FACULDADES INTEGRADAS RUI BARBOSA – FIRB

ANA JÚLIA CITRO PEREIRA DE SOUZA

O DIREITO DIGITAL NO ORDENAMENTO JURÍDICO BRASILEIRO

Andradina–SP
Junho/2024

FACULDADES INTEGRADAS RUI BARBOSA — FIRB

ANA JÚLIA CITRO PEREIRA DE SOUZA

O DIREITO DIGITAL NO ORDENAMENTO JURÍDICO BRASILEIRO

Trabalho de Conclusão de Curso apresentado nas Faculdades Integradas Rui Barbosa – FIRB, sob orientação do Professor Doutor Angelo Raphael Mattos, como requisito parcial para obtenção do título de bacharel em Direito.

Andradina–SP

Junho/2024

Ana Júlia Citro Pereira de Souza

O DIREITO DIGITAL NO ORDENAMENTO JURÍDICO BRASILEIRO

Trabalho de Conclusão de Curso apresentado à banca examinadora como requisito parcial para obtenção do Bacharelado em Direito nas Faculdades Integradas Rui Barbosa – FIRB. Defendido e aprovado em ___ de _____ de 2024 pela banca examinadora constituída por:

Prof. Dr. Angelo Raphael Mattos (Orientador)
Instituição: Faculdades Integradas Rui Barbosa - FIRB

Profa. _____
Instituição: Faculdades Integradas Rui Barbosa - FIRB

Profa. _____
Instituição: Faculdades Integradas Rui Barbosa – FIRB

NOTA: ( ) Aprovado ( ) Reprovado

Andradina, ___ de _____ de 2024

A minha avó Vera, que queria que eu fosse escritora, mas me apaixonei pelo Direito.

AGRADECIMENTOS

Gostaria de expressar meus sinceros agradecimentos a todos que contribuíram para a realização deste trabalho. A minha família, ao meu noivo, e ao meu professor orientador Raphael. Sem o apoio de vocês, eu não teria alcançado este resultado. Agradeço também pelo incentivo, orientação e suporte ao longo do caminho, que foram fundamentais para o sucesso da pesquisa. Muito obrigada!

Hoje, o medo da exposição foi abafado
pela alegria de ser notado.
Zygmunt Bauman

RESUMO

O presente trabalho analisa o cenário digital nacional e apresenta algumas questões sobre essa seara por meio de leis, regulamentos e jurisprudência associados ao ambiente das tecnologias e das redes sociais. Neste contexto, com o desenvolvimento de novas tecnologias, novas esferas de aplicação fundamentada e do desenvolvimento do Direito Digital, as bases teóricas e normativas precisam seguir avançando. A legislação que rege este campo é baseada, em especial, na Lei Geral de Proteção de Dados e no Marco Civil da Internet, decisões relevantes dos tribunais e acordos internacionais. Para a implementação da base teórica do Direito Digital no Brasil, e para o desenvolvimento desta pesquisa, como metodologia, utilizou-se da legislação pertinente, jurisprudência e da revisão bibliográfica.

Palavras-chave: Direito Digital. Internet. Lei Geral de Proteção de Dados. Brasil.

ABSTRACT

This work analyzes the national digital scenario and presents some questions about this field through laws, regulations and jurisprudence associated with the technology and social media environment. In this context, with the development of new technologies, new spheres of grounded application and the development of Digital Law, the theoretical and normative bases need to continue advancing. The legislation that governs this field is based, in particular, on the General Data Protection Law and the Internet Civil Framework, relevant court decisions and international agreements. To implement the theoretical basis of Digital Law in Brazil, and for the development of this research, as a methodology, the relevant legislation, jurisprudence and bibliographic review were used.

Keywords: Digital Law. Internet. General Data Protection Law. Brazil.

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
DPO	*Data Protection Officer*
ECA	Estatuto da Criança e do Adolescente
GDPR	Regulamento Geral de Proteção de Dados
LGPD	Lei Geral de Proteção de Dados
TICs	Tecnologias da Informação e Comunicações

LISTA DE TABELAS

SUMÁRIO

1 Introdução

O Direito Digital no ordenamento jurídico brasileiro refere-se ao conjunto de leis, regulamentos e jurisprudência que governam as atividades e relações no ambiente digital no Brasil. Este campo abrange uma ampla gama de questões legais relacionadas à internet, tecnologia da informação, proteção de dados, crimes cibernéticos, propriedade intelectual online, comércio eletrônico, entre outros. Diante da evidência de que o avanço tecnológico é inafastável, as bases teóricas tradicionais precisam ser revisadas e novos institutos jurídicos precisam ser aprofundados para abranger os crimes que podem ser praticados no ‘’mundo digital’’, principalmente com a utilização das Tecnologias da Informação e Comunicações (TICs), que incorporam um novo modus vivendi (Berni, 2022).

No Brasil, o Direito Digital é uma área em constante evolução devido ao rápido avanço da tecnologia e da internet, o que demanda uma adaptação constante das leis e regulamentações para lidar com novos desafios e questões emergentes. Algumas das principais leis e regulamentos que regem o Direito Digital no Brasil incluem a Lei Geral de Proteção de Dados (LGPD): Lei nº 13.709/2018, que regula o tratamento de dados pessoais por organizações públicas e privadas; o Marco Civil da Internet, Lei nº 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil; o Código Penal Brasileiro, que contém disposições relacionadas a crimes cibernéticos, como fraudes eletrônicas, invasão de dispositivos, difamação online, entre outros; e o Estatuto da Criança e do Adolescente (ECA), que possui disposições relacionadas à proteção de crianças e adolescentes no ambiente digital, como a prevenção da exploração sexual infantil online. Além dessas leis, o Direito Digital no Brasil também é influenciado por decisões judiciais, regulamentações específicas de órgãos governamentais, tratados internacionais e ações de autorregulação de empresas do setor.

Foi utilizada metodologia de revisão bibliográfica, que é um processo sistemático que envolve várias etapas essenciais para a coleta, análise e síntese de fontes de informação relevantes para o tema em questão, fornecendo uma base sólida para a pesquisa e contribuindo significativamente para o desenvolvimento do trabalho acadêmico.

O texto está estruturado de forma organizada, abordando diferentes aspectos do direito digital em capítulos.

No capítulo 2, intitulada "O Direito Digital", são explorados diversos tópicos essenciais, começando com uma discussão sobre a Lei de Proteção de Dados Pessoais (LGPD), seguida pelo Marco Civil da Internet, Cibersegurança e Responsabilidade Civil, Privacidade na Internet e Liberdade de Expressão Online.

Em seguida, no capítulo 3, denominada "Cyberspace, Comércio Eletrônico e Contratos Digitais", são tratados assuntos relacionados ao comércio eletrônico e ao ambiente digital, incluindo questões de Direitos Autorais e Propriedade Intelectual, Tecnologias Emergentes e Jurisdição Transnacional no Ciberespaço.

Por fim, no capítulo 4, intitulado "Jurisprudência e Direito Digital", são analisados casos judiciais relevantes que envolvem questões digitais, como os casos do Google, WhatsApp, Discord e da Carolina Dieckmann, fornecendo exemplos concretos de como o direito digital é aplicado na prática. Essa estrutura permite uma abordagem abrangente e detalhada do tema, explorando tanto aspectos teóricos quanto casos práticos e jurisprudências.

2 O Direito Digital

O advento da era digital transformou profundamente a maneira como interagimos, comunicamos e conduzimos negócios. Essas mudanças se atrelam a um desenvolvimento do espaço virtual conhecido como Internet, definido pela seguinte forma pela Lei nº 12.965/2014, do instituto do Marco Civil da Internet, em seu art. 5º. Nesse contexto, o Direito Digital emerge como um campo essencial para regulamentar e proteger os direitos e responsabilidades dos indivíduos e organizações que operam no ciberespaço. (Rodrigues, 2022).

A legislação brasileira acompanhou essa evolução, promulgando normativas cruciais para adaptar o ordenamento jurídico às complexidades do ambiente digital. Uma das mais notáveis é a Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em 2020. Esta lei representa um marco na proteção da privacidade e segurança dos dados pessoais, estabelecendo regras claras para a coleta, processamento e armazenamento de informações.

> A LGPD complementa, harmoniza e unifica um ecossistema de mais de quarenta normas setoriais que regulam, de forma direta e indireta, a proteção da privacidade e dos dados pessoais no Brasil. Foi inspirada nas discussões que culminaram na GDPR europeia e tem por objetivo não apenas conferir às pessoas maior controle sobre seus dados, mas também fomentar um ambiente de desenvolvimento econômico e tecnológico, mediante regras flexíveis e adequadas para lidar com os mais inovadores modelos de negócio baseados no uso de dados pessoais. Isso inclui modelos de negócio que se valem de algoritmos para auxiliar na tomada de decisões automatizadas. A LGPD também busca equilibrar interesses econômicos e sociais, garantindo a continuidade de decisões automatizadas e também limitando abusos nesse processo, por meio da diminuição da assimetria de informações, e, por consequência, de poder, entre o indivíduo, setor privado e o Estado (Monteiro, 2018, p. 9).

Além disso, o Brasil também é pioneiro na adoção do Marco Civil da Internet, lei citada acima, uma legislação inovadora que estabelece princípios fundamentais para o uso da rede no país. Entre esses princípios, destacam-se a neutralidade de rede, a proteção da privacidade e a responsabilidade dos provedores de serviços online.

O Código Penal Brasileiro também desempenha um papel significativo no contexto do Direito Digital, pois contém disposições que abordam diversas formas de crimes cibernéticos e outras infrações relacionadas ao uso da tecnologia da informação e da internet. Essas disposições visam proteger os direitos dos cidadãos

e garantir a segurança e a integridade do ambiente digital. Alguns pontos-chave sobre o papel do Código Penal Brasileiro no Direito Digital são; as tipificações de crimes cibernéticos, como invasão de dispositivo informatico (art.154-A), interceptação ilegal de comunicações (art. 151), difusão de vírus de computador (art. 264-A) e outros; proteção contra fraudes eletrônicas, como estelionato (art. 171) e falsificação de documentos digitais (art. 298); a responsabilização por crimes cometidos online, seja na qualidade de autores, coautores ou partícipes das condutas ilícitas, garantindo a punição adequada para quem viola a lei no ambiente digital; sanções penais para crimes cibernéticos, que podem incluir penas de detenção ou reclusão, além de multas, de acordo com a gravidade da conduta e as circunstâncias do caso; e a proteção de direitos fundamentais no ambiente digital, como o direito à privacidade, à liberdade de expressão e à segurança da informação, estabelecendo limites para condutas que possam violar esses direitos. (Cassanti, 2014).

No entanto, apesar dos avanços significativos, o Direito Digital no Brasil enfrenta desafios complexos. Questões como cibersegurança, combate à disseminação de fake news, proteção contra ataques cibernéticos e regulamentação de novas tecnologias, como a inteligência artificial, demandam atenção e atualizações constantes na legislação. A Internet é tanto um instrumento capaz de promover quanto de violar Direitos Humanos. (OAB/RS, 2020 apud Piovesan, 2020).

Além disso, a rápida evolução tecnológica muitas vezes supera a capacidade do sistema legal em acompanhar e regular adequadamente as inovações digitais. Os crimes cibernéticos estão cada vez mais presentes na sociedade, se manifestando das mais diferentes formas, causando diversas vítimas, com isso, é importante compreendermos melhor sobre os principais tipos de crimes cibernéticos praticados atualmente. Portanto, é essencial que os legisladores e profissionais do Direito estejam atentos a essas mudanças e trabalhem em conjunto para desenvolver soluções eficazes e equitativas. (Araújo, 2023).

O Direito Digital no Brasil desempenha um papel crucial na proteção dos direitos dos cidadãos e na promoção de um ambiente digital seguro e ético. A contínua evolução nesse campo é fundamental para garantir que as leis e regulamentações acompanhem o ritmo das inovações tecnológicas e protejam adequadamente os interesses de todos os envolvidos no ecossistema digital brasileiro.

2.1 Lei de Proteção de Dados Pessoais (LGPD)

A crescente digitalização da sociedade contemporânea trouxe consigo uma imensa quantidade de dados pessoais sendo coletados, processados e compartilhados a uma velocidade sem precedentes. Em resposta a esse cenário, legisladores em todo o mundo têm trabalhado para estabelecer diretrizes claras e robustas para proteger a privacidade e os direitos individuais. Uma das leis mais significativas nesse contexto é a Lei Geral de Proteção de Dados (LGPD).

Promulgada no Brasil em setembro de 2020, a LGPD representa um marco essencial na proteção dos dados pessoais dos cidadãos. A lei estabelece princípios fundamentais, como o consentimento explícito para a coleta de dados, a transparência no tratamento das informações e a garantia do direito de acesso e correção dos dados por parte dos titulares. A LGPD também busca equilibrar interesses econômicos e sociais, visando garantir a continuidade de decisões automatizadas e também limitando abusos nesse processo, por meio da diminuição da assimetria de informações, e, por consequência, de poder, entre o indivíduo, setor privado e o Estado. (Monteiro, 2018).

> A LGPD garante aos indivíduos o direito a ter acesso a informações sobre que tipos de dados pessoais seus são utilizados para alimentar algoritmos responsáveis por decisões automatizadas. Caso o processo automatizado tenha por finalidade formar perfis comportamentais ou se valha de um perfil comportamental para tomar uma decisão subsequente, essa previsão também incluirá o acesso aos dados anonimizados utilizados para enriquecer tais perfis.
>
> Esse direito ainda inclui a possibilidade de conhecer os critérios utilizados para tomar a decisão automatizada e de solicitar a revisão da decisão por um ser humano quando está afetando os interesses dos titulares. (Monteiro, 2018, p. 11).

Além disso, a LGPD impõe responsabilidades claras às organizações que lidam com dados pessoais. Elas são obrigadas a implementar medidas de segurança para proteger essas informações contra acessos não autorizados e vazamentos, bem claro em seu artigo 19; “A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular" e será dada “por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular”. Monteiro ainda explica que o princípio da transparência deve reger toda e qualquer relação do responsável pelo tratamento de dados pessoais com o titular dos dados, garantindo a este o direito de acesso aos seus dados pessoais. Esse princípio também pressupõe o dever de informar os critérios de tratamentos utilizados para finalidades informadas ao titular. (Monteiro, 2018).

A lei também introduz a figura do Encarregado de Proteção de Dados ou nos termos da *General Data Protection Regulation* (GDPR), o *Data Protection Officer – DPO*, que tem sua função definida no art. 5º, inciso VIII, da Lei nº 13.853/2019:

> Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Desde 2016, a GDPR regulamenta a proteção da identidade e dados pessoais dos cidadãos da União Europeia. Quando mencionamos dados, estamos nos referindo às informações geradas pelas pessoas tanto no ambiente online quanto físico. Exemplos comuns incluem nome, CPF, e-mail e número de celular, porém o conceito abrange também informações sensíveis como orientação política e condições de saúde. (Baldissera, 2021).

O Encarregado de Dados, também conhecido como *Data Protection Officer* (DPO) em inglês, é uma figura essencial no âmbito da proteção de dados, especialmente em conformidade com regulamentações como a LGPD no Brasil e o GDPR na União Europeia. Sua função principal é garantir que a organização cumpra as leis de proteção de dados e promova uma cultura de privacidade dentro da empresa.

Entre as responsabilidades do DPO estão o monitoramento da conformidade, onde o DPO é encarregado de garantir que a organização esteja em conformidade com as leis de proteção de dados, como a LGPD ou o GDPR, e outras regulamentações aplicáveis. Isso envolve monitorar as práticas de coleta, processamento e armazenamento de dados para garantir que estejam em conformidade com os requisitos legais. Eles fornecem aconselhamento e orientação à organização, a seus funcionários e contratados sobre as obrigações legais de proteção de dados. Isso inclui ajudar na interpretação das leis de proteção de dados, fornecer diretrizes sobre boas práticas de privacidade e responder a dúvidas e consultas relacionadas à proteção de dados. (Baldissera, 2012).

Fazem a gestão de incidentes em caso de violação de dados pessoais, desempenhando um papel fundamental na coordenação da resposta da organização. Isso inclui avaliar a gravidade do incidente, notificar as autoridades competentes quando necessário e coordenar as medidas corretivas e de mitigação para resolver o incidente e minimizar seus impactos. Eles mantêm contato com autoridades reguladoras de proteção de dados, como a Autoridade Nacional de Proteção de Dados (ANPD) no Brasil. O DPO representa a organização em questões relacionadas à proteção de dados e responde a solicitações e investigações das autoridades reguladoras. (Baldissera, 2021).

O DPO é responsável por promover uma cultura de privacidade dentro da organização, fornecendo treinamento e conscientização sobre questões de proteção de dados para funcionários e contratados. Isso inclui treinamento sobre as leis de proteção de dados, procedimentos internos de privacidade e melhores práticas para proteger dados pessoais.

Por fim, é importante ressaltar que existem duas maneiras de se trabalhar como DPO, o DPO Interno, que realiza o trabalho de implementação de um sistema interno de proteção de dados em uma organização para garantir conformidade com a LGPD, sendo responsável por supervisionar a conformidade com a LGPD, servir como ponto de contato para questões relacionadas à privacidade e colaborar com a ANPD. Temos também o DPO as a Service, refere-se à contratação de um serviço externo de DPO por parte de uma organização. Muitas empresas optam por terceirizar a função de DPO, especialmente se não possuírem recursos internos suficientes ou expertise especializada em proteção de dados. Um provedor de DPO Service oferece uma gama de serviços, que podem incluir consultoria em

privacidade e proteção de dados, auditorias de conformidade, treinamento de funcionários, gerenciamento de incidentes de segurança e representação perante a ANPD. Esse modelo permite que as organizações atendam aos requisitos da LGPD de forma eficiente e sem a necessidade de recursos internos dedicados exclusivamente à função de DPO. (Baldissera, 2021).

A LGPD não apenas concede direitos e proteções aos indivíduos, mas também impõe sanções significativas para as organizações que não cumprem suas disposições. As multas previstas pela LGPD podem variar de uma porcentagem do faturamento anual da empresa até valores fixos consideráveis. O artigo 52 da LGPD estabelece as penalidades aplicáveis aos infratores da legislação, que incluem: advertência e adoção de medidas corretivas; multa de até 2% do faturamento da pessoa jurídica – com limite de R$ 50 milhões por infração; publicação da infração; bloqueio e eliminação dos dados em questão; multa diária; e, por fim, indenização ao titular dos dados. (Finkelstein e Finkelstein, 2020).

No entanto, a implementação efetiva da LGPD requer um esforço conjunto entre o setor público e privado. As empresas devem investir em tecnologias e práticas que garantam a segurança dos dados, como os DPOs, enquanto os órgãos reguladores e autoridades devem fiscalizar e assegurar a conformidade. (Sarlet, 2020).

Em um mundo cada vez mais digital e interconectado, a legislação de proteção de dados se torna uma pedra angular na preservação da privacidade individual e na manutenção da confiança na economia digital. A LGPD, assim como leis similares em outras nações, sinaliza um compromisso crucial em equilibrar os avanços tecnológicos com a preservação dos direitos e valores fundamentais de cada cidadão.

2.2 Marco Civil da Internet

O Marco Civil da Internet, oficialmente denominado Lei n. 12.965/14, foi sancionado pela ex-presidente Dilma Rousseff em 23 de abril de 2014, entrando em vigor em 23 de junho do mesmo ano. Antes de examinar os principais aspectos da lei, é importante entender o contexto que levou à sua criação.

A lei surgiu como resposta ao Projeto de Lei 84/99, conhecido como "Lei Azeredo", em referência ao então senador Eduardo Azeredo (PSDB-MG), defensor

do projeto. O PL 84/99 tratava de crimes cibernéticos e suas penalidades, além do acesso não autorizado a informações privadas por terceiros, que necessitaria de autorização judicial. No entanto, o projeto foi amplamente criticado por diversos setores da sociedade civil. (Salomão, 2016).

Para Ronaldo Lemos, diretor do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-RJ), a referida Lei possuía uma redação excessivamente abrangente, a proposta de lei transformava em crimes condutas comuns na internet, praticadas por milhões de pessoas. Por exemplo, criminalizava práticas como transferir músicas de um iPod de volta para o computador ou desbloquear um celular para ser utilizado por operadoras diferentes, ambas puníveis com até quatro anos de reclusão. Esses são apenas dois exemplos específicos, mas a aprovação da lei proposta representaria uma ameaça à possibilidade de inovação no país. Seria uma legislação que limitaria permanentemente a capacidade de pesquisa, inovação e produção de novos serviços tecnológicos, engessando os consumidores como meros usuários de produtos tecnológicos.

O Marco Civil, por ser uma legislação de cunho principiológico, tem como principal finalidade estabelecer os princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Para tanto, instituiu uma série de diretrizes que deverão ser seguidas pelos entes federativos (União, Estados, Distrito Federal e Municípios), provedores de Internet, empresas e todos os outros envolvidos na aplicação, disponibilização e uso do ciberespaço. (Ramos, 2021).

O objetivo do Marco Civil da Internet é fornecer um arcabouço legal para a utilização da rede mundial de computadores, promovendo a liberdade de expressão, a privacidade dos usuários e a neutralidade da rede. Ele também busca estabelecer responsabilidades para provedores de internet e plataformas online. (Brasil, 2014).

O Marco Civil da Internet possui três pilares essenciais para a sua interpretação: a neutralidade da rede, liberdade de expressão e a privacidade. (Salomão, 2016).

A neutralidade da rede é um princípio fundamental que visa garantir que todo o tráfego de internet seja tratado de forma igualitária, sem discriminação ou favorecimento por parte dos provedores de serviços de internet (ISPs) ou outras entidades que controlam a infraestrutura da rede. Esse princípio defende que todos os dados transmitidos pela internet devem ser tratados de maneira imparcial, sem

discriminação com base no tipo de conteúdo, origem, destino, protocolo ou aplicativo utilizado. (Souza e Lemos, 2016).

A neutralidade da rede impede que os ISPs privilegiam determinados serviços, aplicativos ou websites em detrimento de outros. Por exemplo, um ISP não pode oferecer velocidades de conexão mais rápidas para acessar certos sites ou serviços online em detrimento de outros, nem pode bloquear, limitar ou reduzir a velocidade de acesso a determinados conteúdos ou aplicativos. Além disso, o Marco Civil da Internet proíbe a comercialização de pacotes diferenciados de internet, nos quais os usuários teriam acesso preferencial a determinados conteúdos ou serviços online em troca de pagamento adicional. Essa prática é conhecida como "zero-rating" e é considerada uma violação da neutralidade da rede, pois cria uma internet com diferentes níveis de acesso com base na capacidade de pagamento dos usuários. (Souza e Lemos, 2016).

Esse princípio é crucial para garantir a igualdade de acesso à informação, promover a concorrência e a inovação online, e proteger a liberdade de expressão e os direitos dos usuários da internet. Sem a neutralidade da rede, poderia haver um cenário em que os ISPs poderiam exercer um controle indevido sobre o fluxo de informações na internet, favorecendo seus próprios interesses comerciais ou os de parceiros estratégicos, em detrimento da diversidade e da livre concorrência no ambiente online.

No entanto, a neutralidade da rede tem sido objeto de debates e controvérsias em todo o mundo, com defensores argumentando que é essencial para preservar a natureza aberta e democrática da internet, enquanto alguns ISPs e grupos de interesse defendem flexibilizações ou mesmo a abolição desse princípio, alegando que isso poderia promover investimentos em infraestrutura de internet e serviços diferenciados para os consumidores. Em muitos países, incluindo os Estados Unidos e alguns países da União Europeia, foram adotadas leis e regulamentações para proteger a neutralidade da rede e garantir que a internet permaneça aberta e acessível a todos os usuários, independentemente de interesses comerciais ou políticos.(Souza e Lemos, 2016).

Segundo o artigo 3º da lei 12.965/2014, parágrafo I, a liberdade de expressão é assegurada como um direito fundamental dos usuários da internet, permitindo que eles expressem suas opiniões, ideias e informações livremente, sem censura prévia ou interferência indevida por parte de autoridades governamentais ou terceiros. Isso

inclui o direito de publicar conteúdo online, participar de discussões em fóruns, redes sociais e blogs, e acessar informações de interesse público.

No entanto, é importante ressaltar que a liberdade de expressão não é absoluta e deve ser exercida de acordo com os limites estabelecidos pela legislação, como a proibição de discurso de ódio, incitação à violência, ameaças, calúnias, difamação e outras formas de manifestações ilegais ou prejudiciais. O Marco Civil da Internet estabelece que os ISPs não podem ser responsabilizados pelo conteúdo gerado por terceiros, a menos que descumpram ordens judiciais específicas para remover conteúdos ilegais após a sua notificação. (Brasil, 2014).

No que diz respeito à privacidade, o Marco Civil da Internet estabelece que os ISPs e outras entidades que coletam, armazenam, processam ou transferem dados pessoais devem respeitar a privacidade dos usuários, garantindo a proteção adequada de suas informações pessoais contra acesso não autorizado, uso indevido, perda ou vazamento. O Marco Civil da Internet também estabelece que a coleta e o tratamento de dados pessoais devem ser realizados de forma transparente e com o consentimento dos usuários, que devem ser informados sobre como seus dados serão utilizados e ter o direito de acessar, corrigir e excluir suas informações pessoais quando necessário. (Fragoso, 2019).

Além disso, o Marco Civil da Internet prevê a responsabilidade dos ISPs em relação à segurança dos dados pessoais dos usuários, exigindo a implementação de medidas técnicas e organizacionais adequadas para proteger essas informações contra ameaças, como acessos não autorizados, ataques cibernéticos e vazamentos de dados. Ele também estabelece que as autoridades competentes podem solicitar informações pessoais de usuários apenas mediante ordem judicial específica e fundamentada, garantindo assim a proteção da privacidade e o devido processo legal. (Fragoso, 2019).

Alguns dos outros princípios do Marco Civil da Internet são; a Responsabilidade dos Provedores, definindo as responsabilidades dos provedores de internet e aplicações online em relação ao conteúdo gerado por terceiros; o Armazenamento de Registros de Conexão, que é utilizado para determinar que os provedores devem manter registros de conexão por um determinado período, respeitando a privacidade dos usuários e por último, a Jurisdição Brasileira, estabelecendo que, em casos de violação de direitos no ambiente digital, a

legislação brasileira deve ser aplicada, mesmo se os serviços forem oferecidos por empresas estrangeiras. (Brasil, 2014).

O Marco Civil da Internet é considerado uma das legislações mais avançadas no mundo no que diz respeito à regulamentação da internet. Ele serve como um modelo para outros países que buscam estabelecer uma estrutura legal para a utilização da rede de forma responsável e inclusiva.

2.3 Cibersegurança e Responsabilidade Civil

O crescimento exponencial da digitalização trouxe consigo um novo conjunto de desafios, com a cibersegurança emergindo como uma preocupação crítica na sociedade contemporânea. A proteção contra ataques cibernéticos e a gestão responsável de dados são agora imperativos fundamentais para indivíduos, organizações e governos. A cibersegurança abrange um amplo espectro de medidas e práticas destinadas a proteger sistemas, redes e dados contra acessos não autorizados, interrupções e danos. Inclui desde a implementação de firewalls e softwares antivírus até a educação e treinamento de usuários para identificar ameaças online. (Brasil, 2021).

Entretanto, quando a segurança é comprometida e ocorrem violações de dados, surge a questão da responsabilidade civil. As organizações que coletam e processam informações pessoais têm o dever de proteger esses dados contra acessos não autorizados ou vazamentos. Caso falhem nessa obrigação, podem ser legalmente responsabilizadas pelos danos causados aos titulares dessas informações.

O Brasil foi convidado a aderir à Convenção de Budapeste em dezembro de 2019. O governo federal considera que, apesar de o Marco Civil da Internet (Lei 12.965, de 2014) ter criado importante estrutura legislativa para o combate aos crimes cibernéticos, os meios digitais não respeitam limites. Por esse motivo é necessário constante aprimoramento da cooperação e coordenação entre os países. Criminalização de condutas, normas para investigação e produção de provas eletrônicas, meios de cooperação internacional são questões tratadas neste acordo. Ele também aborda o acesso indevido e não autorizado a um sistema de computador, fraudes, material de abuso sexual infantil, violações de direito autoral e violações de segurança de redes. (Brasil, 2021). No entanto, a cibersegurança é

uma responsabilidade compartilhada. Os indivíduos também desempenham um papel crucial na proteção de seus próprios dados, adotando práticas seguras, como o uso de senhas robustas e a cautela ao compartilhar informações online.

Além disso, a colaboração entre setor público e privado é essencial na luta contra ameaças cibernéticas em larga escala. Isso envolve a partilha de informações sobre ameaças, o desenvolvimento de regulamentações eficazes e a cooperação na investigação e prevenção de ataques. A cibersegurança e a responsabilidade civil são pilares essenciais para a construção de uma sociedade digital confiável e resiliente. Garantir a segurança dos dados pessoais não é apenas uma questão de conformidade legal, mas também uma demonstração de respeito pela privacidade e pela confiança dos usuários na era digital. (Brasil, 2021).

2.4 Privacidade na Internet

A privacidade na internet é uma das questões mais importantes e complexas da era digital. Em um mundo cada vez mais interconectado, onde informações pessoais são compartilhadas e armazenadas em uma escala global, a proteção da privacidade tornou-se uma preocupação central para indivíduos, empresas e governos. O cerne da privacidade na internet reside na capacidade de controlar as próprias informações pessoais. Trata-se do direito fundamental de determinar o que é compartilhado, com quem e para que finalidade. No entanto, esse direito muitas vezes colide com as práticas de coleta de dados por parte de empresas e organizações, bem como com as necessidades de segurança e investigação por parte das autoridades. (Nóbrega, 2024).

As redes sociais, aplicativos e serviços online desempenham um papel significativo nesse contexto. Ao fornecer plataformas para comunicação e interação, eles também se tornam receptáculos de uma quantidade considerável de dados pessoais. O desafio é equilibrar os benefícios da conectividade digital com a necessidade de proteger a privacidade dos usuários.

Na atualidade, o Brasil é um dos países do mundo com maior utilização das redes sociais. É o quarto país em número de usuários do Facebook, com 70,5 milhões (e também o quarto em percentagem da população, com 34,5%); e o segundo com maior número de pessoas no Twitter. Em 2015, oito em cada dez

crianças e adolescentes com idades entre 9 e 17 anos eram usuários da internet. (Brasil, 2016).

Legislações como a LGPD citada acima e o GDPR na União Europeia representam passos importantes na direção da proteção da privacidade na internet. Elas estabelecem regras claras para a coleta, processamento e armazenamento de dados, além de dar aos usuários mais controle sobre suas informações.

No entanto, a proteção da privacidade na internet é uma responsabilidade compartilhada. Indivíduos devem estar conscientes das configurações de privacidade em suas contas online, enquanto as empresas devem implementar práticas de segurança e transparência em relação aos dados dos usuários. A privacidade na internet é um componente essencial da dignidade e liberdade individuais na era digital. Encontrar o equilíbrio certo entre a conectividade global e a proteção da esfera privada é um desafio complexo, mas crucial para garantir uma internet segura, confiável e inclusiva para todos. (Nóbrega, 2024).

2.5 Liberdade de Expressão Online

A liberdade de expressão, consagrada como um direito fundamental em diversas constituições ao redor do mundo, desempenha um papel crucial na construção e manutenção de sociedades democráticas. Na era digital, essa liberdade ganha novas dimensões e desafios, moldando a forma como as pessoas se comunicam, interagem e exercem sua cidadania.

A internet proporciona uma plataforma global para a expressão de ideias, permitindo que indivíduos de diferentes partes do mundo se conectem, compartilhem informações e participem de debates públicos. Redes sociais, blogs e fóruns online se tornaram canais essenciais para a manifestação de opiniões, o ativismo, a mobilização cívica, sendo livre a manifestação do pensamento e a procura, o recebimento e a difusão de informações ou ideias, por qualquer meio, e sem dependência de censura. (Brasil, 1967).

> Um dos principais marcos dessa transformação aconteceu com a popularização das plataformas que hospedam conteúdo gerado por usuários, popularmente conhecidas como redes sociais. Essas plataformas tiveram um crescimento expressivo na última década, passando a

> desempenhar funções centrais no fluxo de informação e comunicação de nossa sociedade. Plataformas como Facebook, YouTube, Instagram, WeChat e TikTok possuem mais de um bilhão de usuários cada uma, e existem diversas outras na casa das centenas de milhões de usuários, como Twitter, Snapchat, Pinterest e LinkedIn.
> Atualmente, empresas tradicionais de mídia, como jornais e editoras, assim como emissoras de rádio e televisão, instituições públicas, figuras públicas, empresas e pessoas em geral, utilizam-se de redes sociais, muitas vezes como seu canal de comunicação principal, para disseminar informações e publicar conteúdo dos mais diversos tipos. Indiscutivelmente, as redes sociais desempenham uma função central para as pessoas se expressarem na atualidade. (Bícego, 2023, p. 12).

No entanto, a expansão da liberdade de expressão online não está isenta de dilemas complexos. Questões como discurso de ódio, desinformação e cyberbullying desafiam a balança entre a liberdade de expressão e a proteção de outros direitos e da dignidade humana. Além disso, o poder de grandes plataformas digitais na moderação de conteúdo tem gerado debates sobre a regulação e responsabilidade dessas empresas na proteção da liberdade de expressão. A remoção de conteúdos e contas, muitas vezes por decisões algorítmicas, levanta preocupações sobre a censura e a necessidade de transparência nos processos de moderação. (Bícego, 2023).

É importante destacar o papel que as plataformas digitais ocupam no ecossistema, a liberdade de expressão online também está intrinsecamente ligada à proteção da privacidade e à segurança dos usuários. Garantir que os indivíduos possam se expressar livremente sem temer represálias ou vigilância indevida é um componente essencial da liberdade de expressão digital. Dessas plataformas, deve ser cobrada, pela sociedade, postura ativa e ininterrupta na proteção dos usuários. São elas que têm a responsabilidade de estruturar os espaços mais populares de comunicação digital e de responderem às demandas de entidades governamentais. (Gregório, 2019).

> As instâncias governamentais, por sua vez, não podem se eximir de debater melhorias para o ambiente digital e, principalmente, de desenvolverem políticas públicas voltadas para a harmonia desse espaço. Aqui, tem se destacado o trabalho do Tribunal Superior Eleitoral (TSE), que incluiu em suas resoluções regras de propaganda eleitoral para influenciadores, além de apoiar o debate contra a violência política no Brasil. Merece ser lembrado também seu esforço em trabalhar junto às plataformas para mobilizar e exigir medidas de combate à desinformação mais efetivas e concretas. (Durigan; Pereira, 2022).

Nesse contexto, é fundamental que haja um diálogo contínuo entre governos, sociedade civil, empresas de tecnologia e a comunidade online para desenvolver diretrizes e políticas que protejam a liberdade de expressão enquanto abordam os desafios que surgem na era digital.

3 *Cyberspace*, Comércio Eletrônico e Contratos Digitais

O advento do comércio eletrônico revolucionou a forma como consumidores e empresas interagem e conduzem transações comerciais. Esse cenário dinâmico e altamente competitivo trouxe consigo a necessidade de uma abordagem jurídica específica para regular as transações realizadas no ambiente digital, dando origem aos contratos digitais. (Araújo, 2003).

Os contratos digitais, por sua natureza, são acordos celebrados e formalizados de maneira eletrônica, muitas vezes sem a necessidade de assinaturas físicas. Esses contratos são igualmente vinculativos e legalmente reconhecidos, proporcionando segurança e agilidade em um contexto em que a velocidade das transações é essencial.

Contudo, a complexidade dos contratos digitais reside na necessidade de garantir a autenticidade e integridade das partes envolvidas. Para isso, tecnologias como a assinatura digital e a tecnologia blockchain chegam para revolucionar a certificação de documentos, trazendo mais praticidade, segurança e agilidade no processo online. (Totvs, 2023). A assinatura digital utiliza criptografia para verificar a identidade do signatário, enquanto a tecnologia blockchain proporciona uma forma imutável de registro de transações, aumentando a confiabilidade e segurança dos contratos. A assinatura digital é um recurso vinculado ao certificado digital, responsável por garantir a autenticidade do documento assinado de maneira eletrônica, sendo o principal objetivo da ferramenta reproduzir a assinatura de uma pessoa em documentos eletrônicos, com segurança, eficiência e praticidade. (Totvs, 2023).

A legislação de comércio eletrônico também desempenha um papel essencial na regulamentação dessas transações. No Brasil, o Código de Defesa do Consumidor e o Marco Civil da Internet estabelecem diretrizes específicas para o comércio online, garantindo a proteção dos direitos dos consumidores e a responsabilidade das plataformas e vendedores. Ademais, tratados internacionais e regulamentações globais também desempenham um papel importante na harmonização das leis de comércio eletrônico entre países, facilitando o comércio transfronteiriço. Pois, segundo Araújo, as leis também são importantes para garantirem segurança para todas as empresas e consumidores que atuam no comércio virtual. (Araújo, 2003).

Em resumo, o comércio eletrônico e os contratos digitais representam uma nova era no comércio global, impulsionando a economia digital e expandindo as oportunidades de negócios. A integridade e eficácia dos contratos digitais, juntamente com uma legislação de comércio eletrônico adequada, são fundamentais para garantir a confiança e segurança nesse ambiente de negócios em constante evolução.

3.1 Direitos Autorais e Propriedade Intelectual

Os direitos autorais e a propriedade intelectual desempenham um papel crucial na promoção da inovação, criatividade e progresso cultural em uma sociedade. Estes conceitos constituem a espinha dorsal de um sistema legal que busca equilibrar o incentivo à produção de obras intelectuais com o interesse público em ter acesso à informação e à cultura.

Os direitos autorais conferem ao criador de uma obra literária, artística ou científica o direito exclusivo de reproduzir, distribuir e exibir essa criação. Esse conjunto de direitos proporciona um incentivo vital para os artistas e autores, ao garantir que possam colher os frutos do seu trabalho e serem devidamente reconhecidos. Pelo direito de exclusividade, o autor é o único que pode explorar sua obra, gozar dos benefícios morais e econômicos resultantes dela ou ceder os direitos de exploração a terceiros. (Vieira; Barbosa; Carneiro, 2020).

A área do direito denominada Propriedade Intelectual garante a inventores ou responsáveis por quaisquer produções do intelecto o direito à recompensa pela própria criação, e se divide em dois campos: os direitos do autor e a propriedade industrial. Enquanto o primeiro conceito faz parte do direito civil e é regulado principalmente pela Lei n. 9.610/1998, o último pertence ao direito comercial e é orientado pela Lei n. 9.279/1996 (Lei da Propriedade Industrial). No CNJ Serviço desta segunda-feira procuramos esclarecer os principais conceitos relacionados a estas duas áreas da propriedade intelectual. (Vieira; Barbosa; Carneiro, 2020).

A evolução tecnológica e a expansão da internet têm levantado novos desafios para a proteção dos direitos autorais e propriedade intelectual. A facilidade de reprodução e distribuição de conteúdo digital tornou essencial a criação de mecanismos eficazes de controle e proteção desses direitos.

Porém, o equilíbrio entre a proteção dos direitos autorais e o acesso à informação tem sido um tema de debate constante. O uso justo e as exceções aos direitos autorais são elementos cruciais para garantir que a lei promova tanto a criação quanto a disseminação do conhecimento.

A propriedade intelectual traz implicações significativas para a economia, incentivando a inovação e o desenvolvimento tecnológico. Elas proporcionam um ambiente propício para o investimento em pesquisa e desenvolvimento, ao garantir que os criadores e inventores possam colher os benefícios do seu trabalho.

Além disso, a propriedade intelectual serve de contexto para um conceito legal em desenvolvimento no Brasil, que é o direito ao esquecimento. Embora não haja uma legislação específica que aborde diretamente esse direito, ele tem sido discutido em casos judiciais e debates acadêmicos, principalmente no âmbito da proteção de dados pessoais e da privacidade. A Constituição Federal de 1988 prevê o direito à privacidade como um direito fundamental, o que tem servido de base para argumentações em favor do direito ao esquecimento. Além disso, o Marco Civil da Internet (Lei nº 12.965/2014) estabelece princípios e diretrizes para o uso da internet no Brasil, incluindo a proteção da privacidade e dos dados pessoais dos usuários.

O Supremo Tribunal Federal (STF) ainda não emitiu uma decisão definitiva sobre o direito ao esquecimento, mas há casos em que alguns ministros manifestaram posicionamentos favoráveis a esse direito. Por exemplo, em 2019, no julgamento do Recurso Extraordinário 1.010.606, o Ministro Dias Toffoli afirmou que o direito ao esquecimento é uma derivação do direito à privacidade e pode ser aplicado em casos específicos.

Apesar disso, a jurisprudência brasileira ainda não consolidou uma posição uniforme sobre o direito ao esquecimento. Os tribunais têm analisado casos individualmente, levando em consideração os princípios constitucionais, a legislação vigente e os direitos em conflito, como a liberdade de expressão e o acesso à informação. Em suma, embora o direito ao esquecimento ainda não esteja totalmente estabelecido na legislação e jurisprudência brasileira, é um tema em discussão e que tem ganhado relevância no contexto da proteção de dados pessoais e da privacidade, especialmente em um mundo cada vez mais digitalizado. (TJDFT, 2024).

3.2 Tecnologias Emergentes

“Tecnologias emergentes são inovações técnicas ou em desenvolvimento com grande potencial de mudar o curso de nossas vidas e dos negócios.” (Redator Sankhya, 2023)

Uma dessas principais tecnologias é a Inteligência Artificial (IA), que se destaca pela capacidade de máquinas aprenderem e tomar decisões autônomas baseadas em bancos de dados. A IA está revolucionando setores como saúde, finanças, transporte e educação, criando soluções para problemas complexos. (Sankhya, 2023).

Outra inovação significativa é a Internet das Coisas (IoT), que surgiu em 1999 e foi criada pelo pesquisador britânico Kevin Ashton. Ela conecta dispositivos e objetos cotidianos à internet, permitindo comunicação e interação entre eles. Essa interconexão está gerando uma revolução na automação residencial, na indústria e na gestão de cidades inteligentes.

A tecnologia blockchain, que é usada para comércios digitais, como foi dito anteriormente, está redefinindo a confiança e a segurança na era digital. Ao criar um registro distribuído e imutável de transações, ela oferece um novo paradigma para transações financeiras, contratos inteligentes e até mesmo a gestão da cadeia de suprimentos. Além disso, a biotecnologia e a nanotecnologia prometem avanços extraordinários no campo da medicina e da engenharia de materiais. Desde terapias genéticas revolucionárias até materiais super-resistentes e leves, essas disciplinas estão moldando o futuro da saúde e da indústria.

Apesar disso, o avanço dessas tecnologias não está isento de desafios éticos e regulatórios. Questões sobre privacidade de dados, segurança cibernética e o impacto social e ambiental dessas inovações exigem reflexão cuidadosa e uma abordagem equitativa para o seu desenvolvimento e implementação. As tecnologias emergentes representam um convite para a humanidade explorar novas fronteiras de inovação e progresso. Para Brown (2010), a partir do pensamento divergente, faz-se a transformação, para enfim buscar o pensamento convergente, resultando na criação da inovação.

3.3 Jurisdição Transnacional no Ciberespaço

A jurisdição transnacional no ciberespaço refere-se à capacidade e ao alcance das leis de um país sobre atividades que ocorrem online e que podem envolver partes localizadas em diferentes jurisdições. Isso ocorre porque a natureza global da internet desafia os conceitos tradicionais de jurisdição, que são baseados principalmente em fronteiras geográficas. É essa natureza transnacional da internet que desafia o conceito de jurisdição territorial, de acordo com Israel (Lorenzo apud Israel, 2020). Dentro deste contexto, é oportuno apresentar uma tabela que evidencia as diversas abordagens e jurisdições adotadas por países em relação à regulação do ciberespaço. A tabela abaixo apresenta alguns exemplos destacados:

Tabela 1 — Exemplos de Abordagens e Jurisdições no Ciberespaço

País	Abordagem	Jurisdição
Estados Unidos	Modelo baseado na liberdade de expressão e autorregulação	Primariamente doméstica, mas pode se estender a outras jurisdições em casos específicos
China	Controle estatal e censura da internet	Jurisdição estatal, com restrições significativas
União Europeia	Regulamentação de proteção de dados e privacidade	Jurisdição regional através do Regulamento Geral de Proteção de Dados (GDPR)
Brasil	Marco Civil da Internet e princípios democráticos	Jurisdição nacional, com cooperação internacional em casos específicos

Fonte: Lorenzo, 2023.

Esta tabela ilustra como distintos países adotam abordagens diversas na regulamentação do ciberespaço, refletindo suas visões e políticas individuais. Tal diversidade de enfoques ressalta os desafios enfrentados na busca por uma regulamentação internacional abrangente.

Um dos principais desafios é a determinação da jurisdição aplicável em casos de atividades criminosas online, como fraudes, hacking e pornografia infantil. A falta de fronteiras físicas no ciberespaço torna difícil estabelecer onde um crime ocorreu e, consequentemente, qual jurisdição deve lidar com o caso. Além disso, as leis de diferentes países nem sempre estão alinhadas, o que pode levar a conflitos quando

uma atividade é considerada legal em um país, mas ilegal em outro. Isso cria incertezas e dificulta a aplicação consistente da lei no ciberespaço. A execução de decisões judiciais também pode ser um desafio, especialmente quando se trata de remover conteúdo ilegal ou prejudicial da internet. Embora o Brasil tenha leis que permitem a remoção de conteúdo considerado ilegal, fazer cumprir essas decisões em plataformas e serviços online sediados em outros países pode ser difícil. (Costa, 2017).

Neste contexto entra a questão da soberania no ciberespaço, que é complexa devido à sua natureza transnacional e descentralizada da internet. Enquanto os Estados procuram exercer autoridade sobre as atividades que ocorrem em seus territórios virtuais, enfrentam desafios significativos devido à falta de fronteiras geográficas claras na internet. A capacidade dos Estados de regular e controlar as atividades online é complicada pela diversidade de leis, regulamentações e normas culturais em diferentes partes do mundo. (Lorenzo, 2023).

Um aspecto crucial é a determinação da jurisdição e da lei aplicável, especialmente quando as transações e comunicações online atravessam várias fronteiras. Além disso, a segurança cibernética é uma preocupação crescente, o que levanta questões sobre como exercer soberania para defender tais interesses.

A regulamentação de conteúdo online é outro ponto de debate, com Estados buscando proteger interesses públicos, como segurança, privacidade e moralidade, mas enfrentando preocupações sobre censura e liberdade de expressão. A cooperação internacional é fundamental para lidar com esses desafios, com Estados buscando desenvolver acordos e mecanismos de cooperação para questões como segurança cibernética e combate ao crime online. Em situações desse tipo, a determinação sobre quem possui o direito e a responsabilidade de intervir torna-se intricada, demandando uma compreensão mais aprofundada da soberania no ciberespaço. (Lorenzo,2023).

Dentro desse contexto, é pertinente apresentar uma tabela que ilustra as diversas abordagens e perspectivas adotadas pelos países em relação à soberania no ciberespaço. Abaixo estão alguns exemplos destacados na tabela:

Tabela 2 — Abordagens e Perspectivas sobre a Soberania no Ciberespaço

País	Abordagem	Perspectiva
Estados Unidos	Foco na liberdade de expressão e na autorregulação	Ênfase na liberdade individual e na autodeterminação online
China	Controle estatal e censura da internet	Ênfase na segurança e na estabilidade do regime político
União Europeia	Regulamentação de proteção de dados e privacidade	Ênfase na proteção dos direitos individuais e na privacidade
Brasil	Marco Civil da Internet e princípios democráticos	Ênfase na garantia da liberdade de expressão e na proteção dos direitos dos cidadãos

Fonte: Lorenzo, 2023.

A tabela evidencia as diferentes posturas adotadas por diversos países em relação à soberania no ciberespaço, refletindo suas visões, prioridades e políticas individuais. Tal diversidade de abordagens ressalta a complexidade e a necessidade de uma coordenação global na governança do ciberespaço.

Outra questão relevante é a neutralidade da rede, que visa garantir que todo o tráfego de internet seja tratado de forma igualitária, sem discriminação ou favorecimento. No entanto, a aplicação desse princípio pode ser desafiadora quando diferentes jurisdições têm políticas de regulação da internet conflitantes. Para enfrentar esses desafios, os países têm buscado acordos de cooperação internacional e desenvolvido tratados específicos para lidar com questões de jurisdição no ciberespaço. Organizações internacionais, como a Interpol e a Europol, desempenham um papel crucial na coordenação e colaboração entre os países para combater crimes cibernéticos e garantir a aplicação adequada das leis no ambiente digital. (Lorenzo, 2023).

4 Jurisprudência e Direito Digital

Ao longo dos anos, os tribunais brasileiros têm enfrentado uma ampla gama de casos digitais, cujas decisões ajudaram a moldar o campo do direito digital no país. Isso inclui casos emblemáticos sobre aplicação da Lei Geral de Proteção de Dados (LGPD), responsabilidade de empresas de internet pelo conteúdo gerado por terceiros, crimes cibernéticos como fraudes online e invasões de sistemas, questões de liberdade de expressão e censura na internet, violações de direitos autorais em ambiente digital, entre outros.

Essas decisões jurisprudenciais são essenciais para estabelecer precedentes legais e orientar futuros casos semelhantes. Elas refletem a interpretação das leis existentes pelos tribunais e ajudam a definir os limites e as responsabilidades dos diferentes atores no ambiente digital, sejam eles indivíduos, empresas ou o próprio Estado.

4.1 O Caso do Google

O caso Google e o "Direito ao Esquecimento" que foi inspirado em uma decisão da União Europeia, onde o Superior Tribunal de Justiça (STJ) tem proferido decisões sobre o "direito ao esquecimento", determinando que buscadores como o Google removam resultados de pesquisa que violem a privacidade ou causem danos injustificados. O direito ao esquecimento foi pacificado pelo Supremo Tribunal Federal como inconstitucional, mas essa decisão não impede a aplicação da desindexação, ou seja, a responsabilização das plataformas de busca na internet em relação a informações ou nomes pesquisados. Com esse entendimento, a 18ª Câmara Cível do Tribunal de Justiça do Paraná garantiu a um homem o direito de ser "deixado em paz" pelo Google após seu nome ser relacionado a uma operação policial sem que ele tenha sido sequer denunciado. (Tajra, 2023).

4.2 O Caso do WhatsApp

Em 2016, juízes ordenaram suspensões no WhatsApp, alegando que o aplicativo não colaborou com informações para investigações. Houve uma série de

bloqueios do aplicativo em território brasileiro devido à recusa da empresa em fornecer dados criptografados em investigações criminais. Esses casos geraram um debate intenso sobre privacidade, criptografia e a responsabilidade das empresas de tecnologia em colaborar com investigações. (g1, 2022).

Embora não seja um caso específico, a entrada em vigor da LGPD em 2020 e os primeiros casos relacionados à violação de dados pessoais e proteção da privacidade têm gerado jurisprudência significativa sobre a aplicação da legislação.

4.3 O Caso do Discord

O Discord, como uma plataforma de comunicação online, pode ser alvo de diversos tipos de crimes virtuais. Embora seja uma ferramenta valiosa para a comunicação e colaboração, também pode ser explorada por indivíduos mal-intencionados para atividades ilegais.

Como o caso do Pedro Ricardo Conceição da Rocha, conhecido na internet como *King*. Ele é apontado como criador do principal grupo na plataforma *Discord* onde eram praticados estupros virtuais e indução a automutilação e suicídio. Pedro respondeu por associação criminosa; divulgação e armazenamento de arquivos contendo cenas de abuso sexual infantojuvenil; estupro de vulnerável; e induzimento, instigação ou auxílio a suicídio ou a automutilação. (Brasil de Fato, 2023).

4.4 O Caso da Carolina Dieckmann

O caso envolvendo Carolina Dieckmann foi um dos primeiros e mais emblemáticos incidentes relacionados à violação de privacidade e segurança digital no Brasil. Em 2012, a atriz teve seu computador hackeado e fotos íntimas foram roubadas e divulgadas na internet sem seu consentimento. Este caso gerou grande repercussão na mídia e despertou debates sobre a necessidade de atualização das leis de proteção de dados e de combate aos crimes cibernéticos no país. Foi um marco importante que chamou a atenção para a vulnerabilidade dos indivíduos no ambiente digital e a necessidade de proteção de sua privacidade e segurança.

A resposta legal ao incidente envolveu uma investigação policial para identificar os responsáveis pelo crime cibernético. Posteriormente, foram realizadas mudanças na legislação brasileira, como a inclusão do crime de "invasão de dispositivo informático" no Código Penal Brasileiro, através da Lei Carolina Dieckmann (Lei nº 12.737/2012), em homenagem à atriz, que em 2023 completou 10 anos de vigência. (Araújo, 2023).

A fim de garantir segurança no ambiente virtual, em 2011, seis deputados federais apresentaram proposta para tratar sobre invasões de dispositivos eletrônicos e uso das informações obtidas. O projeto de lei contra os crimes decorrentes do uso indevido de informações e materiais pessoais relativos à privacidade de qualquer indivíduo na internet, foi analisado pelos senadores. Essa lei, popularmente conhecida como "Lei Carolina Dieckmann", tipifica como crime a invasão de dispositivos informáticos com o fim de obter, adulterar ou destruir dados pessoais, e prevê pena de reclusão de até dois anos, além de multa. O relator da proposta na Comissão de Ciência e Tecnologia, senador Eduardo Braga, do MDB do Amazonas, observou que até a votação do projeto, em 2012, não havia na legislação penal norma específica para os crimes de informática, inclusive a captura de dados de cartões de crédito ou de débito que permitem as falsificações. Ele apontou os prejuízos que desde então já cresciam no Brasil. Essa legislação foi um importante avanço na proteção da privacidade e segurança digital dos cidadãos brasileiros. (Araújo, 2023).

O caso da Carolina Dieckmann serve como um exemplo concreto das questões enfrentadas no campo do Direito Digital, destacando a importância de uma legislação robusta e de mecanismos eficazes para proteger os direitos dos usuários da internet e punir os infratores. Além disso, evidencia a necessidade contínua de conscientização sobre segurança digital e da implementação de medidas de prevenção e proteção contra crimes cibernéticos.

Embora a Lei nº 12.737/2012 tenha representado um avanço significativo na legislação brasileira para enfrentar os crimes cibernéticos e proteger a privacidade digital, ela não escapou de críticas por parte de algumas pessoas e especialistas. Uma das críticas mais comuns é em relação às penalidades previstas na lei, que alguns consideram excessivas. A pena de até dois anos de reclusão pode ser vista como desproporcional em comparação com outros tipos de crimes. Além disso, há preocupações sobre a falta de especificidade da legislação em relação aos tipos de

condutas consideradas crimes de invasão de dispositivos informáticos. A redação da lei pode ser interpretada de forma ampla e vaga, o que pode gerar incertezas e interpretações diversas por parte dos tribunais. (Filho, 2024).

Outra crítica diz respeito aos desafios na aplicação da lei na prática. Identificar os responsáveis por ataques cibernéticos pode ser uma tarefa complexa, especialmente considerando a falta de capacidade técnica das autoridades para investigar e punir esses crimes, bem como a necessidade de cooperação internacional em casos que envolvem transnacionalidade.

Além disso, algumas vozes argumentam que a lei não aborda de maneira abrangente a proteção de dados pessoais em si, focando mais na punição dos invasores de dispositivos informáticos do que na proteção efetiva da privacidade dos usuários da internet. Essas críticas ressaltam a complexidade e os desafios envolvidos na legislação relacionada ao Direito Digital. Elas destacam a importância de uma abordagem equilibrada que leve em consideração não apenas a punição de criminosos cibernéticos, mas também a proteção efetiva dos direitos dos usuários da internet, incluindo a proteção de seus dados pessoais e a garantia de sua privacidade online. (Filho, 2024).

CONSIDERAÇÕES FINAIS

Ao concluir este estudo sobre o Direito Digital no ordenamento jurídico brasileiro, é evidente que a rápida evolução tecnológica impôs desafios significativos tanto para os legisladores quanto para os operadores do Direito. A transformação digital altera profundamente as relações sociais, econômicas e culturais, exigindo uma constante adaptação das normas jurídicas para garantir a proteção dos direitos fundamentais e a promoção da justiça.

O Brasil tem demonstrado esforços consideráveis para acompanhar essas mudanças, como evidenciado pela promulgação de leis importantes como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018). Estas legislações representam marcos fundamentais para a regulamentação do ambiente digital, estabelecendo diretrizes claras sobre direitos e deveres dos usuários, empresas e do próprio Estado na era da informação.

Entretanto, o dinamismo do setor tecnológico impõe a necessidade de uma constante atualização normativa e uma vigilância contínua por parte dos legisladores e do Judiciário. A interpretação e aplicação dessas leis devem ser feitas de forma a equilibrar a inovação tecnológica com a proteção dos direitos individuais e coletivos. É crucial que as normas acompanhem o ritmo das inovações para evitar lacunas legais que possam prejudicar a segurança jurídica e a confiança dos cidadãos no sistema.

Outro ponto importante abordado neste trabalho é a capacitação dos operadores do Direito. É imprescindível que advogados, juízes, promotores e demais profissionais do setor se especializem e se atualizem continuamente sobre as questões relativas ao Direito Digital. Apenas com um conhecimento profundo e atualizado será possível aplicar a legislação de forma eficaz e justa.

Além disso, o diálogo entre o Direito e outras disciplinas, como a tecnologia da informação e a ciência de dados, é essencial para a construção de um ordenamento jurídico mais robusto e adaptado às novas realidades. A interdisciplinaridade enriquece o debate e possibilita soluções mais integradas e eficientes para os problemas que surgem no ambiente digital.

Por fim, este estudo reforça a importância da participação ativa da sociedade civil na construção e aprimoramento das normas jurídicas. A colaboração entre governo, setor privado e cidadãos é fundamental para o desenvolvimento de

políticas públicas inclusivas e que atendam às reais necessidades da população no contexto digital. A busca por um equilíbrio entre inovação tecnológica e proteção dos direitos fundamentais deve continuar a guiar o desenvolvimento do ordenamento jurídico brasileiro, garantindo uma sociedade mais justa, segura e inclusiva.

REFERÊNCIAS

ARAÚJO, Iran. **Os crimes cibernéticos e o Direito Penal Brasileiro.** Disponível em: <https://www.jusbrasil.com.br/artigos/os-crimes-ciberneticos-e-o-direito-penal-brasileiro/1894019562>. Acesso em: 02 abr. 2024

BRASIL DE FATO (2023, 14 de julho). **Jovem no RJ suspeito de criar grupo no Discord vai responder por estupro de vulnerável.** Disponivel em:<https://www.brasildefato.com.br/2023/07/14/jovem-no-rj-suspeito-de-criar-grupo-no-discord-vai-responder-por-estupro-de-vulneravel>. Acesso em 03 abr. 2024.

_____, Janaina. **Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos.** Disponível em: <https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos>. Acesso em: 02 abr. 2024.

_____, Michele Silva. **Comércio eletrônico: evolução e perspectivas.** 2003. Monografia (Bacharelado em Relações Internacionais) - Centro Universitário de Brasília, Brasília, 2003.

BERNI, Duilio Landell de Moura. **Fundamentos para uma Autonomia Científica do Direito Digital no Ordenamento Jurídico Brasileiro.** TEDE. Disponivel em: <https://tede2.pucrs.br/tede2/handle/tede/10161#preview-link0>. Acesso em: 03 abr. 2024.

BRASIL. Lei nº 5.250, de 9 de fevereiro de 1967. **Dispõe sobre a liberdade de manifestação de pensamento e de informação e estabelece normas para a imprensa.** Diário Oficial da União, Brasília, DF, 09 fev 1967.

_____. **O direito ao esquecimento e as liberdades de informação e de expressão.** 04/03/2024. Disponível em: <https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/direito-constitucional/o-direito-ao-esquecimento-e-o-conflito-com-os-direitos-a-liberdade-de-informacao-e-de-expressao>. Acesso em: 1 abr. 2024.

_____. Lei nº 12.965. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Diário Oficial da União, Brasília, DF, 23 de abril de 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 abr. 2024.

_____. **Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético.** senadonoticias, 15/12/2018. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico >. Acesso em: 31 out. 2023.

_____. 2016. **Internet e direitos humanos.** gov.br, 10/11/2016. Disponível em: <https://www.gov.br/mdh/pt-br/sdh/noticias/2016/novembro/internet-e-direitos-humanos>. Acesso em: 31 out. 2023.

_____, **Supremo Tribunal Federal. Acórdão nº 1010606.** Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755910773>. Acesso em: 02 abr. 2024.

BÍCEGO, Bruno. **Liberdade de Expressão e Moderação de Conteúdo: proteção de direitos fundamentais em plataformas online.** 2023. 45f. Monografia - Pontifícia Universidade Católica, São Paulo, 2023.

BROWN, T. **Design Thinking: uma metodologia poderosa para decretar o fim**

das velhas ideias. Rio de Janeiro: Elsevier, 2010.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais.** 1ª ed. Rio de Janeiro: Brasport, 2014.

COSTA, Filipe. **OS DESAFIOS DO DIREITO INTERNACIONAL NO CIBERESPAÇO**: A INEFICÁCIA DO SISTEMA DE RESPONSABILIZAÇÃO INTERNACIONAL DOS ESTADOS E DOS NÍVEIS PROBATÓRIOS DAS CORTES INTERNACIONAIS. 2017. Disponível em: <https://repositorio.ufba.br/bitstream/ri/24853/1/Costa%2c%20Filipe%20Gomes%20Di as.pdf>. Acesso em: 03 abr. 2024.

DE GREGÓRIO, Giovanni. **Democratising Online Content Moderation: A Constitutional Framework.** ***Journal Title***. Disponível em: <https://deliverypdf.ssrn.com/delivery.php?ID=720026113081005109121024124094096102019014069017088036022084108118020102072069030100025100029023038019107087117110099028025087042047011052015006024070008005030068029035087041088123002020108112120118003122076082025004024015079107119028093002076031081026&EXT=pdf&INDEX=TRUE>. Acesso em: 02 abr. 2024.

DIAS, Patricia Yurie. **Os desafios do direito digital e das políticas públicas para proteger o direito à privacidade no âmbito da atuação dos provedores da internet.** Disponível em: <https://periodicos.uem.br/ojs/index.php/EspacoAcademico/article/view/52117>. Acesso em: 18 out. 2023.

DURIGAN, Victor: PEREIRA, Laura. **Liberdade de expressão e segurança: internet como espaço da prática democrática.** Disponivel em: <https://www.jota.info/opiniao-e-analise/colunas/tecnologia-cultura-digital/liberdade-de-expressao-e-seguranca-internet-como-espaco-da-pratica-democratica-19052022>. Acesso em: 04 nov. 2023.

FILHO, Gracia Bernardo Advogados. **Lei Carolina Dieckmann: saiba o que é.** Disponível em: <https://www.gbfadvogados.com.br/single-post/lei-carolina-dieckmann-o-que-e#:~:text=A%20Lei%20Carolina%20Dieckmann%20foi,ambos%20do%20mesmo%20diploma%20legal>. Acesso em: 01 abr. 2024.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. P**rivacidade e lei geral de proteção de dados pessoais.** Revista de Direito Brasileira, v. 23, n. 9, p. 284-301, 2020.

FRAGOSO, Nathalie. **O Impacto do Marco Civil sobre a proteção da privacidade no Brasil.** Disponível em: <https://internetlab.org.br/pt/especial/o-impacto-do-marco-civil-sobre-a-protecao-da-privacidade-no-brasil/>. Acesso em: 07 abr. 2024.

GUIMARÃES, Antônio Márcio da Cunha *at all*. **DIREITO DIGITAL.** Disponível em: <https://revistas.pucsp.br/index.php/DIGE/article/view/35175> Acesso em: 19 out. 2023.

ISRAEL, Carolina. **Território, jurisdição e ciberespaço: entre os contornos westfalianos e a qualidade transfronteiriça da Internet.** 2020. Disponível em: <https://www.revistas.usp.br/geousp/article/view/161521/160400.>. Acesso em: 03 abr. 2024.

LEMOS, Ronaldo. **O Marco Civil como Símbolo do Desejo por Inovação do Brasil**. In: LEITE, George Salomão; LEMOS, Ronaldo. Marco Civil da Internet. São Paulo: Editora Atlas S.A., 2014, p. 4.

_____, Ronaldo; SOUZA, Carlos Affonso. **Marco Civil da Internet: Construção e Aplicação.** Juiz de Fora: Editar Editora Associada Ltda, 2016.

Lorenzo, J. V. (2023). **A Aplicação do Direito Internacional no Ciberespaço: Questões de Soberania e Jurisdição.** Ciências Jurídicas, Ciências Sociais, v. 26, ed. 122, mai. 2023. Disponível em: <https://revistaft.com.br/a-aplicacao-do-direito-internacional-no-ciberespaco-questoes-de-soberania-e-jurisdicao/#:~:text=O%20ciberespa%C3%A7o%20n%C3%A3o%20obedece%20a,observado%20por%20Israel%20(2020)>. Acesso em: 03 abr. 2024.

MAZZUOLI, Valerio de Oliveira. **Curso de Direitos Humanos.** São Paulo: Forense, 2019.

MONTEIRO, R. L. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?**. Instituto Igarapé, Artigo Estratégico 39. 2018. 27p. Disponível em: <https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf>. Acesso em: 31 out. 2023.

NÓBREGA, Ana. **Privacidade na internet: saiba proteger seus dados.** Disponível em: <https://www.ecycle.com.br/privacidade-na-internet/>. Acesso em: 03 abr. 2024.

OLIVEIRA, Ana Paula. **Entenda quem é o DPO/Encarregado de dados.** Disponível em: <https://www.jusbrasil.com.br/artigos/entenda-quem-e-o-dpo-encarregado-de-dados/1270633228> Acesso em: 09 abr. 2024.

RAMOS, Rahellen. **O que é o Marco Civil da Internet?.** Disponível em: <https://www.politize.com.br/marco-civil-da-internet /> Acesso em: 20 out. 2023.

RODRIGUES, Lucas Fernandes (2022). **Direitos Humanos e a Era Digital: A Necessidade da Proteção de Dados como um Direito Fundamental.** Revista Ratio Iuris – UFPB, v. 1, n. 1.

SALOMÃO, Mariana Silva. **Marco Civil da Internet: Perspectivas de Aplicação e seus Desafios.** Rio de Janeiro: Escola da Magistratura do Estado do Rio de Janeiro, 2016.

SARLET, Ingo Wolfgang. **Proteção de Dados Pessoais como Direito Fundamental na Constituição Federal Brasileira de 1988: Contributo para a Construção de uma Dogmática Constitucionalmente Adequada.** Revista Brasileira de Direitos Fundamentais & Justiça, v. 14, n. 42, pp. 179 á 218, janeiro a junho de 2020.

VIERA: BARBOSA: CARNEIRO. **O que é o Direito Autoral e propriedade intelectual?.** VBC Advogados Associados, 08/02/2020. Disponível em: <https://www.vbcadvogados.com.br/o-que-e-direito-autoral-e-propriedade-intelectual/>. Acesso em: 31 out. 2023.

Direitos Humanos no contexto da democracia digital no Brasil e no mundo são discutidos em painel. OAB/RS, 2020. Disponível em: <https://bit.ly/2DWDOoz>. Acesso em: 31 out. 2023.

WhatsApp já foi bloqueado por decisão judicial em 2015 e 2016 no Brasil. g1, 18/03/2022. Disponível em: <https://g1.globo.com/tecnologia/noticia/2022/03/18/whatsapp-ja-foi-bloqueado-por-decisao-judicial-em-2015-e-2016-no-brasil.ghtml>. Acesso em: 29 out. 2023.

O que são tecnologias emergentes e quais as principais. Sankhya, 19/06/2023. Disponível em: <https://www.sankhya.com.br/blog/tecnologias-emergentes/>. Acesso em: 31 out. 2023.

Contrato eletrônico: o que é, tipos, validade jurídica e como fazer. Equipe TOTVS, 18/10/2023. Disponível em: <https://www.totvs.com/blog/gestao-para-assinatura-de-documentos/contrato-eletronico/>. Acesso em: 31 out. 2032.