços aos usuários. As assistentes virtuais também “ouvem” o que está sendo dito; os alto-falantes inteligentes estão constantemente ouvindo o ambiente em que se encontram esperando capturarem uma palavra de ativação. Contando com isso, foi solicitado à *Amazon* os arquivos da assistente pessoal *Alexa* que pode ter sido testemunha de um crime. Esse avanço tecnológico que encanta e auxilia em inúmeras tarefas diárias, também amedronta e faz com que limites sejam questionados (Lima, 2022, p.17).

Falando em limites, o modelo de marketing que utiliza tecnologia para oferecer produtos e serviços mostra-se bastante intrusivo, pois é capaz de traçar o perfil do consumidor a partir de suas preferências. Como destaca Magrani, é fundamental evitar os abusos da publicidade direcionada, que “coleta informações para vender produtos, valendo-se de táticas como *targeting* e *profiling*”. Nesse contexto, evidencia-se a relevância da LGPD, como será analisado adiante.

> Independentemente do tamanho da empresa, resta claro que, em maior ou menor proporção, as empresas precisam adequar-se às melhores práticas, estar em conformidade com as legislações relacionadas à sua área de atuação, ter como norte a integridade e a ética, compreender a importância de transferir esses valores aos colaboradores, esclarecendo a postura esperada, indicando diretrizes a serem seguidas (Lima, 2022, p.21).

A Constituição de 1988 garante, em seu art. 5º, X, a inviolabilidade da intimidade, da vida privada, da honra e da imagem, com direito à indenização por dano material ou moral. Já o art. 5º, XII, assegura o sigilo da correspondência e das comunicações telegráficas, de dados e telefônicas, nos termos da lei. Soma-se a isso o habeas data (art. 5º, LXXII), que permite ao titular acessar e corrigir informações pessoais mantidas sobre si (Brasil, Constituição Federal/1988, art. 5º, XII e LXXII).

> A privacidade tem relação com a vida privada, com o direito de ter sua intimidade protegida e está intimamente relacionada com a dignidade da pessoa humana.

> As primeiras discussões jurídicas sobre a privacidade surgiram a partir do artigo "*the right to privacy*" ou o "direito à privacidade" trazido em 1890 por Samuel Warren e Louis Brandeis, também conhecido como "*the right to be let alone*" ou "o direito de ser deixado só" ou em paz (Lima, 2022, p.28).

O direito de decidir sobre os próprios dados é a autodeterminação informativa. Essa decisão só é válida se a pessoa entender, de forma clara, as finalidades, os riscos e os impactos do uso de suas informações — nada de textos obscuros, meias-verdades ou termos incompreensíveis ao cidadão médio.

> No Brasil, a proteção à intimidade e à vida privada está contemplada na Constituição Federal de 1988, em seu art. 5°, X, tornando a privacidade um direito fundamental. Adiante, na Carta Magna, destaca-se a inviolabilidade do domicílio e da correspondência. Ressalta-se ainda o Pacto de São José da Costa Rica que entrou em vigor através do Decreto n° 678/1992, trazendo a proteção à família e à privacidade, além da dignidade da pessoa humana (Lima, 2022, p.31).

Autodeterminação informativa é o controle do titular sobre o uso e o fluxo dos seus dados. Em outras palavras: ele decide como, por quem e para que seus dados serão tratados. Já as liberdades de expressão, informação, comunicação e opinião não são absolutas; precisam ser ponderadas caso a caso quando colidem com direitos de privacidade e com o ordenamento jurídico, em linha com os fundamentos de direitos humanos previstos na LGPD.

Por fim, evidencia-se que a LGPD representa uma oportunidade para que as empresas adotem um novo direcionamento por meio de uma mudança cultural, preparando-se para os desafios e possibilidades que surgirão. O futuro dependerá diretamente da importância que a organização atribuir à legislação, ao respeito aos titulares de dados pessoais, aos esforços de implementação e à sua capacidade de adaptação e transformação.

Este texto apresentou um panorama geral sobre a temática, de forma sintética e sem a pretensão de esgotá-la. Ressalte-se que o processo de adequação é complexo, multidisciplinar e exige tempo. Além disso, cada plano de conformidade é único e deve ser construído de acordo com a área de atuação e as particularidades de cada atuação profissional e/ou empresa.

### 4.1. Conceito e Finalidade da LGPD

A LGPD dispõe sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, Lei nº 13.709/2018, art. 1º).

Entre seus fundamentos (art. 2º) destacam-se o respeito à privacidade, a autodeterminação informativa e o desenvolvimento econômico e tecnológico (Teixeira, 2022, p.8).

### 4.2. Âmbito de Aplicação e Exclusões

Nos termos do art. 3º, a LGPD aplica-se a qualquer operação de tratamento realizada no território nacional ou que vise oferecer bens ou serviços a titulares localizados no Brasil, ainda que o processamento ocorra no exterior (Brasil, Lei nº 13.709/2018, art. 3º).

As exclusões do art. 4º, como tratamentos para fins jornalísticos ou de segurança pública, reforçam o caráter transversal, porém não absoluto, da norma (Teixeira, 2022, p.10).

### 4.3. Princípios Norteadores

O art. 6º da LGPD reúne dez princípios. Finalidade, adequação e necessidade sustentam a minimização de dados; livre acesso e qualidade garantem transparência; segurança e prevenção exigem controles técnicos e administrativos; não discriminação coíbe usos abusivos; responsabilização e prestação de contas impõem *compliance* contínuo (Brasil, Lei nº 13.709/2018, art. 6º).

Na prática: elucida finalidades explícitas e colete apenas o necessário (finalidade/adequação/necessidade); ofereça portal de titular e métricas de qualidade de dados (livre acesso/qualidade); aplique criptografia, controle de acesso, *logging* e gestão de vulnerabilidades (segurança/prevenção); bloqueie decisões discriminatórias por desenho (não discriminação); mantenha trilhas de auditoria, DPIAs e relatórios periódicos (responsabilização/prestação de contas).

### 4.4. Bases Legais para o Tratamento

As bases legais do art. 7º legitimam o tratamento de dados. São elas: consentimento; cumprimento de obrigação legal ou regulatória; execução de contrato (e procedimentos preliminares); políticas públicas pela administração pública; estudos por órgão de pesquisa (com anonimização sempre que possível); exercício regular de direitos em processos; proteção da vida ou da incolumidade física; tutela da saúde; interesse legítimo; e proteção do crédito. Escolher e documentar a base correta evita nulidades e sanções (Brasil, Lei nº 13.709/2018, art. 7º).

Deste modo define dez hipóteses de licitude:

**a)** consentimento;

**b)** obrigação legal/regulatória;

**c)** contrato e pré-contratuais;

**d)** administração pública em políticas públicas;

**e)** pesquisa por órgão de pesquisa (preferencialmente com anonimização);

**f)** exercício de direitos em processos judicial/administrativo/arbitral; **g)** proteção da vida/incolumidade;

**h)** tutela da saúde;

**i)** interesse legítimo do controlador/terceiro (com balanceamento);

**j)** proteção do crédito. A correlação “finalidade ↔ base legal” deve ser explícita e evidenciada em registros de tratamento.

### 4.5. Direitos dos titulares

Em seu art. 18 garante, entre outros, confirmação de tratamento, acesso, correção, portabilidade, eliminação, informação sobre compartilhamentos e revogação do consentimento. Para viabilizar esses direitos, é preciso ter procedimentos internos claros, registros de atividades (art. 37) e canais de atendimento que funcionem (Brasil, Lei nº 13.709/2018, art. 18 e 37).

Sendo assim o titular pode: confirmar se há tratamento, acessar dados, corrigir, portar, eliminar, saber com quem se compartilha e revogar consentimento. A execução exige governança: políticas operacionais, registro de operações (art. 37), SLAs para prazos e um canal de atendimento monitorado (Brasil, Lei nº 13.709/2018, art. 37).

### 4.6. Agentes de Tratamento e Responsabilidades

Controlador e operador (art. 5º, VI e VII) respondem solidariamente pelos danos causados. O encarregado de dados (art. 41) atua como ponto de contato com titulares e a (ANPD), devendo ter suas informações públicas (Brasil, Lei nº 13.709/2018, art. 5º, VI e VII).

Boas práticas, relatórios de impacto e registro de operações são instrumentos de *accountability* que influenciam a dosimetria das sanções administrativas, art. 52. (Teixeira et al., 2022, p.28).

### 4.7. Paradigma Jurídico

A LGPD consolida um novo foco jurídico que equilibra avanço e inovação tecnológica e a proteção da dignidade visando a proteção dos direitos e garantias fundamentais, elencados na Constituição Federal (Brasil, Lei nº 13.709/2018, art. 5º).

Empresas e órgãos públicos que implementam governança de dados na área de TI, respeitando os princípios legais, ganham eficiência operacional, favorecem a confiança do cliente e do usuário e reduzem a probabilidade de problemas jurídicos atinentes.

A internalização de uma cultura de privacidade, sustentada por programas de *compliance*, educação permanente e uso da tecnologia de forma juridicamente coerente, constitui a via mais seguras para transformar a LGPD de obrigação legal em vantagem competitiva, tendo como consequências o respeito a direitos de clientes e usuários.

## 5. O MARCO CIVIL DA INTERNET:

O Marco Civil da Internet consolidou princípios, direitos e deveres para o uso da rede no Brasil, projetando-se como parâmetro regulatório central para a sociedade em rede (Brasil, Lei n.º 12.965/2014).

Sua adoção dialoga com demandas de liberdade de expressão, proteção da privacidade e desenvolvimento tecnológico, temas indispensáveis a qualquer debate acadêmico contemporâneo sobre governança digital.

Este capítulo examina tais diretrizes, com ênfase na responsabilidade dos provedores e na interface com a proteção de dados, traçando panorama crítico que subsidia discussões jurídicas e organizacionais acerca do *_compliance_* digital.

## 5.1. Contextualização Histórica e Fundamentos

O Marco Civil da Internet foi criado num cenário de decisões judiciais divergentes, que geravam insegurança jurídica e incoerências em relação às garantias constitucionais. Por isso, adotou-se uma abordagem principiológica visando unificar critérios de liberdade de expressão e privacidade no ambiente da rede mundial de computadores e dar previsibilidade à atuação do Judiciário.

Diante de jurisprudência fragmentada e prováveis violações a direitos fundamentais, o Marco Civil focou em uma arquitetura normativa de princípios. O objetivo é padronizar parâmetros necessários à coerência no tocante à liberdade de expressão e proteção de dados e respeito à privacidade na Internet, além de reduzir desencontros decisórias no Poder Judiciário.

O Marco Civil da Internet estabelece princípios, garantias e direitos para o uso da rede no Brasil, proporcionando um enquadramento jurídico consistente para liberdade de expressão e proteção da privacidade. Aspectos operacionais foram detalhados pelo Decreto nº 8.771, de 11/05/2016, que regulamenta pontos específicos da lei em questão (BRASIL, 2014).

> Trata-se de uma lei principiológica, pois estabelece parâmetros gerais acerca de princípios, garantias, direitos e deveres para o uso da Internet no Brasil, além de determinar algumas diretrizes a serem seguidas pelo Poder Público sobre o assunto (Lei n. 12.965/2014 – Marco Civil da Internet – MCI, art. 1º). Em seu texto também há regras específicas a serem cumpridas por agentes que operam na

> Internet, especialmente as dirigidas aos provedores de conexão e de aplicações de Internet, como veremos adiante (Teixeira et al., 2020, p.90).

O item 4 da justificativa registra que a ausência de parâmetros normativos para dinâmicas na rede mundial de computadores, resultava em jurisprudência instável e potencial violação de direitos fundamentais.

No item 16, priorizou-se a responsabilização subjetiva (culpa/dolo) visando equilibrar liberdade de expressão e responsabilidade jurídicas, priorizando o modelo "u*ser-generated conten*t" e a não exigência de aprovação prévia por provedores. O anteprojeto ancora-se na presunção de inocência, reservando tratamento excepcional aos eventuais abusos prudentemente constatados.

O problema identificado era "processo regulatório": sem padrão, cada caso se tornava uma regra, quebrando previsibilidade. A escolha por responsabilidade subjetiv**a** evita impor *by design* moderação prévia nos intermediários (custosa e arriscada a falsos positivos), preserva fluxo de publicação por usuários e orienta mecanismos de *notice-and-takedown* proporcionais. A base é presunção de inocência: só há sanção quando há evidência de abuso, tratado como exceção, não como regra do sistema que envolve a TI.

> O Marco Civil da Internet (Lei n. 12.965/2011) é resultado do Projeto de Lei n. 2.126/2011, que tramitou inicialmente na Câmara dos Deputados, sendo amplamente discutido e objeto de várias audiências públicas. Ao ser aprovado nesta Casa Legislativa em 2014, foi para o Senado Federal, onde recebeu o número 21/2014, tendo sido aprovado em curtíssimo espaço de tempo, sem margem para qualquer discussão e alteração no âmbito desta segunda Casa (Teixeira et al., 2020, p.91).

## 5.2. Princípios, Direitos e Garantias

O art. 2º trata da liberdade de expressão e pluralidade cultural como fundamentos. O art. 3º consolida princípios operacionais — proteção da privacidade e neutralidade de rede — que estruturam a governança da Internet no país e reduzem assimetrias de poder entre usuários e provedores (Brasil, Lei n.º 12.965/2014, art. 2º).

> Quanto à **liberdade de expressão** (cujo direito está assegurado na Constituição Federal, art. 5º, inc. IX, consistindo na liberdade de manifestação intelectual, artística, científica e de comunicação, sem censura ou necessidade de licença, como visto em outro item desta obra), o usuário da Internet pode se expressar escrevendo e postando o que bem entender, sendo que o conteúdo somente pode ser removido pelo provedor mediante ordem judicial. Como veremos adiante, nos casos de imagens (fotos e vídeos) com conteúdo pornográfico, os interessados envolvidos nas cenas podem exigir a retirada do conteúdo no provedor mediante notificação própria ou de seu procurador, não sendo, neste caso, necessária ordem judicial. Obviamente que o exercício da liberdade de expressão não impede de o prejudicado pleitear indenização com o internauta ofensor se a manifestação deste causar dano de ordem moral e/ou patrimonial, ficando o provedor livre de responsabilidade, via de regra (Teixeira, 2020, p.92).

No eixo de privacidade, a lei garante respaldo ao sigilo de dados pessoais e de comunicações, além da proteção restrita aos registros. Conteúdo só pode ser acessado através de ordem judicial. Medidas de *traffic management* são admitidas para manter a qualidade do serviço, desde que transparentes e sem inspeção de conteúdo ou discriminação de tráfego.

> A **neutralidade** (ou **princípio da neutralidade**) no uso da Internet consiste no fato de que o acesso à Internet pelo usuário pode dar-se de forma livre para quaisquer fins: realizar pesquisas ou compras, estabelecer comunicações, como por *e-mail*, utilizar redes sociais em geral, jogar *games*, visualizar e postar textos, fotos e vídeos etc. Dessa forma, o tratamento deve ser neutro, não podendo haver diferenciação em razão do uso realizado pelo internauta, sendo possível apenas serem oferecidos pacotes com valores diversos para fins da velocidade

> na navegação. Assim, o usuário pode usar a conexão à Internet para o fim que desejar (*e-mails*, *blogs* etc.) sem precisar pagar valores distintos pa-ra tanto e sem estar sujeito à fiscalização do provedor (Teixeira, 2020, p.92).

O Marco Civil reforça a neutralidade de rede: quem transmite, comuta ou roteia tráfego deve tratar todos os pacotes de forma isonômica, sem discriminar por conteúdo, origem/destino, serviço, terminal ou aplicação (Brasil, Lei n.º 12.965/2014, art. 9º).

### 5.3. Responsabilidade Civil dos Provedores

A responsabilização dos agentes técnicos obedece à lógica de que "cada qual responde na medida de sua contribuição à consumação da conduta delituosa", o que significa dizer que o provedor de conexão não é civilmente responsável pelo conteúdo que trafega, essa é a inteligência do art. 18 da lei em questão, enquanto o provedor de aplicações somente o será se, após decisão judicial, não retirar o material ilícito (Brasil, Lei n.º 12.965/2014, art. 19).

Essa regra criou verdadeiro **safe harbor**, afastando filtragem prévia de conteúdos e prevenindo censura privada (Capanema, 2020, p.53).

Em relação aos provedores de Internet, o Marco Civil da Internet focou em estabelecer normas específicas aos provedores de conexão e de aplicações em relação à rede mundial de computadores.

> Conforme visto em outra passagem, na doutrina, provedor de serviços de Internet é aquele que realiza uma atividade de prestação de serviços ligada ao funcionamento da rede mundial de computadores, sendo muito comum ocorrer confusão entre as espécies de provedores. Assim, provedor de serviços de Internet é um gênero do qual são espécies: provedor de *backbone*, provedor de acesso, provedor de correio eletrônico, provedor de hospedagem e provedor de conteúdo (Teixeira et al., 2020, p.93).

O Marco Civil da Internet, considera que há dois papéis distintos: **provedor de conexão**, responsável pela oferta de acesso e transporte de pacotes (camada de rede), e **provedor de aplicações**, que opera na camada de aplicação — e-mail, hospedagem, serviços online e distribuição de conteúdo. Essa definição orienta responsabilidades, guarda de registros e deveres de transparência (Brasil, Lei n.º 12.965/2014).

> Quanto às espécies de provedores, embora cada uma delas preste um serviço diferente (como visto anteriormente), é usual que alguns dos serviços sejam ofertados em conjunto por um mesmo provedor. Por exemplo, um provedor pode prover acesso, fornecer correio eletrônico e hospedagem. Entretanto, as diferenças nos conceitos existem e são indispensáveis, devendo ser identificadas a fim de se verificar qual a responsabilidade de acordo com a atividade desenvolvida. Isso é comprovado pelo art. 3º, VI, da Lei n. 12.965/2014, ao asseverar que a responsabilidade dos agentes deve ocorrer conforme as suas atividades desenvolvidas (Teixeira et al., 2020, p.93).

Ante o exposto os provedores de conexão, logo quem entrega o acesso à rede mundial de computadores, não respondem por danos causados por conteúdo de responsabilidade usuários (Brasil, Lei n.º 12.965/2014, art. 18).

### 5.3.1. O Alcance do art. 19

O modelo do art. 19 adota *notice-and-takedown* judicial: só há responsabilidade civil do provedor se, após ordem do juiz, ele não remover o conteúdo. Isso mitiga *overblocking* e protege a liberdade de expressão. Exceções de *fast track* existem (v.g., art. 21 para imagens íntimas não consentidas), nas quais a mera notificação do titular é suficiente para caracterizar o dever de retirada (Brasil, Lei n.º 12.965/2014, art. 19).

> O art. 19, ao condicionar a responsabilização à recusa em cumprir ordem judicial, transfere ao Estado-juiz a última palavra sobre a licitude do discurso na *web*, preservando a liberdade de expressão, ainda que reconheça situações excepcionais – como a divulgação não consentida de imagens íntimas – em que

> notificação extrajudicial basta para caracterizar o dever de remoção (Furtado et al., 2020, p.320).

### 5.4. Interseção com a LGPD

A conexão entre o Marco Civil e a LGPD se revela no art. 7º, que prevê ao usuário o direito à exclusão definitiva de seus dados, antecipando salvaguardas depois aprofundadas pela LGPD (Brasil, Lei n.º 12.965/2014, art. 7º).

O tratamento convergente reforça a tutela do titular e reafirma o princípio da autodeterminação informativa, base para políticas de *_accountability_* organizacional (Miranda, 2020, p.173).

A arquitetura principiológica do Marco Civil projeta-se como instrumento de governança digital apto a equilibrar inovação, direitos fundamentais e responsabilidade.

Ao delimitar a atuação dos provedores em consonância com o Poder Judiciário e ao dialogar com a LGPD, a lei oferece base normativa capaz de sustentar práticas de *_due diligence_* e de fortalecer a confiança no ecossistema digital brasileiro.

> Ainda no campo dos direitos dos usuários da Internet no Brasil, o Marco Civil trata das questões que envolvem a captação de dados (normalmente via uso de *cookie*) e a formação de banco de dados (*mailing list*) e sua cessão ou comercialização para terceiros. Conforme o art. 7º, o usuário tem direito: (i) a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, não sejam vedadas pela legislação e estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de Internet; (ii) a necessidade de **consentimento expresso** sobre coleta, uso, armazenamento e tratamento de dados pessoais deverá constar de forma destacada das demais cláusulas contratuais (Teixeira et al., 2020, p.97).

## 6. A LEI DOS CRIMES CIBERNÉTICOS – LEI CAROLINA DIECKMANN:

A utilização de aplicativos, softwares, redes sociais, sites, etc. expõe o profissional de TI e os usuários a uma crescente probabilidade de afetar o direito de outrem, o uso de dados e imagens, demanda especial cuidado para não consumar conduta que pode ser enquadrada nos dispositivos legais e gerar severas consequências.

> A Lei Federal n.º 12.737/2012, popularmente denominada Lei Carolina Dieckmann, emergiu como resposta legislativa, Tipificando a invasão de dispositivo informático e promovendo ajustes em outros artigos penais, inaugurando o que se convencionou chamar de Lei dos Crimes Cibernéticos (Teixeira et al., 2022, p.620).

No caso que deu origem à chamada Lei Carolina Dieckmann, não é metodologicamente adequado, nem juridicamente correto, centrar a análise na eventual "falta de cuidados pessoais" da atriz em matéria de segurança da informação; sob a ótica do Direito Penal e da proteção de dados, ela figura como vítima de condutas tipificadas, quais sejam: invasão de dispositivo informático, subtração de dados e divulgação não autorizada de conteúdo íntimo, sendo a **ilicitude** e a **reprovabilidade** concentradas na atuação de quem violou seu sistema, independentemente de eventuais fragilidades técnicas (como senhas fracas ou ausência de mecanismos adicionais de proteção).

Ainda que se reconheça, em termos técnicos, que boas práticas de segurança digital (uso de autenticação em dois fatores, criptografia, senhas robustas, atualização de sistemas etc.) podem reduzir vulnerabilidades, tais aspectos não transferem à vítima qualquer corresponsabilidade pelo crime, nem atenuam a gravidade da invasão.

Para fins deste trabalho, o episódio deve ser compreendido como marco legislativo que evidenciou a necessidade de tipificação específica de crimes cibernéticos, reforçando, de um lado, o dever do Estado de proteger usuários em ambiente digital e,

de outro, a responsabilidade ética e profissional dos especialistas em Tecnologia da Informação em projetar sistemas mais seguros e orientar adequadamente usuários e organizações, sem incorrer em culpabilização da vítima quando a violação decorre de conduta dolosa de terceiros.

## 6.1. Contexto Histórico e Motivações Normativas

Grande quantidade de escândalos envolvendo o vazamento de fotografias íntimas e crescente e diversa constatação de fraudes na utilização de aplicativos, sites e redes sociais, impulsionaram o Projeto de Lei nº 2.793/2011, convertido na Lei 12.737/2012.

> O novo diploma alterou dispositivos do Código Penal para coibir a interceptação sem consentimento e a interrupção de serviços telemáticos, conferindo densidade penal à proteção da inviolabilidade dos segredos na era da informação (Teixeira et al., 2022, p.622).

### 6.1.1. Principais Alterações Introduzidas

Face à sua aplicabilidade e relevância, criminaliza a invasão de dispositivo informático alheio, prevendo pena de reclusão de 1 a 4 anos, quando há prejuízo econômico (Brasil, Lei n.º 12.737/2012, art. 154-A).

> Também foram modificados o art. 266, para abranger a interrupção de serviço informático, e o art. 298, equiparando o cartão de crédito ou débito a documento particular, medida que permitiu qualificar a clonagem como falsificação (Teixeira et al., 2022, p.625).

## 6.2. Tipificação do Crime de Invasão de Dispositivo Informático

O cerne da Tipificação penal reside no verbo "invadir" utilizando-se da violação de mecanismo de segurança da informação com a finalidade específica de obter, adulterar

ou destruir dados ou instalar vulnerabilidades, conduta dolosa, que deve ser repreendida com rigor.

> A lei exige dolo direto, dispensando resultado naturalístico. Caso haja difusão ou comercialização dos dados obtidos, a pena é majorada em até dois terços, refletindo a gravidade do abalo à confiança na economia digital (Teixeira et al., 2022, p.630).

### 6.3. Interrupção de Serviço Informático ou Telemático

A redação vigente do art. 266 da referida lei tipifica a conduta daqueles que "interrompem, impedem ou dificultam o restabelecimento" de serviço telemático de utilidade pública, aumentando a tutela sobre portais governamentais e infraestruturas críticas de grande relevância social e econômica (Brasil, Lei n.º 12.737/2012, art. 266).

A Internet é reconhecida como serviço essencial, o que justifica a proteção penal reforçada. (Teixeira et al., 2022, p.633).

### 6.4. Falsificação de Cartão e Demais Crimes Correlatos

Para coibir as crescentes e diversificadas fraudes bancárias na rede muncial de computadores, o parágrafo único do art. 298 da lei em estudo, passou a equiparar cartões bancários a documentos particulares, ante a sua importância, efeito e relevância (Brasil, Lei n.º 12.737/2012, art. 298).

A falsificação ou clonagem de cartões, fenômeno potencializado por **malware** e esquemas de **phishing**, passou a sujeitar o infrator a pena de reclusão de 2 a 6 anos (Teixeira et al., 2022, p.635).

## 6.5. Técnicas Especiais de Investigação

A invasão virtual disposta no art. 190-A do Estatuto da Criança e do Adolescente, estendida aos crimes do art. 154-A, respalda o agente policial operar em ambiente virtual, quando e se autorizado judicialmente, o que pode ocorrer por até 90 dias, que poderão ser extendidos, devidamente justificados e fundamentados (Brasil, Lei n.º 12.737/2012, art. 154-A).

Tais mecanismos exigem cadeia de custódia rígida e observância ao devido processo, para que a prova digital preserve autenticidade e integridade (Brito et al., 2020, p.112).

## 6.6. Impactos Práticos e Desafios Jurídicos

A integração da Lei Federal 12.737/2012 assimilando-se os dispositivos posteriores, como a Lei Federal 14.155/2021, é essencial à manutenção da efetividade normativa, ante as novas e diversas modalidades criminosas.

> Mesmo com o reforço legal, o Brasil figura entre os países com maior incidência de fraudes digitais, exigindo políticas públicas que integrem educação digital, investimentos em cibersegurança e cooperação internacional em **cybercrime**. (Teixeira et al., 2022, p.633).

No contexto da Lei de Crimes Cibernéticos (Lei 12.737/2012 e demais dispositivos correlatos do CP e legislação especial), os principais problemas e desafios jurídicos não estão apenas na letra da lei, mas na forma como ela dialoga com a realidade técnica da Tecnologia da Informação.

Em primeiro lugar, há o desafio da tipificação e atualização normativa: a lei nasceu focada em condutas como invasão de dispositivo informático, violação de dados e fraudes eletrônicas, mas o cenário tecnológico evolui mais rápido do que o legislador

(ransomware, *phishing* sofisticado, *deepfakes*, *botnets*, engenharia social avançada etc.), o que gera lacunas, sobreposição de tipos penais e necessidade constante de interpretação extensiva pelos tribunais.

Em segundo lugar, existe o problema da atribuição de autoria e da prova digital: crimes cibernéticos podem ser praticados de forma remota, com uso de VPN, *proxies*, redes anônimas, dispositivos de terceiros e técnicas de mascaramento de IP, o que torna complexa a identificação do agente, a preservação da cadeia de custódia da prova e a compatibilização entre requisitos do Marco Civil, LGPD e normas processuais penais; aqui, decisões técnicas de arquitetura, logs e segurança, tomadas por profissionais de TI, têm impacto direto na viabilidade da persecução penal.

Um terceiro grupo de desafios diz respeito ao equilíbrio entre investigação e direitos fundamentais**:** para responsabilizar criminalmente o autor, muitas vezes é necessária a quebra de sigilo de dados de tráfego, registros de conexão e informações de contas, o que exige compatibilizar a tutela da intimidade, da privacidade e da proteção de dados (LGPD, CF, Marco Civil) com o dever estatal de investigar e punir delitos, sob controle rigoroso de legalidade, necessidade e proporcionalidade.

Soma-se a isso a discussão sobre a responsabilidade de intermediários e profissionais de TI**:** embora o núcleo do crime recaia sobre quem pratica a conduta ilícita, a jurisprudência tem considerado que a alta especialização técnica pode ser valorada negativamente quando usada para fins criminosos e, ao mesmo tempo, que a omissão grave em deveres de segurança, guarda de registros ou resposta a incidentes pode, em certos cenários, ter relevância penal (por exemplo, em hipóteses de dolo eventual ou participação).

Para o profissional de TI, isso se traduz no desafio de projetar sistemas e infraestruturas que sejam, ao mesmo tempo, seguros, conformes às leis e capazes de

cooperar com a justiça**,** assumindo um papel ativo na prevenção, documentação e mitigação de riscos, e não apenas na execução técnica de soluções.

## 7. RESPONSABILIDADES CIVIS DOS PROFISSIONAIS DE TI:

O aumento constante da dependência de sistemas de informação, tornou os profissionais de TI, cada vez mais expostos às consequências legais, civis e criminais, quando do tratamento, utilização e exposição de dados de pessoas e empresas.

Nesse âmbito, a atuação técnica dos citados profissionais, os projeta a efeitos jurídicos relevantes, pois falhas de configuração, vulnerabilidades ou descumprimento de políticas de segurança da informação, podem causar danos consideráveis a pessoas e empresas, o que gera o dever de indenizar.

> Este capítulo analisa os contornos da responsabilidade civil aplicável a esses profissionais à luz do ordenamento brasileiro, articulando dispositivos do Código Civil, da LGPD e de normas setoriais, bem como a doutrina especializada sobre o tema (Teixeira et al., 2025, p.248).

### 7.1. Fundamentos Legais da Responsabilidade Civil

O sistema jurídico adota, como regra, a responsabilidade subjetiva, ou seja, especificamente pessoal. Aquele que, por ato ilícito, por ação ou omissão, violar direito e causar dano a pessoas e empresas, fica obrigado a repará-los, assim dispõe o art. 186 do Código Civil. Já o art. 927, parágrafo único, prevê responsabilidade objetiva quando a atividade desenvolvida implicar risco para terceiros, logo poderão responder tantos as empresas responsáveis, quanto o profissional específico e causador do dano (Brasil, Lei n.º 10.406/2012, art. 186 e 927).

A operação cotidiana de redes, bancos de dados e infraestruturas críticas de TI enquadra-se nessa cláusula de risco, especialmente em ambientes de alta disponibilidade (Nunes, 2023, p.112).

### 7.1.1. Responsabilidade Subjetiva e Objetiva

Quando da prestação de serviços de TI, a responsabilização assume natureza contratual e/ou extracontratual. Em contratos de prestação de serviços técnicos especializados na área de TI, a culpa é aferida pela violação do dever de diligência técnica e pela inobservância de normas de segurança e legislação atinentes, que raramente é objeto de prioridade.

Contudo, quando a atividade envolver armazenamento massivo de dados sensíveis, a jurisprudência tem aplicado a responsabilidade objetiva, dada a presunção de risco inerente à atividade (Teixeira et al., 2025, p.97).

## 7.2. Responsabilidade Civil na LGPD

A LGPD assim dispõe em seu art. 42: o controlador ou operador responde por dano patrimonial, moral, individual ou coletivo decorrente de tratamento de dados realizado em desconformidade com a Lei Federal n.º 13.709.

A norma prevê cumplicidade entre os agentes técnicos envolvidos e admite excludentes de responsabilidade, quando provada a ausência de violação legal e normativa ou culpa exclusiva de terceiro.

Essa sistemática reforça a obrigação de adoção de medidas de prevenção e *compliance* pelos profissionais encarregados de arquitetar soluções tecnológicas (Tasso, 2020, p.104).

### 7.3. Responsabilidade Contratual dos Prestadores de Serviços de TI

Os contratos de prestação de serviços de TI, diligentemente devem contemplar cláusulas de delimitem de forma clara e objetiva os serviços a serem prestados, considerando as responsabilidades específicas, as obrigações, as garantias e quanto a confidencialidade.

O descumprimento de um (SLA), culminando em indisponibilidade de sistemas ou vazamento de dados, pode acarretar indenização calculada sobre perdas e danos efetivos e lucros cessantes, à luz dos arts. 389 e 927 do Código Civil (Leonardi, 2019, p.249).

### 7.4. Seguros de Riscos Cibernéticos e Mitigação de Danos

A Circular Superintendência de Seguros Privados (SUSEP) n.º 535/2016, alterada para incluir o ramo 27 – Riscos Cibernéticos, fomenta a transferência de parte do risco inerente às operações digitais.

A contratação de apólices capazes de cobrir custos de resposta a incidentes, multas regulatórias e responsabilidade civil reclamada por terceiros constitui boa prática recomendada aos profissionais e empresas de TI (Longhi, 2020, p.142).

### 7.5. Boas Práticas e ****Compliance****

O despertar e o nível de prioridade, que cada profissional e empresa, tiver com a consolidação de uma cultura profissional e empresarial, dedicada ao conhecimento e enquadramento no que diz respeito à legislação atinente, considerando todos os aspectos abarcados é o que proporcionara uma blindagem tal que proteja a atuação tanto do profissional de TI, quanto das empresas do ramo.

Planos de resposta a incidentes, registro de evidências e treinamento periódico das equipes formam o núcleo de um programa efetivo de governança de dados (Leonardi, 2019, p.101).

A responsabilidade civil e penal dos profissionais de TI é ampla e complexa, tendo que ser avaliada, considerando cada contexto específico e atual.

A legislação brasileira atinente, combina padrões de diligência técnica, cláusulas gerais de risco e deveres específicos de proteção de dados, impondo ao profissional a adoção de melhores práticas de segurança da informação e adequada gestão de rotinas e providências corporativas.

A prevenção, o seguro específico e a observância da legislação atinente, constituem o tríplice alicerce, necessário à mitigação de contingências e consolidar a confiança no ecossistema da TI.

## 8. RESPONSABILIDADES PENAIS DOS PROFISSIONAIS DE TI:

O aumentos, a complexidade e a diversificação das fraudes na rede mundial de computadores, os vazamentos de dados e ataques de negação de serviço, colocam os profissionais de TI severamente expostos às consequências jurídicas e econômicas.

Este capítulo apresenta os pressupostos dogmáticos da responsabilidade penal desses profissionais, conjugando dispositivos legais com a doutrina especializada (Pacheco, 2011, p.15).

### 8.1. Pressupostos Constitucionais e Penais

A Constituição Federal em sua redação vigente, consagra o princípio da legalidade estrita, que é a base estrutural do direito penal atinente. No contexto infraconstitucional,

o art. 18 do Código Penal diferencia: dolo e culpa, exigindo elemento volitivo para a tipificação penal coerente (Brasil, Decreto-Lei n.º 2.848/1940, art. 18).

Contudo, determinadas condutas omissivas vinculadas à garantia de segurança dos sistemas podem configurar crime culposo, por exemplo, se a negligência de um administrador resulta em dano a dados de terceiros (Teixeira et al., 2022, p.212).

### 8.1.1. Crimes Informáticos Tipificados no Código Penal

A Lei Federal n.º 12.737/2012 em seu o art. 154-A, criminaliza a invasão de dispositivo informático com violação de mecanismo de segurança ou instalação de vulnerabilidade, prevendo pena de reclusão de 1 a 4 anos quando resultante prejuízo econômico.

Também merece destaque o art. 266, §1º, que abrange a interrupção ou perturbação de serviço telemático de utilidade pública, frequente em cenários de **denial-of-service** distribuídos (Cruz et al., 2020, p.47).

## 8.2. Responsabilidade Penal do Administrador de Sistemas

O administrador de redes responde penalmente quando participa, direta ou indiretamente, da invasão ou da sabotagem de dispositivo informático, quando age com dolosamente de forma conivência e/ou omissiva.

> Se, porém, a violação resulta de falha na adoção de medidas mínimas de segurança, previamente exigidas por contrato ou política interna, a imputação poderá ocorrer em modalidade culposa, nos termos do art. 18, § 1º, do Código Penal (Teixeira et al., 2022, p.435).

### 8.3. Responsabilidade Penal do Desenvolvedor de TI

O desenvolvedor de TI incorre em ilícito se cria **malware** ou implementa funções ocultas para coleta, manipulação e utilização indevida de dados de pessoas e empresas.

Tal conduta enquadra-se no que dispõe o art. 154-B do Código Penal, que em sua redação pune a divulgação ou comercialização de favorecimentos ilícitos que visam permitir a invasão, prevista no artigo anterior (Brasil, Decreto-Lei n.º 2.848/1940, art. 154-B).

A doutrina sublinha que o dolo específico, finalidade de obter vantagem ilícita ou causar dano, deve restar comprovado (Lopes et al., 2023, p.301).

### 8.4. Delegação de Responsabilidades e Crime Empresarial

Em estruturas empresariais grandes e complexas, a responsabilização penal pode alcançar também diretores de TI, quando demonstrada a ciência sobre falhas críticas e a deliberação de não corrigi-las, logo conduta omissiva.

A teoria do domínio do fato, aplicada pelo Supremo Tribunal Federal, admite atribuição penal ao gestor que detém o poder de evitar o resultado lesivo, mas permanece inerte (Pacheco, 2011, p.88).

### 8.5. Excludentes de Ilicitude e Boas Práticas

Os restes de intrusão (**penetration testing**), quando previamente autorizados pelo controlador do sistema de TI, configuram exercício regular de direito, excluindo a ilicitude, desde que documentados de forma específica, adequada e coerente.

Já o acesso além do escopo combinado pode caracterizar *_over-reach_* doloso, retomando a Tipificidade do art. 154-A (Cruz et al., 2020, p.102).

### 8.6. *Compliance* Penal e Mitigação de Risco

Nesse contexto a responsabilização penal dos profissionais de TI reflete o reconhecimento de que a segurança da informação redunda-se em bem jurídico indispensável à ordem econômica e social. A legislação vigente e aspectos jurídicos correlatos, impõe não apenas a proibição de ações lesivas, como também o dever de prevenir ataques, vazamentos e utilizações indevidas. Assim necessário se faz que o conhecimento técnico jurídico deve caminhar em sintonia com a implantação e evolução da cultura ética, através de programas robustos de prevenção.

> Programas de *_compliance_* penal, alinhados à ISO 37001 e à ISO 27001, reduzem a exposição criminal dos profissionais e da empresa. Políticas claras de resposta a incidentes, logs imutáveis e trilhas de auditoria são ferramentas essenciais para demonstrar a diligência exigida pelo art. 13 do Código Penal quanto aos deveres de garantia. (Lopes et al., 2023, p.412).

## 9. JURISPRUDÊNCIA DO STJ EM TECNOLOGIA DA INFORMAÇÃO:

Esta seção trata de julgados relevantes do Superior Tribunal de Justiça.

**9.1. Desenvolvimento WEB e Direito Autoral.** BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 1.870.771/SP, Relator: Ministro Antonio Carlos Ferreira, Segunda Seção, julgado em 24 mar. 2021, DJe 30 mar. 2021 (Tema Repetitivo 1066). Disponível em: <https://processo.stj.jus.br>. Acesso em: 19 jun. 2025.

Na jurisprudência selecionada para o item 9.1, o STJ, ao julgar o REsp 1.870.771/SP sob o rito dos repetitivos (Tema 1066), enfrenta a controvérsia sobre a possibilidade de cobrança, pelo ECAD, de direitos autorais pela simples disponibilização de aparelhos de rádio e televisão em quartos de hotéis, motéis e estabelecimentos afins.

A Corte afirma que esses quartos são considerados “locais de frequência coletiva” para fins da Lei 9.610/98, de modo que a utilização de obras musicais e audiovisuais nesses ambientes configura execução pública, ainda que o uso seja individual pelo hóspede.

Além disso, o Tribunal afasta a alegação de “bis in idem”, ao entender que a contratação de TV por assinatura e o pagamento de direitos pela emissora não exoneram o empreendimento hoteleiro do dever de remunerar os titulares das obras, pois se trata de fato gerador distinto, vinculado à forma como o hotel incorpora essas obras à sua atividade econômica.

Do ponto de vista do profissional de Tecnologia da Informação, especialmente daquele que atua em desenvolvimento web e soluções digitais, o problema central evidenciado por esse precedente reside no reconhecimento de que a simples disponibilização de infraestrutura tecnológica, seja física (televisores, rádios) ou virtual (plataformas web, portais de *streaming*, aplicativos), pode configurar “utilização” de obras protegidas e atrair responsabilidade jurídica pelo uso não autorizado de conteúdo alheio.

A decisão reforça que não basta alegar que “quem transmite é o provedor de conteúdo” ou que “já existe um contrato com terceiros”: a forma como o serviço é estruturado e ofertado ao público (no caso, aos hóspedes) integra o modelo de negócios do tomador e gera um novo fato gerador em matéria de direitos autorais.

Em termos práticos, isso significa que o desenvolvedor web, o arquiteto de sistemas e o gestor de TI devem considerar, já na concepção de sites, plataformas e

ambientes digitais, as exigências de licenciamento, autorização prévia e repartição de responsabilidades contratuais, sob pena de expor o cliente, e em certos cenários também a si próprios, a litígios e condenações por violação de direitos autorais no ambiente digital.

**9.2. Lei Geral de Proteção de Dados.** BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 1.914.596/RJ, Relator: Ministro Luis Felipe Salomão, Quarta Turma, julgado em 23 nov. 2021, DJe 06 dez. 2021. Disponível em: <https://processo.stj.jus.br>. Acesso em: 19 jun. 2025.

Na jurisprudência selecionada para o item 9.2, o STJ analisa o REsp 1.914.596/RJ, em que familiares de Marielle Franco ajuizaram ação cominatória contra o Google Brasil visando, além da remoção de conteúdos ofensivos divulgados no YouTube, a identificação dos usuários responsáveis pelas publicações, para futura responsabilização civil e/ou criminal.

O Tribunal reconhece a necessidade de compatibilizar o Marco Civil da Internet com a Lei Geral de Proteção de Dados, afirmando que, havendo indícios de ilicitude e pedido específico para obtenção de dados cadastrais (nome, endereço, RG, CPF) a partir de IPs já fornecidos pelo provedor de aplicação, a privacidade do usuário não prevalece.

Nesse contexto, o STJ decide ser possível determinar que provedores de conexão forneçam dados cadastrais dos usuários ofensores, mesmo não tendo integrado a relação processual, por força do dever legal de guarda previsto nos arts. 10, §1º, e 22 do Marco Civil, afastando a tese de que isso significaria condenação de terceiros estranhos à lide.

Do ponto de vista do profissional de Tecnologia da Informação, o problema central evidenciado por esse precedente é que o modelo técnico de guarda e tratamento de dados (logs de conexão, registros de acesso, estruturação de IPs e dados cadastrais)

deixa de ser uma escolha meramente operacional e passa a ter consequências jurídicas diretas.

A decisão reforça que provedores de aplicação e de conexão devem manter registros em condições de permitir a identificação efetiva de usuários, de forma segura e em conformidade com o Marco Civil e a LGPD, sabendo que esses dados poderão ser compartilhados com o Poder Judiciário como base em obrigação legal e exercício regular de direito, quando presentes indícios de ilícito.

Isso exige do engenheiro de computação e demais profissionais de TI uma atuação atenta à governança de logs, à definição de prazos e camadas de acesso, à documentação das bases legais de tratamento e ao desenho de arquiteturas que conciliem minimização de dados e proteção da privacidade com a possibilidade de rastreabilidade e responsabilização de abusos no ambiente digital.

**9.3. Marco Civil da Internet.** BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 1.784.156/SP, Relator: Ministro Marco Aurélio Bellizze, Terceira Turma, julgado em 5 nov. 2019, DJe 21 nov. 2019. Disponível em: <https://processo.stj.jus.br>. Acesso em: 19 jun. 2025.

Na jurisprudência selecionada para o item 9.3, o STJ, ao julgar o REsp 1.784.156/SP, discute a extensão da obrigação, prevista no Marco Civil da Internet, de guarda e fornecimento de registros de acesso por parte dos provedores de aplicações.

O caso envolve a TIM (provedora de conexão) e o Google (provedor de aplicações), em ação de obrigação de fazer proposta para identificar o responsável pela disponibilização de conteúdo ilícito relacionado à adesão irregular ao plano TIM Beta.

A controvérsia central consiste em saber se, além do endereço IP, o provedor de aplicações está obrigado a armazenar e fornecer também a “porta lógica de origem”

associada a IPs da versão IPv4, diante do cenário de esgotamento desses endereços e do uso de técnicas de compartilhamento (NAT), que tornam insuficiente o IP isoladamente para individualizar o terminal.

O STJ, em interpretação teleológica dos arts. 5º, VIII, 10 e 15 do Marco Civil, conclui que, enquanto perdurar o uso de IPv4 compartilhado, a porta lógica integra, na prática, o próprio dado de acesso à aplicação, devendo ser guardada e fornecida sob ordem judicial, sob pena de esvaziar a finalidade da lei de viabilizar a identificação de autores de ilícitos no ambiente digital.

Para o profissional de Tecnologia da Informação, o problema central evidenciado por esse precedente é que decisões de arquitetura de rede e de registro de logs deixam de ser meramente técnicas e passam a ter consequências jurídicas diretas.

Ao afirmar que tanto provedores de conexão quanto de aplicação devem adaptar seus sistemas para armazenar, de forma segura e íntegra, não só IP, data e hora, mas também a porta lógica de origem nos ambientes com IPv4 compartilhado, o STJ reforça que o engenheiro de computação e demais profissionais de TI têm o dever de projetar infraestruturas e bases de logs compatíveis com as exigências do Marco Civil, garantindo rastreabilidade suficiente para a identificação de usuários em investigações civis e criminais, sem violar indevidamente a privacidade.

Isso implica planejar políticas de guarda, formatos de registro, mecanismos de proteção dos dados e fluxos de atendimento a ordens judiciais, sob pena de expor a organização e, em certas hipóteses, o próprio profissional responsável – a riscos de responsabilidade por omissão, impossibilidade de cumprimento de decisões judiciais e eventual frustração da persecução de ilícitos praticados por meio de seus sistemas.

**9.4. Lei Carolina Dieckmann – Crimes Cibernéticos. Lei Carolina Dieckmann – Crimes Cibernéticos.** BRASIL. Superior Tribunal de Justiça. Habeas Corpus n. 351.013/BA, Relator: Ministro Reynaldo Soares da Fonseca, Quinta Turma, julgado em 29 jun. 2016. Disponível em: <https://processo.stj.jus.br>. Acesso em: 19 jun. 2025.

Na jurisprudência analisada no item 9.4, o STJ examina habeas corpus impetrado em favor de acusado apontado como líder de organização criminosa altamente especializada em fraudes bancárias realizadas pela internet, envolvendo, entre outros delitos, invasão de dispositivo informático (art. 154-A do Código Penal, introduzido pela Lei 12.737/2012 – Lei Carolina Dieckmann), furto qualificado mediante informática, falsificação de documento particular e organização criminosa.

Ao manter a prisão preventiva, a Quinta Turma destaca a estruturação do grupo, o uso de técnicas sofisticadas para burlar sistemas de internet banking, o elevado prejuízo causado a instituições financeiras e correntistas, bem como o risco concreto de reiteração delitiva, enfatizando que, em crimes cibernéticos dessa natureza, “basta uma máquina com acesso à rede mundial de computadores” para que o agente retome suas atividades ilícitas, o que justifica a custódia como forma de garantir a ordem pública e desarticular a organização.

Do ponto de vista do profissional de Tecnologia da Informação, o problema central evidenciado por esse precedente é que a elevada especialização técnica em redes, segurança e sistemas de informação deixa de ser elemento neutro: quando empregada para fins ilícitos, ela é valorizada negativamente pelo Judiciário como fator de maior periculosidade e reprovabilidade.

A decisão sinaliza que o engenheiro de computação e demais profissionais de TI não são vistos apenas como “usuários avançados”, mas como agentes cuja expertise pode agravar o juízo sobre o risco de reiteração e fundamentar medidas cautelares mais severas.

No plano preventivo, isso reforça a exigência de uma atuação profissional pautada por ética, *compliance* e segurança da informação, em estrita observância à Lei Carolina Dieckmann e ao restante do ordenamento penal, sob pena de o uso desviado do conhecimento técnico resultar não apenas em danos econômicos relevantes, mas em graves consequências na esfera da liberdade pessoal.

**9.5. Responsabilidade Civil dos Profissionais de TI.** BRASIL. Superior Tribunal de Justiça. Agravo em Recurso Especial n. 2.130.619/SP, Relator: Ministro Francisco Falcão, Segunda Turma, julgado em 17 mar. 2023, DJe 27 mar. 2023. Disponível em: <https://processo.stj.jus.br>. Acesso em: 19 jun. 2025.

Na jurisprudência selecionada para o item 9.5, o STJ, ao julgar o AREsp 2.130.619/SP, analisa ação indenizatória proposta por consumidora contra concessionária de energia elétrica em razão do vazamento de seus dados pessoais (nome, RG, gênero, data de nascimento, telefones, endereço e informações contratuais como carga instalada e consumo estimado).

A Corte de origem havia reconhecido dano moral presumido, sobretudo por se tratar de pessoa idosa, mas o STJ reforma o acórdão e restabelece a sentença de improcedência, firmando dois pontos centrais:

a) os dados vazados são dados pessoais comuns, e não dados sensíveis, à luz do art. 5º, II, da LGPD;

b) o simples vazamento de dados pessoais comuns, embora configure falha indesejável no tratamento de dados, não gera automaticamente dano moral indenizável, exigindo-se prova concreta de lesão à esfera de direitos da personalidade.

Assim, o Tribunal afasta a ideia de dano moral in re ipsa para esse tipo de incidente e diferencia, de forma clara, a gravidade jurídica do vazamento de dados sensíveis em relação a dados meramente identificadores.

Do ponto de vista do profissional de Tecnologia da Informação, o problema central evidenciado por esse precedente é a necessidade de compreender que a responsabilidade civil decorrente de incidentes de segurança em dados pessoais é construída a partir de uma combinação entre classificação adequada dos dados**,** medidas técnicas de proteção **e** demonstração de efetivo prejuízo.

A decisão não “autoriza” descuido com segurança da informação; ao contrário, ela reforça que vazamentos de dados comuns continuam sendo falhas relevantes de tratamento sob a LGPD e podem gerar outras consequências (administrativas, contratuais, reputacionais).

Contudo, sob o ângulo indenizatório, o STJ sinaliza que nem todo incidente de segurança implicará, por si só, obrigação de indenizar por dano moral, o que torna ainda mais importante que o engenheiro de computação e demais profissionais de TI documentem políticas de segurança, gestão de riscos, registros de incidentes e esforços de mitigação.

Em termos práticos, a atuação técnica passa a dialogar diretamente com a avaliação judicial de culpa, nexo causal e extensão do dano, exigindo do profissional de TI uma postura alinhada à governança de dados e ao cumprimento diligente das exigências da LGPD, sob pena de ver sua atuação questionada em demandas indenizatórias.

## 10. CONCLUSÃO:

O presente trabalho buscou responder à questão de pesquisa no sentido de que o profissional de TI pode atuar de forma a evitar falhas jurídicas e, por consequência, reduzir o risco de condenações civis e penais quando estrutura sua prática sobre três eixos indissociáveis, que demanda incontinente atualização:

a) **domínio técnico com foco em segurança da informação**, adotando medidas como controle de acessos, criptografia, monitoramento de incidentes e políticas formais de proteção de dados, em linha com os pilares de confidencialidade, integridade e disponibilidade;

**b) observância sistemática do arcabouço normativo aplicável à área**, em especial LGPD, Marco Civil da Internet, Lei dos Crimes Cibernéticos, Código Civil e Código Penal, compreendendo que o tratamento inadequado de dados, o desenvolvimento de sistemas inseguros ou o descumprimento contratual podem gerar responsabilidade subjetiva ou objetiva e danos patrimoniais e morais a usuários e organizações;

**c) implantação de uma cultura contínua de *compliance* digital e governança**, que envolva contratos e SLAs bem redigidos, definição clara de papéis (controlador, operador, encarregado), capacitação permanente das equipes, análise de jurisprudência dos tribunais superiores e adoção de boas práticas de auditoria, registro e prestação de contas.

Nesse modelo preventivo e estratégico, o profissional de TI deixa de atuar apenas como executor técnico e passa a se posicionar como agente consciente de seus deveres legais, alinhando inovação tecnológica, Métodologia científica e responsabilidade jurídica, o que permite mitigar riscos, reforçar a confiança social na tecnologia e sustentar juridicamente sua atuação profissional e empresarial.

Os objetivos específicos foram alcançados ao se mapear os principais desafios legais, identificar os riscos associados à proteção de dados, contratos e propriedade intelectual, e analisar as jurisprudências do STJ que evidenciam a crescente responsabilização dos profissionais de TI.

Constatou-se que a implantação de políticas de *compliance* e segurança da informação são fundamentais para prevenir infrações e fortalecer a governança tecnológica de resultados adequados.

Assim, conclui-se que a responsabilidade do profissional de Tecnologia da Informação ultrapassa o aspecto estritamente técnico, exigindo postura ética, proativa e alinhada à legislação vigente. O êxito nessa área pressupõe a integração consistente entre soluções tecnológicas, observância dos aspectos legais e adequada gestão de riscos, de modo a conferir segurança, conformidade e sustentabilidade à atuação profissional.

**Para continuidade desta pesquisa sugere-se os seguintes trabalhos futuros:**

- Painel jurisprudencial aplicado (STJ/STF + ANPD) sobre responsabilização em TI;

- Estudo de maturidade de compliance e segurança (ABNT NBR ISO/IEC 27001, ISO 37001, NIST CSF) em organizações de TI;

- Framework contratual e de SLA “LGPD-*first*” para serviços de TI;

## 11 - REFERÊNCIAS BIBLIOGRÁFICAS:


BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Marco Civil da Internet. *Diário Oficial da União*, Brasília, DF, 24 abr. 2014.

BRASIL. Lei n.º 12.737. de 30 de novembro de 2012. Tipificação Criminal de Delitos Informáticos. Lei Carolina Dieckmann. *Diário Oficial da União*, Brasília, DF, 3 dez. 2012.

BRASIL. Decreto-Lei n.º 2.848. de 7 de dezembro de 1940. Código Penal. *Diário Oficial da União*, Brasília, DF, 3 jan. 1941.

BRASIL. Lei n.º 10.406. de 10 de janeiro de 2002. Código Civil *Diário Oficial da União*, Brasília, DF, 11 jan. 2002.

BASAN, Arthur Pinheiro. Publicidade Digital e Proteção de Dados Pessoais. São Paulo. Editora Foco, 2021.

BISCALCHIN, Ana Carolina Silva; ALMEIDA, Marco Antônio de. Direitos Autorais, Informação e Tecnologia: Impasses E Potencialidades. Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict), desenvolvido em associação com a Universidade Federal do Rio de Janeiro (UFRJ). São Paulo. 2021. Disponível em: https://revista.ibict.br/liinc/article/view/3310. Acesso em: 16 jun. 2025.

BRITO CRUZ, Francisco; FRAGOSO, Nathalie (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. III. São Paulo. InternetLab, 2020.

CASTANHEIRA, Henrique Almeida Bazan. Provedores de Aplicação, Direitos Fundamentais e Responsabilidade Civil por Conteúdos de Terceiros.

Mestrado (Direito). Universidade Federal de Minas Gerais, Belo Horizonte. Disponível em:https://sucupira-legado.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=16808757. Acesso em: 7 jun. 2025.

Carneiro FILHO, Alexandre Jorge et al., Direito Digital e Proteção de Dados Pessoais. São Paulo. Escola Paulista de Magistratura, 2020.

FRANCO, Ticiane Moraes. Marco civil da Internet: a neutralidade de rede na perspectiva das telecomunicações. Mestrado (Direito nas Relações Econômicas e Sociais Instituição de Ensino). Faculdade de Direito Milton Campos. Nova Lima. 2024. Disponível em: https://sucupira-legado.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=1507001. Acesso em: 17 junho 2025.

GUIMARÃES, Clayton Douglas Pereira; GUIMARÃES, Glayber Daywerth Pereira; FILHO, Pedro Alberto Alves Marciel; QUINELATO, Pietra Daneluzzi. Associação Guimarães de Estudos Jurídicos, 2022.

LIMA, Ana Paula Moraes; ALMEIDA, Dionice; MAROSO, Eduardo Pereira. LGPD – Lei Geral de Proteção de Dados. São Paulo. Literare Books International, 2020.

LONGHI, João Victor Rozatti; JÚNIOR, José Luiz de Moura Faleiros; BORGES, Gabriel Oliveira de Aguiar; REIS, Guilherme. Fundamentos do Direito Digital. São Paulo. LAECC – Laboratório Americano de Estudos Constitucionais Comparados, 2020.

LOPES, Alan Moreira; SANTOS, Keila; TEIXEIRA, Tarcisio. Direito Digital: Teoria e Prática. São Paulo. TIrant Lo Blanch, 2021.

MARCHIONI, Artur. A Responsabilização das Plataformas Digitais Sobre o Conteúdo Postado por Terceiros: Possibilidades no Enfrentamento a Disseminação de Discurso de Ódio. Dissetação (Mestrado em Direito). Universidade Estadual Paulista Júlio de Mesquita Filho (Franca). 2023,
Disponível em: https://sucupira-legado.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=13904739. Acesso em: 3 jun. 2025.

PACHECO, Wilfredo. Crimes Digitais: Responsabilidade Penal de Hackers, Crackers e Engenheiros Sociais. 1ª Edição, 2011.

RONHA, Amanda Nunes. *Compliance* Digital e Segurança da Informação: Desafios Impostos pela Lei Geral de Proteção de Dados. Dissertação (Mestrado em Direito da Sociedade da Informação). Centro Universitário das Faculdades Metropolitanas Unidas, São Paulo, 2021. Disponível em: https://sucupira-legado.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=11102852. Acesso em: 1 jun. 2025.

SCALQUETTE, Ana Cláudia; VANZOLINA, Patrícia; ROCHA, Renata; SCALQUETE, Rodrigo Arnoni. Inteligência Artificial: Uso de Dados Pessoais. São Paulo. Almedina Brasil, 2022.

TEIXEIRA, Tarcísio. Direito Digital e Processo Eletrônico. 6ª Edição. São Paulo. SaraivaJur, 2022.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR

Av. Universitária, 1069 ● Setor Universitário
Caixa Postal 86 ● CEP 74605-010
Goiânia ● Goiás ● Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br ● reitoria@pucgoias.edu.br

# RESOLUÇÃO n° 038/2020 – CEPE

## ANEXO I

APÊNDICE ao TCC

## Termo de autorização de publicação de produção acadêmica

O estudante Paulo Henrique de Toledo Cardoso do Curso de Engenharia da Computação, matrícula 20231003300589, telefone: 62 984462170 e-mail paulohtcengcomp@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do Autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado Responsabilidade Civil e Penal dos Profissionais de TI, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto(PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 16 de Setembro de 2025.

Assinatura do autor: PAULO HENRIQUE DE TOLEDO CARDOSO:80890059187

Assinado digitalmente por PAULO HENRIQUE DE TOLEDO CARDOSO:80890059187
ND: C=BR, O=ICP-Brasil, OU=AC SOLUTI Multipla v5, OU=Renovacao Eletronica, OU=Certificado Digital, OU=Certificado PF A3, CN=PAULO HENRIQUE DE TOLEDO CARDOSO:80890059187
Razão: Eu sou o autor deste documento
Localização:
Data: 2025.09.16 14:27:17-03'00'
Foxit PDF Reader Versão: 2024.4.0

Nome completo do autor: Paulo Henrique de Toledo Cardoso

Assinatura do professor–orientador: __SOLANGE DA SILVA

Nome completo do professor-orientador: _

gov.br
Documento assinado digitalmente
SOLANGE DA SILVA
Data: 16/09/2025 19:58:29-0300
Verifique em https://validar.iti.gov.br

-