



CURSO DE DIREITO

GENIFFER DE FIGUEIREDO LUCAS

**RESPONSABILIZAÇÃO DAS PLATAFORMAS DIGITAIS EM CRIMES
CIBERNÉTICOS: UMA ANÁLISE A PARTIR DA PLATAFORMA
DISCORD**

**Cuiabá/MT
2026**



CURSO DE DIREITO

GENIFFER DE FIGUEIREDO LUCAS

**RESPONSABILIZAÇÃO DAS PLATAFORMAS DIGITAIS EM CRIMES
CIBERNÉTICOS: UMA ANÁLISE A PARTIR DA PLATAFORMA
DISCORD**

Trabalho de Conclusão de Curso
apresentado à Banca Avaliadora do
Departamento de Direito, da Faculdade de
FASIPE CPA, como requisito parcial para
a obtenção do título de Bacharel em
Direito.

Orientadora: Prof^a Luana Fátima Zapello

**Cuiabá/MT
2026**

GENIFFER DE FIGUEIREDO LUCAS

**RESPONSABILIZAÇÃO DAS PLATAFORMAS DIGITAIS EM CRIMES
CIBERNÉTICOS: UMA ANÁLISE A PARTIR DA PLATAFORMA
DISCORD**

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Curso de Direito – FASIPE Cuiabá, como requisito parcial para a obtenção do título de Bacharel em Direito.

Aprovado em:

Luana Fatima Zapello
Professor(a) Orientador(a)
Departamento de Direito – FASIPE Cuiabá

NOME EXAMINADOR:
Professor(a) Avaliador(a)
Departamento de Direito – FASIPE Cuiabá

NOME EXAMINADOR:
Professor(a) Avaliador(a)
Departamento de Direito – FASIPE Cuiabá

Professor(a) Avaliador(a)
Departamento de Direito – FASIPE Cuiabá
Coordenador do Curso de Direito

**Cuiabá/MT
2026**

LUCAS, Geniffer de Figueiredo. RESPONSABILIZAÇÃO DAS PLATAFORMAS DIGITAIS EM CRIMES CIBERNÉTICOS: uma análise a partir da plataforma discord 2026. 47 F. Trabalho de Conclusão de Curso – Faculdade de Cuiabá – FASIPE.

RESUMO

Analisa-se a responsabilidade civil da plataforma Discord diante dos crimes cibernéticos e falhas de segurança sistêmica, com ênfase na proteção de vulneráveis. Objetiva-se investigar o dever de cuidado da empresa sob a ótica do Código de Defesa do Consumidor e da recente virada jurisprudencial do Supremo Tribunal Federal nos Temas 533 e 987, que discutem a constitucionalidade do Marco Civil da Internet. A metodologia consiste em uma pesquisa bibliográfica e documental de natureza qualitativa, utilizando o método dedutivo para analisar doutrinas de Robert Alexy e Paulo Bonavides, além de dados extraídos de inquéritos civis do Ministério Público de São Paulo. Os resultados demonstram que a arquitetura do Discord, ao privilegiar o anonimato e a fragmentação em servidores privados sem moderação proativa, favorece a impunidade digital e a propagação de conteúdos ilícitos. Conclui-se que a imunidade do Artigo 19 do Marco Civil tornou-se insuficiente, sendo imperativa a transição para um regime de responsabilidade objetiva e proativa. O equilíbrio entre privacidade e segurança pública deve ser pautado pela função social da empresa e pelo fortalecimento da autonomia ética do usuário.

Palavras-chave: Responsabilidade Civil; Discord; Direitos Fundamentais; Marco Civil da Internet; Segurança Digital.

LUCAS, Geniffer de Figueiredo. ACCOUNTABILITY OF DIGITAL PLATFORMS IN CYBERCRIMES: an analysis based on the Discord. 2026. 47 F. Final Course Project – Faculty of Cuiabá – FASIPE.

ABSTRACT

This study analyzes the civil liability of the Discord platform regarding cybercrimes and systemic security failures, emphasizing the protection of vulnerable individuals. It aims to investigate the company's duty of care from the perspective of the Consumer Defense Code and the recent jurisprudential shift of the Brazilian Supreme Court (STF) in Themes 533 and 987, which debate the constitutionality of the Civil Framework of the Internet. The methodology consists of qualitative bibliographic and documentary research, employing the deductive method to analyze the doctrines of Robert Alexy and Paulo Bonavides, alongside data from civil inquiries by the São Paulo Public Prosecutor's Office. Results demonstrate that Discord's architecture, by prioritizing anonymity and fragmentation into private servers without proactive moderation, fosters digital impunity and the spread of illicit content. It is concluded that the immunity provided by Article 19 of the Civil Framework has become insufficient, making a transition to an objective and proactive liability regime imperative. The balance between privacy and public safety must be guided by the company's social function and the strengthening of the user's ethical autonomy.

Keywords: Civil Liability; Discord; Fundamental Rights; Civil Framework of the Internet; Digital Security.

LISTA DE TABELAS

Tabela 1 – Classificação dos Crimes Cibernéticos.....	13
Tabela 2 – Comparativo entre Crimes Comuns e Delitos Informáticos.....	18
Tabela 3 – Sanções Administrativas Previstas na LGPD.....	20
Tabela 4 – Cronologia e Marcos do Marco Civil da Internet.....	23
Tabela 5 – Estrutura Organizacional da Plataforma Discord.....	24
Tabela 6 – Matriz de Responsabilidade e Moderação de Conteúdo.....	26

SUMÁRIO

1. INTRODUÇÃO	8
2. A EVOLUÇÃO DO AMBIENTE DIGITAL E OS CRIMES CIBERNÉTICOS	10
2.1 A história da internet, sua expansão no Brasil e o surgimento das redes sociais	10
2.2 Ciberdelitos: Classificação e Modalidades Criminosas	12
2.3 O Impacto do Anonimato: Da Invisibilidade de Gigas à Vigilância Digital	14
3. O MARCO JURÍDICO BRASILEIRO APLICÁVEL À INTERNET	17
3.1 A criação e os fundamentos do Marco Civil da Internet	17
3.2 A Lei Geral de Proteção de Dados (LGPD) e a Privacidade do Usuário	19
3.3 A Natureza Jurídica das Plataformas e os Limites da Autonomia Contratual e Individual	21
3.4 O Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025) e a Implementação de Ferramentas Protetivas	22
4 DISCORD	25
4.1 A Estrutura Técnica do Discord: Servidores, Bots e a Gestão de Comunidades	25
4.2 Privacidade versus Segurança Pública	27
4.3 A Cultura da Impunidade e a Fragilidade da Denúncia	29
5 ARTIGO 19 DO MARCO CIVIL DA INTERNET E A TESE DA INCONSTITUCIONALIDADE PARCIAL	32
5.1 O Regime de Responsabilidade Passiva Original (2014-2025)	32
5.2 O Julgamento dos Temas 533 e 987: A Virada de Paradigma no STF	33
5.3 A Configuração da Falha Sistêmica e a Natureza Híbrida do Discord frente à Jurisprudência do STF	34
5.4 A Autonomia Individual e Contratual como Fronteiras no Direito Digital	35
6 CONSIDERAÇÕES FINAIS	37
REFERÊNCIAS	39

1 INTRODUÇÃO

A evolução exponencial das tecnologias de informação e comunicação transformou a internet em um pilar fundamental da sociedade contemporânea, alterando as dinâmicas de interação social e institucional. Essa mesma infraestrutura que promove a conectividade também atua como cenário para o surgimento de novas modalidades criminosas. No Brasil, o ordenamento jurídico buscou acompanhar essa transição através dos marcos regulatórios como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Entretanto, o surgimento de plataformas com arquiteturas complexas, como o Discord, impõe desafios inéditos à eficácia dessas normas e à segurança pública.

O problema central desta pesquisa reside na dificuldade de fiscalização estatal e na responsabilidade das plataformas perante crimes cibernéticos ocorridos em ambientes semifechados. A estrutura do Discord, baseada em servidores privados e canais de comunicação muitas vezes inacessíveis aos mecanismos tradicionais de monitoramento, levanta o questionamento: até que ponto a plataforma deve ser civilmente responsabilizada pela disseminação de conteúdos ilícitos e pela prática de crimes em seus domínios? A relevância deste tema acentua-se diante da recente virada jurisprudencial do Supremo Tribunal Federal, que passou a exigir das big techs um dever de cuidado mais rigoroso para evitar falhas sistêmicas que facilitem a atividade criminosa.

Diante desse cenário, o presente trabalho tem como objetivo geral analisar a responsabilidade civil das plataformas digitais frente aos crimes cibernéticos, com foco específico na análise do Discord. Para tal, pretende-se investigar o panorama histórico e jurídico da internet no Brasil, discutir os fundamentos éticos e filosóficos que norteiam o comportamento humano e a autonomia no ambiente digital, e avaliar a eficácia dos mecanismos de moderação do conteúdo em face da nova interpretação constitucional sobre o Artigo 19 do Marco Civil da Internet. Justifica-se esta abordagem pela necessidade premente de equilibrar o direito à privacidade e a liberdade de associação com o dever de segurança e a proteção de direitos fundamentais das vítimas.

A metodologia adotada para a consecução destes objetivos consiste em uma pesquisa de natureza qualitativa e caráter dedutivo, pautada na revisão bibliográfica e na análise documental. Foram utilizados como base teórica os principais dispositivos legais brasileiros, a doutrina especializada em Direito Digital e Civil, além da análise de casos concretos e relatórios de transparência. Estruturalmente, o trabalho divide-se em capítulos que percorrem desde a evolução histórica e os fundamentos filosóficos da conduta humana até o exame detalhado da arquitetura do Discord e as implicações da responsabilidade objetiva das redes sociais no cenário jurídico atual.

2 A EVOLUÇÃO DO AMBIENTE DIGITAL E OS CRIMES CIBERNÉTICOS

2.1 A história da internet, sua expansão no Brasil e o surgimento das redes sociais

De acordo com estudos sobre a evolução da Internet (Carvalho; Arita; Nunes, 1999), sua origem antecede o surgimento da Web e remonta ao início da década de 1960, quando a empresa RAND, financiada pela Força Aérea dos Estados Unidos, desenvolveu um projeto que buscava criar uma rede de comunicação militar capaz de resistir a ataques nucleares. Essa preocupação surgiu devido ao clima tenso da Guerra Fria, período em que o governo norte-americano temia falhas na comunicação em caso de conflito. Essa gênese militar imprimiu na rede uma lógica de descentralização, criando uma arquitetura onde a informação não possui um centro único de controle, o que molda até hoje os desafios jurídicos para a implementação de mecanismos de vigilância e proteção de dados (Bioni, 2019).

Em 1969, ainda nesse contexto de competição tecnológica e militar com a antiga União Soviética, o Departamento de Defesa dos Estados Unidos, por meio da ARPA, deu início à ARPANET, uma rede experimental que se tornou a base histórica do que hoje conhecemos como Internet. As primeiras ligações foram estabelecidas entre quatro universidades: UCLA, SRI, Universidade da Califórnia em Santa Bárbara e a Universidade de Utah. Com o crescimento acelerado, surgiram incompatibilidades entre os equipamentos utilizados, pois não havia um padrão definido para comunicação entre máquinas. Na década de 1970, os pesquisadores Vinton Cerf e Robert Kahn desenvolveram então os protocolos TCP/IP, que permitiram organizar o envio e recebimento dos pacotes de dados entre computadores interligados.

Essa padronização técnica foi o passo decisivo para a transformação da internet em um ambiente social, pois permitiu que diferentes redes se comunicassem, transformando o ciberespaço em um novo território onde direitos e deveres civis precisam ser observados (Pinheiro, 2023). Em 1975, a administração da ARPANET saiu do âmbito acadêmico e passou para a *Defense Communication Agency*. Porém, em 1983, preocupações com segurança levaram à criação da

MILNET, voltada exclusivamente às necessidades das Forças Armadas, enquanto a ARPANET começou a ser gradualmente desativada. Pouco depois, a *National Science Foundation* conectou sua própria rede, a NSFnet, transformando-a em um *backbone* para o tráfego científico.

Ainda na década de 1980, o surgimento das empresas como Apple e Microsoft impulsionou o acesso doméstico a microcomputadores. Em 1989, o pesquisador Tim Berners-Lee apresentou o projeto da *World Wide Web*, introduzindo recursos como o protocolo HTTP e a linguagem HTML. Essa facilitação do acesso mudou a forma como a sociedade interage com a informação, mas com essa exposição massiva de dados em ambiente digital gerou novos riscos à personalidade e à privacidade (Schreiber, 2023).

No cenário brasileiro, o processo de implantação da rede iniciou-se formalmente em 1987, sob uma forte influência da comunidade acadêmica que buscava integrar o Brasil aos fluxos globais de informação científica. As discussões iniciais envolveram instituições como a USP e o LNCC, culminando na criação da Rede Nacional de Pesquisa (RNP) em 1989. O objetivo primordial da RNP, era estabelecer uma infraestrutura de alto desempenho para o ensino e pesquisa, conectando diversas capitais brasileiras por meio das redes de computadores que superavam as limitações técnicas da época (Carvalho, 2006).

A década de 1990 marcou a transição da internet acadêmica para o modelo comercial no Brasil. Em 1995, a criação do Comitê Gestor da Internet, representou um marco na governança da rede no país, adotando um modelo multissetorial que envolve governo, setor empresarial, terceiro setor e academia.

De acordo com as discussões trazidas pelo Comitê Gestor da Internet no Brasil, essa estrutura de governança foi essencial para garantir a estabilidade e a segurança da rede nacional, promovendo a disseminação do domínio ".br" como um símbolo de confiabilidade e identidade digital para os brasileiros (Ctic.br, 2010).

A expansão comercial permitiu que o Brasil atingisse patamares de conectividade sem precedentes. Segundo dados recentes da pesquisa TIC Domicílios 2024, aproximadamente 84% da população brasileira está conectada, consolidando o acesso por meio de dispositivos móveis como a principal porta de entrada para o ambiente virtual. Essa "conectividade de bolso" facilitou o surgimento

e a popularização de redes sociais e plataformas de comunicação em tempo real, como o Discord, que operam sob arquiteturas complexas de troca de dados.

Contudo, essa evolução tecnológica traz desafios jurídicos profundos. O avanço da sociedade digital brasileira exige que o ordenamento jurídico proteja o cidadão contra novas formas de violência e monitoramento indevido. A proteção de dados pessoais é um direito fundamental, e o pilar que deve sustentar a interação entre usuários e plataformas, garantindo que o desenvolvimento técnico não ocorra às custas da dignidade humana e da privacidade individual (Pinheiro, 2023).

Nesse sentido, a trajetória da internet no Brasil, demonstra que o ambiente digital deixou de ser uma ferramenta acessória para se tornar o palco principal das relações sociais e jurídicas contemporâneas. Essa migração massiva da vida privada para servidores controlados por entes privados, exige que o Direito Civil repense as formas tradicionais da reparação de danos, especialmente diante da velocidade e do alcance global das ofensas cometidas no ciberespaço (Schreiber, 2023).

2.2 Ciberdelitos: Classificação e Modalidades Criminosas

A internet consolidou-se como uma ferramenta de extrema agilidade, capaz de aproximar o agente criminoso da vítima de forma instantânea, facilitando a consumação de delitos em cenários de vulnerabilidade técnica e informacional. A investigação e a compreensão exigem uma distinção clara entre os delitos que utilizam a rede apenas como meio e aqueles que a têm como fim. O crime cibernético se caracteriza pela transposição de condutas ilícitas tradicionais para o ambiente digital, onde a desterritorialização e a volatilidade das provas tornam a repressão estatal um desafio constante (Brasil, 2024).

Nessa linha, conforme ensinam Goulart e Cordova (2024), os crimes cometidos no ambiente virtual são geralmente agrupados em duas categorias fundamentais. A primeira compreende os crimes impróprios, nos quais o dispositivo funciona apenas como o instrumento para a prática de ilícitos já previstos no Código Penal, como fraudes, estelionatos e crimes contra a honra. A segunda categoria abrange os crimes próprios ou puros, em que o computador e os sistemas informáticos são o alvo direto da conduta criminosa, visando a destruição de dados ou a interrupção de serviços essenciais.

Dentro dessa classificação, destaca-se o *hacking*, caracterizado pelo acesso não autorizado a sistemas para subtração de dados sensíveis. Contudo, a modalidade que apresenta maior crescimento no Brasil é o *phishing*. Segundo o Manual de Investigação Cibernética, essa técnica baseia-se na engenharia social, onde o criminoso manipula psicologicamente a vítima para que ela voluntariamente entregue suas credenciais ou informações financeiras (Brasil; Barreto, 2024). A relevância dessa prática é confirmada pelo Anuário Brasileiro de Segurança Pública (2025), que aponta uma migração estrutural da criminalidade: enquanto delitos de rua diminuem, o estelionato eletrônico saltou para 281 mil casos em 2024, representando um aumento de 17%.

A vulnerabilidade não se restringe apenas à técnica, mas também à faixa etária dos usuários. Conforme dados coletados pelo Instituto de Pesquisa DataSenado em 2025, os golpes virtuais atingem todas as camadas da população, desafiando o senso comum de que apenas idosos seriam vítimas frequentes. Os dados revelam que jovens e adultos em idade produtiva são alvos constantes devido à alta exposição em plataformas digitais.

Tabela 1 – Percentual de Vítimas de Crimes Digitais por Faixa Etária (2024)

Faixa Etária	Percentual de Vítimas
16 a 29 anos	27%
30 a 39 anos	23%
40 a 49 anos	20%
50 a 59 anos	14%
60 anos ou mais	16%

Fonte: DataSenado (2025)

Outra ameaça severa ao ambiente institucional é o *ransomware*, modalidade de *malware* que sequestra dados mediante criptografia e exige resgate. Segundo o Relatório de Avaliação da Política Pública do Senado Federal, o impacto desses ataques ultrapassa o prejuízo financeiro, atingindo a própria soberania e segurança nacional, uma vez que órgãos públicos e infraestruturas críticas têm sido alvos frequentes dos grupos criminosos organizados (Brasil, 2024). A complexidade reside na dificuldade de rastreio, uma vez que os pagamentos são solicitados em ativos digitais que facilitam a lavagem de dinheiro.

Além dos danos patrimoniais, a SaferNet Brasil (2025), alerta para a gravidade dos crimes contra a dignidade humana. No último período, as notificações totalizaram 87.689 queixas únicas, com um protagonismo preocupante dos casos de abusos sexuais infantis e misoginias, potencializados pelo uso de inteligência artificial generativa para a criação dos conteúdos ilícitos. No entanto, a legislação brasileira, por meio do Marco Civil da Internet e da LGPD, tenta criar barreiras, mas a velocidade da inovação tecnológica muitas vezes supera a capacidade de respostas das normas vigentes (Pinheiro, 2023).

Por fim, o cenário da expansão digital revelado pela pesquisa TIC Domicílios 2024, demonstra que a universalização do acesso, não foi acompanhada por uma educação digital preventiva. Práticas como o *cyberbullying* e o roubo da identidade encontram solo fértil em plataformas como o Discord, que priorizam a agilidade da interação em detrimento dos mecanismos rígidos de verificação. Contudo, a facilidade do anonimato e a arquitetura dessas plataformas criam um sentimento de impunidade, exigindo que a responsabilidade civil seja aplicada de forma a incentivar um dever de cuidado mais rigoroso pelos provedores de aplicação (Schreiber, 2023).

2.3 O Impacto do Anonimato: Da Invisibilidade de Giges à Vigilância Digital

A compreensão das dinâmicas delitivas no ambiente virtual exige uma análise que transcende o aspecto técnico, adentrando no campo da filosofia moral e da teoria política. O anonimato, ou a percepção subjetiva de estar oculto sob camadas de criptografias e pseudônimos, atua como um catalisador de comportamentos que, em circunstâncias da exposição social direta, seriam reprimidos pelo receio da sanção ou do julgamento coletivo.

Esta desinibição digital encontra um pilar interpretativo fundamental no "Mito de Giges", narrado por Platão em sua obra *A República*. Na alegoria, o personagem descobre um anel que, ao ser girado, lhe confere o poder da invisibilidade. Diante da certeza de que suas ações não seriam descobertas, Giges abandona qualquer senso de justiça e moralidade, cometendo crimes atrozes para satisfazer seus desejos pessoais (Platão, 2006).

No século XXI, o "Anel de Giges" materializa-se na própria interface das plataformas digitais. O Discord, com sua estrutura dos servidores fechados e a possibilidade de alteração constante das identidades virtuais, permite que o usuário se sinta imune ao olhar da justiça, mimetizando a invisibilidade do mito grego para agir à margem da lei.

Para aprofundar a análise sobre o controle desses impulsos e a estrutura do poder na rede, recorre-se ao conceito de panoptismo. O Panóptico, idealizado originalmente como uma arquitetura carcerária, baseia-se em um mecanismo de vigilância onde o indivíduo, por não saber se está sendo observado em um dado momento, passa a policiar o próprio comportamento, internalizando a norma (Foucault, 1999). No Direito tradicional, a publicidade dos atos e a presença física das autoridades, funcionam como este olhar vigilante.

Contudo, observa-se uma ruptura com a lógica foucaultiana em plataformas da comunicação privada. A arquitetura das "painéis" (grupos restritos e criptografados), inverte o Panóptico: em vez da sensação de vigilância constante que gera a autodisciplina, o usuário é imerso em uma cultura de opacidade técnica. Quando a sensação de estar sendo vigiado desaparece, a barreira ética da autodisciplina falha, dando lugar a uma percepção de impunidade absoluta. No entanto, essa quebra de visibilidade dificulta a aplicação do dever de cuidado, transformando nichos digitais em zonas de sombra jurídica (Pinheiro, 2023).

É nesse cenário de invisibilidade que o ambiente digital se aproxima do que Thomas Hobbes denomina como "Estado de Natureza" em sua obra *Leviatã*. Para o autor, a ausência de um poder central soberano capaz de impor o medo da punição faz com que a sociedade mergulhe em um estado de guerra de "todos contra todos", onde não há noção do justo ou injusto, mas apenas o predomínio da força (Hobbes, 2003).

Nesse contexto, o homem torna-se o "lobo do próprio homem" (*homo homini lupus*), agindo de forma predatória. O Discord, ao permitir a criação de comunidades onde as regras estatais parecem não alcançar, cria microcosmos desse estado hobbesiano. Logo, nesses espaços, agentes tecnicamente mais capazes ou organizados em grupos de ataque, subjagam vítimas através de assédios, extorsões e vazamento de dados, acreditando que a arquitetura da plataforma os protege da soberania do Estado.

Dessa forma, a problemática jurídica emerge da tensão entre a liberdade total, que remete ao caos do estado de natureza, e a necessidade de preservação da integridade coletiva por meio do contrato social digital. O paralelo entre Gíges, Foucault e Hobbes ilustra que, no ambiente virtual, o anonimato não deve ser interpretado como um salvo-conduto para o ilícito. A solução jurídica contemporânea, portanto, não reside apenas na vigilância estatal onipresente, que feriria garantias constitucionais, mas no fortalecimento da imputabilidade. Portanto, a responsabilidade deve recair tanto sobre a conduta do agente que se esconde nas sombras quanto sobre o dever das plataformas em oferecer uma infraestrutura que impeça a transformação da autonomia digital em um cenário de barbárie e impunidade (Schreiber, 2023).

3 O MARCO JURÍDICO BRASILEIRO APLICÁVEL À INTERNET

3.1 A criação e os fundamentos do Marco Civil da Internet

O advento da Lei nº 12.965, popularmente conhecida como o Marco Civil da Internet (MCI), representou um divisor de águas no ordenamento jurídico brasileiro. Diferente de outras normas que surgiram de gabinetes fechados, o MCI foi fruto de uma construção colaborativa inédita, iniciada em 2009 através de uma consulta pública coordenada pelo Ministério da Justiça em parceria com o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas (FGV). Conforme explica o Serviço Federal de Processamento de Dados (2025), a lei não foi um evento isolado, mas o ápice de um longo processo de maturação sobre a necessidade de estabelecer "regras do jogo" para o ambiente digital.

Historicamente, o Brasil tentou regulamentar a rede sob uma ótica puramente punitiva, como observado no Projeto de Lei 84/1999 (conhecido como Lei Azeredo), que focava excessivamente na tipificação de crimes e na vigilância. No entanto, a sociedade civil e setores acadêmicos reagiram, defendendo que, antes de punir, era necessário garantir direitos. Esse conflito de visões, gerou um hiato legislativo: enquanto a tecnologia avançava a passos largos, o Brasil permanecia em um vácuo normativo. O Marco Civil surgiu, portanto, com um propósito civilista: ser uma "Constituição Digital" que equilibrasse a liberdade de expressão com a proteção de dados e a responsabilidade dos provedores.

Dois fatos políticos foram determinantes para acelerar a aprovação do texto que enfrentava forte resistência no Congresso Nacional. O primeiro foi o vazamento de fotos íntimas da atriz Carolina Dieckmann, que resultou na Lei nº 12.737/2012; o segundo, e mais impactante, foram as denúncias de Edward Snowden em 2013, sobre o esquema de espionagem em massa dos Estados Unidos, que atingiu inclusive a cúpula do governo brasileiro. Esses eventos evidenciaram que a internet não era apenas uma ferramenta de lazer, mas um campo de soberania e direitos fundamentais que não podiam mais esperar (Senado Notícias, 2013).

Fundamentado no tripé da Liberdade, Privacidade e Neutralidade, o Marco Civil trouxe o suporte operacional ao Artigo 5º da Constituição Federal para o campo telemático, sintetizando seus princípios na estrutura abaixo:

Tabela 2 – Pilares Fundamentais da Lei nº 12.965/2014 (Marco Civil da Internet)

Pilar Fundamental	Base Legal	Descrição e Aplicação
Neutralidade de Rede	Artigo 9º	Impede a discriminação ou degradação do tráfego de dados. Garante que a operadora não favoreça sites ou apps específicos.
Privacidade e Proteção	Artigo 7º e 10	Garante a inviolabilidade das comunicações e exige ordem judicial para quebra de sigilo de dados e registros.
Liberdade de Expressão	Artigo 2º e 3º	Estabelece que o uso da internet no Brasil tem como condição a liberdade de expressão e a manifestação do pensamento.
Responsabilidade Civil	Artigo 19	Determina que provedores só respondem por danos de terceiros se descumprirem ordem judicial de remoção de conteúdo.

Fonte: Própria (2025)

A neutralidade de rede (Art. 9º) foi o ponto de maior conflito com as empresas de telecomunicações. Ela impede que provedores de conexão discriminem o tráfego de dados por conteúdo ou serviço. Sem ela, operadoras poderiam "viciar" o mercado, favorecendo grandes plataformas em detrimento dos pequenos desenvolvedores ou cobrando pacotes diferenciados para acesso a redes sociais. O MCI garantiu que a rede permanecesse democrática e isonômica.

Todavia, emerge aqui uma polêmica central que atinge diretamente o objeto desta pesquisa: a responsabilidade civil por danos (Artigo 19). O legislador optou por um regime de responsabilidade subjetiva para os provedores de aplicações de internet (como o Discord). Em regra, a plataforma só responde civilmente por danos

decorrentes do conteúdo gerado por terceiros se, após a ordem judicial específica, não tomar providências para tornar o conteúdo indisponível.

Essa escolha visava proteger a liberdade de expressão, evitando que as empresas se tornassem "juízes privados". Contudo, como ressalta a doutrina de Patrícia Peck Pinheiro (2023), esse modelo cria um descompasso temporal perigoso: o crime cibernético ocorre em milissegundos, enquanto uma ordem judicial pode levar dias. No caso de crimes graves em servidores fechados, essa "imunidade temporária" pode acabar servindo como um escudo para a impunidade, mantendo a "invisibilidade de Giges" enquanto o processo judicial não se concretiza.

Dessa forma, o Marco Civil simboliza um avanço, mas seu equilíbrio entre liberdade e responsabilidade é constantemente testado pela arquitetura de redes fechadas, onde a autorresponsabilidade do usuário e o dever de vigilância da plataforma tornam-se os novos centros do debate jurídico.

3.2 A Lei Geral de Proteção de Dados (LGPD) e a Privacidade do Usuário

Com a promulgação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), o Brasil consolidou o conceito de autodeterminação informativa. Se o Marco Civil da Internet estabeleceu os direitos e deveres na rede, a LGPD veio para disciplinar o ciclo de vida das informações pessoais como devem ser coletadas, tratadas, armazenadas e descartadas. Este avanço culminou na Emenda Constitucional nº 115/2022, que elevou a proteção dos dados pessoais ao status de direito fundamental no Artigo 5º da Constituição Federal.

Para plataforma de comunicação instantânea e comunidades fechadas, como o Discord, a LGPD impõe uma governança ética rigorosa. O tratamento de dados não é mais uma escolha comercial, mas uma obrigação legal pautada em princípios como a finalidade e a necessidade. Isso significa que o Discord deve coletar apenas o mínimo de dados necessários para o seu funcionamento, garantindo ao usuário a titularidade sobre suas informações. No entanto, emerge aqui o conflito central para a segurança pública: o equilíbrio entre o sigilo de dados e a repressão a ilícitos.

A LGPD não deve ser lida como um salvo-conduto para a impunidade sob o manto do anonimato. O Artigo 2º da lei estabelece que, embora a privacidade e a inviolabilidade da intimidade sejam fundamentos, a defesa dos direitos humanos e o

desenvolvimento nacional também o são. Para facilitar a compreensão das obrigações da plataforma sob este novo regime, a tabela abaixo sintetiza os princípios que regem a atuação do Discord como gestor de dados:

Tabela 3 – Princípios de Tratamento de Dados Aplicáveis às Plataformas (Art. 6º LGPD)

Princípio	Descrição Legal	Aplicação no Ecossistema Discord
Finalidade	Realização do tratamento para propósitos legítimos e específicos.	A plataforma não pode usar dados de segurança para fins comerciais sem aviso.
Transparência	Garantia de informações claras e precisas sobre o tratamento.	O usuário deve saber quais dados de logs são mantidos e por quanto tempo.
Segurança	Uso de medidas técnicas para proteger dados de acessos não autorizados.	Dever de implementar criptografia e barreiras contra invasões em servidores.
Responsabilização	Demonstração da adoção de medidas eficazes para cumprir a lei.	A plataforma deve provar que possui meios de identificar abusos em sua rede.

Fonte: Própria (2025)

Sob a ótica da proteção de dados, o Discord assume a posição jurídica de Controlador, pois é quem detém o poder de decisão sobre o tratamento dos dados pessoais em seus servidores. Isso gera o dever de implementar medidas técnicas e administrativas aptas a mitigar riscos. Em ambientes de alta opacidade, como os servidores privados, a opacidade técnica não pode ser confundida com ausência de responsabilidade. Se a plataforma falha em cooperar com investigações de crimes graves sob a justificativa de uma interpretação absoluta da privacidade, ela viola os princípios da boa-fé e da transparência (Schreiber, 2022).

Nesse sentido, a LGPD reforça que o usuário não é um "produto" ou um "dado estatístico", mas um sujeito de direitos. Contudo, essa proteção deve ser equilibrada, onde a privacidade garantida pela lei serve para proteger a liberdade do cidadão, e não para blindar criminosos que utilizam a infraestrutura tecnológica para ferir a dignidade de outrem. A governança de dados, portanto, deve ser a "primeira parede" de proteção, onde a plataforma utiliza os logs e metadados que coleta para garantir a segurança do seu ecossistema, prevenindo que o anonimato digital se torne um refúgio para a barbárie.

3.3 A Natureza Jurídica das Plataformas e os Limites da Autonomia Contratual e Individual

Para determinar como o Discord pode ser responsabilizado, o primeiro passo é definir o que ele representa perante a lei. Atualmente, entende-se que as redes sociais não são apenas "lugares neutros", mas prestadoras de serviço. Isso significa que a relação entre o Discord e o usuário é uma relação de consumo, protegida pelo Código de Defesa do Consumidor (CDC).

Nesse contexto, surge a autonomia contratual. Quando o usuário cria uma conta e aceita os "Termos de Uso", ele está exercendo sua liberdade de aceitar um contrato. Logo, essa autonomia não é absoluta. O Discord não pode usar esse contrato para isentar-se de toda e qualquer responsabilidade. Como a empresa lucra com os dados e a presença dos usuários, ela assume o risco do negócio. Portanto, o contrato assinado não pode anular o dever básico de segurança que o CDC exige.

Além disso, é preciso considerar a autonomia individual. Ela representa a liberdade da escolha e a ética de cada pessoa. No Direito Digital, devemos separar as responsabilidades, ou seja, o usuário que comete um crime deve responder por sua conduta individual (o mau uso da sua autonomia). Porém, isso não retira a culpa da plataforma se ela falhar tecnicamente. Se o Discord oferece ferramentas que facilitam o anonimato radical e não vigia comunidades criminosas, ele falha no seu dever de cuidado.

Esse equilíbrio foi reforçado pelo Supremo Tribunal Federal (STF) em 2025. A justiça entendeu que, embora a liberdade de expressão e a autonomia do usuário sejam importantes, as plataformas têm o dever de agir contra crimes graves. Assim, a autonomia da vontade do usuário não existe sozinha, dependendo de um

ambiente seguro fornecido pela plataforma. Quando o Discord ignora riscos para manter uma postura de neutralidade, ele assume o risco e deve responder por essa falha de segurança.

3.4 O Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025) e a Implementação de Ferramentas Protetivas

A promulgação da Lei nº 15.211, de 17 de setembro de 2025, denominada Estatuto Digital da Criança e do Adolescente, consolida um novo paradigma jurídico no Brasil, deslocando o foco da mera punição para a prevenção estrutural no ambiente virtual. Este diploma legal surge em um momento crítico, onde a digitalização da infância não é mais uma opção, mas uma realidade onipresente. De acordo com os dados apresentados no Resumo Executivo da pesquisa TIC Kids Online Brasil (2025), a conectividade entre menores de 9 a 17 anos atingiu um patamar de quase universalidade, com cerca de 84% desse público acessando a rede múltiplas vezes ao dia (Cetic.br, 2025).

Essa evolução normativa reflete a necessidade premente de operacionalizar o princípio constitucional da prioridade absoluta, positivado no artigo 227 da Carta Magna, transpondo-o de forma impositiva para as relações desenvolvidas no ecossistema da internet. Conforme leciona Patrícia Peck (2021), a hiperconectividade infanto-juvenil exige do ordenamento uma barreira protetiva dinâmica, visto que as vulnerabilidades desse grupo em desenvolvimento são potencializadas pela ausência de fronteiras físicas e pela exposição contínua a estímulos comerciais e interações desreguladas.

A carência de uma legislação específica como o ECA Digital justifica-se pela insuficiência dos mecanismos tradicionais de proteção diante da sofisticação dos algoritmos e da arquitetura das plataformas como o Discord. A Lei nº 15.211/2025 introduz o conceito de "acesso provável", determinando que qualquer serviço tecnológico que possua atratividade ou facilidade do acesso para menores deve, obrigatoriamente, adotar medidas de segurança por padrão (*safety by design*).

Isso implica que a responsabilidade não é mais mitigada pela alegação de que o serviço não era destinado a crianças, caso o uso por este público seja previsível (Brasil, 2025). Sob essa ótica, Tarcísio Teixeira (2023) pondera que as empresas de tecnologia frequentemente utilizavam cláusulas contratuais genéricas

de limitação de idade para transferir todo o dever de vigilância exclusivamente aos pais. A introdução do critério da previsibilidade do acesso altera essa dinâmica de corresponsabilidade, obrigando o provedor de aplicação a gerenciar ativamente os riscos sistêmicos de sua própria engenharia de interface antes mesmo do lançamento do produto no mercado consumidor.

Para compreender a urgência dessa transição legislativa, é necessário observar a evolução do comportamento digital e dos riscos associados entre os anos de 2024 e 2025, conforme demonstrado na tabela abaixo:

Tabela 4- Evolução da Frequência de Uso da Internet por Crianças e Adolescentes (9 a 17 anos)

Frequência de Uso	TIC Kids 2024 (%)	TIC Kids 2025 (%)	Tendência
Mais de uma vez por dia	85%	84%	Estabilidade
Pelo menos uma vez por dia	10%	12%	Crescimento
Pelo menos uma vez por semana	3%	3%	Estabilidade
Total de usuários ativos	98%	99%	Universalização

Fonte: Própria (2024 - 2025)

A estabilidade em níveis elevados demonstrada na Tabela 4, reforça que a proteção digital deve ser contínua e sistêmica. O Estatuto Digital (2025) inova ao exigir que os fornecedores dos produtos e serviços de tecnologia mantenham os representantes legais no Brasil, com poderes para responder judicial e administrativamente por falhas na proteção de menores (Art. 40, Lei 15.211/2025). Essa medida visa combater a sensação de impunidade que frequentemente ampara plataformas estrangeiras que operam sem fiscalização direta em território nacional.

Além disso, a nova legislação impõe uma diferenciação clara entre as obrigações das plataformas conforme o grau de intervenção e risco. Conforme abaixo, sistematiza-se a transição de deveres entre o ECA tradicional e o novo Estatuto Digital:

Tabela 5 - Comparativo de Diretrizes de Proteção: ECA (1990) vs. Estatuto Digital (2025)

Critério de Proteção	ECA (Lei 8.069/90)	Estatuto Digital (Lei 15.211/25)
Foco de Atuação	Proteção física e social analógica.	Proteção em ambientes digitais e algoritmos.
Responsabilidade	Prioritariamente da família e do Estado.	Responsabilidade compartilhada e solidária com plataformas.
Mecanismos de Segurança	Reativos (pós-ocorrência do dano).	Proativos (Safety by Design e Privacidade por Padrão).
Controle de Acesso	Classificação indicativa de TV e cinema.	Verificação robusta de idade e controle parental nativo.
Transparência	Inexistência de obrigações algorítmicas.	Relatórios obrigatórios sobre gestão de riscos sistêmicos.

Fonte: Própria (1990; 2025)

A implementação das ferramentas exigidas pelo ECA Digital como sistema de moderação eficazes e canais de denúncia acessíveis, constitui uma resposta direta ao aumento dos crimes cibernéticos contra a dignidade sexual e a integridade psíquica de menores. Como ressaltado pela pesquisa TIC Kids (2025), o acesso à internet em áreas rurais e em regiões como o Norte e Nordeste apresenta desafios específicos relacionados à segurança e à mediação, o que exige que as ferramentas

de proteção sejam resilientes e adaptáveis às diferentes realidades socioeconômicas (Cetic.br, 2025).

Em suma, o Estatuto Digital não deve ser visto apenas como um conjunto de restrições, mas também como uma ferramenta de empoderamento e segurança. Ao obrigar as *big techs* a assumirem o bônus e o ônus de sua presença no desenvolvimento de crianças e adolescentes, a lei busca restaurar o equilíbrio entre a inovação tecnológica e o respeito inarredável aos direitos humanos fundamentais, garantindo que o ciberespaço seja um local de crescimento, e não de vitimização.

4 DISCORD

4.1 A Estrutura Técnica do Discord: Servidores, Bots e a Gestão de Comunidades

Para compreender a responsabilidade civil no âmbito do Discord, é imperativo analisar a arquitetura técnica da plataforma, que se distancia substancialmente das redes sociais convencionais do fluxo algorítmico global. Enquanto plataformas como Instagram ou X (antigo Twitter) baseiam-se em murais públicos e distribuição massiva de conteúdo, o Discord estrutura-se como um ecossistema de comunidades independentes e fragmentadas, denominadas "servidores". Cada servidor opera como uma célula privada e autônoma, onde o criador do grupo detém o poder soberano de estabelecer normas internas, gerenciar o ingresso dos membros e moderar interações (Guia do iniciante, 2026).

Essa escolha arquitetônica por grupos fechados cria o que a doutrina identifica como "zonas de sombra" para a fiscalização. Diferente das postagens públicas que podem ser indexadas e encontradas por qualquer usuário ou autoridade, no Discord as conversas ocorrem em ambientes protegidos por convites ou senhas. Juridicamente, essa estrutura transfere o ônus da vigilância para usuários voluntários, os moderadores da comunidade em detrimento de um controle centralizado e rigoroso por parte da empresa. No plano teórico, essa ausência de um poder central efetivo mimetiza o "estado de natureza" de Thomas Hobbes, onde a falta de uma autoridade soberana capaz de impor ordem, resulta em espaços onde a lei do mais forte ou a impunidade do criminoso podem prevalecer. Ao delegar a

moderação, a plataforma retira a si mesma e o Estado do centro das interações, criando um cenário de risco sistêmico para usuários hipervulneráveis.

Nesse contexto, existem os *Bots* (robôs de automação), ferramentas essenciais para a gestão das comunidades. Embora o Discord os promova como auxiliares na expulsão dos usuários ofensivos e na organização das tarefas, esses programas possuem uma natureza ambivalente. Sob a ótica do Direito, o ponto nodal reside no fato de que a plataforma oferece a infraestrutura para esses robôs, mas não fiscaliza proativamente se estão sendo utilizados para fins ilícitos, como a exclusão célere de provas ou a ocultação da identidade dos agressores.

De acordo com o *Discord DSA Transparency Report (2025)*, a plataforma afirma realizar medidas por iniciativa própria (*Own-initiative measures*). Porém, os dados mostram uma dependência crítica das denúncias dos usuários para detectar violações em ambientes privados. Na tabela a seguir, sistematiza-se o impacto da automação e da estrutura de servidores na eficácia da moderação, conforme os dados de 2025:

Tabela 6 -Métricas de Moderação e Ação por Iniciativa da Plataforma (2025)

Categoria de Conteúdo	Medidas por Iniciativa Própria	Precisão da Automação (Precision)	Eficácia de Detecção (Recall)
Exploração e Abuso Infantil	35.731	92,30%	90,50%
Discurso de Ódio e Ódio Organizado	50.283	55,10%	97,30%
Conteúdo Violento e Extremo	628	86,00%	90,50%

Fonte: Própria com base em Discord DSA Transparency Report (2025)

A análise dos dados da Tabela 6 revela que, apesar da alta taxa de "Recall" (capacidade de encontrar o conteúdo), a "Precisão" em certas categorias, como o

discurso de ódio, ainda é baixa (55,10%), o que justifica a dependência da moderação humana voluntária. Todavia, sob o prisma do Artigo 14 do Código de Defesa do Consumidor, essa configuração técnica configura uma falha no dever de segurança. Ao lucrar indiretamente com a permanência dos usuários em ambientes que facilitam o anonimato e a destruição das evidências, o Discord assume a responsabilidade objetiva pelos danos decorrentes de um serviço que, por design, prioriza a privacidade do agressor em detrimento da segurança do vulnerável.

4.2 Privacidade versus Segurança Pública

O grande desafio jurídico ao analisar a responsabilidade civil do Discord, reside no conflito direto entre direitos fundamentais protegidos pela Constituição Federal de 1988 que, embora aparentem exclusão mútua, devem coexistir de forma harmonizada. De um lado, encontram-se a Privacidade e a Intimidade (Art. 5º, X, CF), que garantem ao cidadão o direito de não ser vigiado em suas comunicações particulares, assegurando um espaço de liberdade individual livre de ingerências estatais ou privadas. Do outro lado, situam-se a Segurança Pública (Art. 144, CF) e a Dignidade da Pessoa Humana (Art. 1º, III, CF), que impõem ao Estado e a toda a sociedade o dever inarredável de proteger as pessoas contra crimes, abusos e graves violações de direitos.

Muitas vezes, o conceito de privacidade no mundo digital é interpretado de forma equivocada como um "escudo absoluto", capaz de impedir qualquer tipo de controle ou fiscalização. Entretanto, é princípio basilar do Direito brasileiro que nenhum direito fundamental possui caráter ilimitado ou absoluto. Conforme a teoria de Robert Alexy (2025), os direitos fundamentais são "mandados de otimização", caracterizados por serem normas que exigem que algo seja realizado na maior medida possível, diante das possibilidades jurídicas e fáticas.

No cenário das redes sociais fragmentadas, o ponto onde começa o direito do criminoso de se esconder, marca o exato limite onde termina o direito da vítima de ser protegida. Quando um servidor privado no Discord deixa de ser um espaço de convivência social e passa a ser utilizado para o planejamento de crimes graves como ataques a instituições de ensino, abusos sexuais ou esquemas de fraude financeira, o direito à privacidade deve ceder espaço ao interesse coletivo. A intimidade serve para resguardar a vida pessoal do cidadão e não para constituir uma zona de impunidade hermética onde a lei é incapaz de penetrar.

Para a resolução desse impasse, o ordenamento jurídico utiliza o Princípio da Proporcionalidade ou da Ponderação de Bens. Segundo a doutrina de Paulo Bonavides (2016), a proporcionalidade exige que o aplicador do Direito analise, no caso concreto, três subelementos: a adequação, a necessidade e a proporcionalidade em sentido estrito.

No contexto dos crimes contra a vida ou que vitimam crianças e adolescentes, a segurança coletiva e a integridade física possuem peso jurídico superior à privacidade de quem utiliza a rede para fins ilícitos. A solução jurídica, portanto, não demanda uma vigilância totalitária ou o fim da criptografia, o que seria um retrocesso democrático, mas exige que as plataformas digitais sejam colaborativas e diligentes na gestão de seus riscos sistêmicos.

A autonomia da vontade do usuário, que se apresenta como a primeira barreira de proteção no ambiente virtual, não pode ser exercida de modo a anular o direito à vida de terceiros. Se a plataforma Discord fornece as ferramentas tecnológicas para a criação das comunidades fechadas e o uso de robôs de automação, ela assume, simultaneamente, o risco do empreendimento e o dever de oferecer mecanismos eficazes para que crimes sejam denunciados, interrompidos e punidos. A omissão da empresa sob o pretexto de "proteger a privacidade", acaba por incentivar o comportamento do "lobo digital", que encontra no silêncio da plataforma o ambiente ideal para atacar, ciente de que a invisibilidade algorítmica opera a seu favor.

Nesse sentido, a responsabilidade da empresa consiste em garantir um equilíbrio dinâmico: a privacidade dos usuários que utilizam o serviço para fins lícitos deve ser integralmente preservada, mas a plataforma deve deter o controle sobre sua própria infraestrutura para impedir que sua tecnologia se transforme em um esconderijo para práticas criminosas.

A jurisprudência brasileira, consolidada no julgamento dos Temas 987 e 533 da Repercussão Geral pelo Supremo Tribunal Federal em 2025, evoluiu para entender que a liberdade de expressão e a privacidade não são salvo-condutos para a destruição da segurança pública. O STF estabeleceu que, em casos de violação a direitos de crianças e adolescentes ou risco iminente à vida, a responsabilidade da plataforma pode ser configurada mesmo sem ordem judicial prévia, caso haja inércia após denúncia interna ou conhecimento do risco sistêmico.

Reforçando este entendimento, o advento da Lei nº 15.211/2025 (Estatuto Digital) e os novos regulamentos de transparência (DSA), impõem ao Discord a obrigação de realizar avaliações periódicas de risco. A plataforma, portanto, ao gerir esse ecossistema virtual, assume o dever jurídico de assegurar que a ordem e a lei sejam respeitadas dentro de seus limites digitais. A falha no dever de cuidado, ao permitir que servidores se tornem centros de radicalização ou exploração sem qualquer intervenção técnica, desvirtua a função social do contrato do serviço digital, atraindo a responsabilidade civil objetiva por danos decorrentes de um serviço defeituoso em sua segurança.

4.3 A Cultura da Impunidade e a Fragilidade da Denúncia

A eficácia do sistema jurídico no ambiente digital é frequentemente comprometida pela complexidade das normas de competência e pela morosidade das respostas institucionais, criando um cenário de desamparo para as vítimas. A investigação dos crimes ocorridos em plataformas de comunicação de alta complexidade, como o Discord, enfrenta, inicialmente, o desafio da atribuição investigativa. De acordo com o rol estabelecido pelo Art. 144, § 1º da Constituição Federal e pela Lei nº 10.446/2002, a Polícia Federal detém competência para apurar infrações com repercussão interestadual ou internacional que exijam repressão uniforme.

Isso inclui conteúdos que difundam misoginia, neonazismo ou graves violações dos direitos humanos, crimes que, pela natureza transfronteiriça da internet, raramente se limitam a uma única jurisdição estadual. Sob a perspectiva da criminologia cibernética, Spencer Toth Sydow (2020) ressalta que essa dispersão geográfica impõe severos obstáculos à colheita inicial de provas, uma vez que o conflito de atribuições entre órgãos federais e estaduais atrasa as primeiras diligências, permitindo que a atividade ilícita continue se expandindo no ambiente de rede sem barreiras geográficas imediatas.

Todavia, a fragmentação entre as esferas de atuação da Polícia Federal e da Polícia Civil estadual cria um verdadeiro labirinto burocrático para o usuário leigo. Quando a comunicação de um crime carece de elementos mínimos de autoria ou é direcionada a um órgão sem atribuição específica, o processo investigativo sofre atrasos significativos, muitas vezes resultando no arquivamento prematuro de

notícia-crime. Essa realidade é severamente agravada pela arquitetura do Discord, onde o uso extensivo de pseudônimos e a transitoriedade volátil dos dados, que podem ser deletados instantaneamente por administradores dos servidores ou pelos próprios autores, tornam a denúncia um mecanismo lento.

Sem a preservação imediata dos metadados, a denúncia torna-se ineficaz para a instauração de inquéritos policiais capazes de identificar o infrator na "vida real". Dados institucionais da SaferNet Brasil (2024) demonstram que uma parcela expressiva das denúncias de crimes virtuais naufraga justamente nessa etapa, pois a volatilidade técnica da rede choca-se com as exigências formais do processo penal, gerando um vácuo probatório decorrente da quebra precoce da cadeia de custódia das evidências digitais.

Nesse cenário, a denominada "Cultura da Impunidade" floresce não apenas pela audácia do infrator, mas pela falha de segurança sistêmica e pela resistência colaborativa da plataforma. Ao delegar a responsabilidade da denúncia quase exclusivamente ao usuário, muitas vezes uma criança ou adolescente sem instrução técnica sobre preservação de provas, sem oferecer ferramentas nativas que garantam a custódia de evidências digitais (como logs de acesso, IDs de usuário imutáveis e registros de IP), o Discord falha no seu dever de cooperação.

De acordo com o entendimento firmado pelo STF nos Temas 987 e 533 (2025), a responsabilidade civil das plataformas deve ser analisada sob a ótica do "dever de cuidado". Se a empresa lucra com a interface que permite o anonimato e a destruição rápida de provas, ela não pode eximir-se das consequências quando essa mesma arquitetura é utilizada como ferramenta para o cometimento de ilícitos. Conforme adverte Patrícia Peck (2021), essa transferência do ônus regulatório e probatório para o elo mais vulnerável da relação jurídica viola o princípio da boa-fé objetiva, visto que a hipossuficiência técnica do internauta o impede de produzir os registros exigidos pelas autoridades, perpetuando o anonimato radical no ambiente virtual.

A fragilidade da denúncia também se manifesta na ausência dos canais de resposta em tempo real. Enquanto o crime ocorre em "tempo de rede", a resposta institucional muitas vezes segue o "tempo do papel". A Lei nº 15.211/2025 (Estatuto Digital) buscou mitigar essa lacuna ao impor obrigações de transparência e canais de denúncia prioritários para casos envolvendo menores. Contudo, o Discord, ao

manter uma estrutura de moderação que prioriza a autonomia dos servidores privados em detrimento da fiscalização centralizada, cria zonas do "não-direito".

A responsabilidade civil, portanto, fundamenta-se na teoria do risco-proveito: o fornecedor do serviço deve oferecer uma engenharia que facilite, e não dificulte, a ação das autoridades. Essa descentralização radical do ecossistema da plataforma, frequentemente defendida pela empresa sob o pretexto de proteção à privacidade, atua na prática como um escudo corporativo que retarda o cumprimento de ordens de identificação, submetendo a proteção da dignidade infantojuvenil a escolhas de design tecnológico focadas puramente no engajamento comercial.

Desta forma, a omissão da plataforma em colaborar de forma célere e proativa com as requisições policiais, ou a manutenção de um sistema que permite a remoção das evidências sem rastros técnicos, configura um defeito na prestação do serviço, conforme o Art. 14 do Código de Defesa do Consumidor. A impunidade digital deixa de ser uma falha do Estado para ser uma externalidade negativa gerada pelo modelo de negócio da plataforma.

Diante disso, Tarcísio Teixeira (2023) aponta que o dever de indenizar deve operar também como um mecanismo de desincentivo econômico, forçando a readequação de condutas comerciais nocivas no mercado de consumo tecnológico. Portanto, a reparação civil torna-se o instrumento necessário não apenas para compensar a vítima individual, mas para aplicar a função pedagógica do dano moral coletivo, compelindo a plataforma a adotar padrões de segurança e cooperação sistêmica que garantam que o ambiente virtual não se torne um refúgio imune à jurisdição estatal e à proteção integral dos direitos fundamentais.

5 ARTIGO 19 DO MARCO CIVIL DA INTERNET E A TESE DA INCONSTITUCIONALIDADE PARCIAL

5.1 O Regime de Responsabilidade Passiva Original (2014-2025)

Desde a promulgação da Lei nº 12.965/2014, o Brasil consolidou um modelo de responsabilidade civil para provedores de aplicações da internet pautado na intervenção judicial prévia. O Artigo 19 do Marco Civil da Internet (MCI), estabeleceu que o provedor só seria civilmente responsável por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomasse providências para tornar o conteúdo indisponível.

Este modelo, inspirado no *safe harbor* norte-americano (Seção 230 da CDA), visava proteger a liberdade de expressão e evitar a censura privada colateral, desonerando as empresas de um monitoramento editorial preventivo. Todavia, a doutrina contemporânea e a jurisprudência recente do Supremo Tribunal Federal (Temas 533 e 987) passaram a questionar a constitucionalidade dessa "isenção quase absoluta", especialmente quando confrontada com direitos da personalidade e da dignidade humana.

A estrutura do Artigo 19 criou o que juristas denominam "vácuo normativo". Enquanto o sistema exigia o tempo institucional de um processo judicial para a remoção de um conteúdo, a dinâmica algorítmica das redes como o Discord, permitia que danos irreparáveis como o vazamento de dados de menores ou a apologia ao crime se propagassem em milissegundos. Até meados de 2025, o sistema jurídico brasileiro operava sob uma passividade institucionalizada que se provou anacrônica diante da desinformação automatizada e do uso da Inteligência Artificial para a criação de conteúdos ilícitos.

O ponto de ruptura desse modelo ocorreu com a percepção de que a "neutralidade da rede" não poderia significar "neutralidade perante o ilícito". Conforme previsto no Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025), a responsabilidade das plataformas foi elevada ao status de "dever de cuidado" (*duty of care*), mitigando a regra do Artigo 19 quando o risco envolve vulneráveis. Compreende-se que a liberdade tecnológica não é um direito absoluto, devendo ser ponderada pelo princípio da proporcionalidade (Alexy, 2002), sob pena de converter o ambiente digital em um território de imunidade para a barbárie.

5.2 O Julgamento dos Temas 533 e 987: A Virada de Paradigma no STF

Em 26 de junho de 2025, o Supremo Tribunal Federal (STF), ao julgar os RE 1.037.396 (Tema 987) e RE 1.057.258 (Tema 533), sob a relatoria dos ministros Dias Toffoli e Luiz Fux, alterou definitivamente o cenário da responsabilidade civil digital no Brasil. Por maioria de 8 a 3 votos, a Corte declarou a inconstitucionalidade parcial e progressiva do Artigo 19 do Marco Civil da Internet (MCI).

A tese firmada, estabelece que o Artigo 19 continua em vigor apenas para conteúdos relacionados a crimes contra a honra (calúnia, injúria e difamação), onde a remoção ainda depende da ordem judicial para preservar o debate público e evitar o "efeito resfriador" (*chilling effect*). Entretanto, para conteúdos ilícitos graves como pornografia infantil, incitação ao terrorismo, racismo e automutilação, o STF incorporou o modelo de *notice and take down* (notificação e retirada), exigindo que os provedores ajam com diligência técnica e em prazo razoável após serem notificados extrajudicialmente pelo usuário, sob pena de responsabilidade civil direta.

Essa decisão rompe com a passividade original do "Estado de espera judicial" e impõe às plataformas, como o Discord, deveres de cuidados proativos (*duty of care*). Na prática, o STF reconheceu que o modelo de 2014 tornou-se um salvo-conduto para a inércia empresarial. No caso do Discord, onde a moderação é frequentemente descentralizada em servidores privados, a virada de paradigma entende-se que a empresa não pode mais ignorar denúncias de usuários sob o pretexto de aguardar uma citação judicial. Se o conteúdo é manifestamente ilegal e agride a segurança de vulneráveis, o risco da demora é transferido da vítima para a plataforma, que detém a capacidade técnica de estancar o dano.

Além disso, o julgamento enfatizou a aplicação do Princípio da Prevenção. Ao declarar a inconstitucionalidade parcial, o STF sinalizou que a imunidade garantida pelo Artigo 19 não alcança o lucro sobre o ilícito. Para o Discord, isso implica que, se o sistema de assinaturas (Nitro) ou a infraestrutura da plataforma facilitam a manutenção de comunidades voltadas à exploração de menores, a responsabilidade deixa de ser subsidiária para tornar-se solidária e objetiva, independentemente da provocação do Poder Judiciário.

5.3 A Configuração da Falha Sistêmica e a Natureza Híbrida do Discord frente à Jurisprudência do STF

O ponto mais inovador da decisão do STF, com aplicação direta à problemática do Discord, é o conceito da falha sistêmica. Conforme fixado na tese de repercussão geral (Temas 533 e 987), a responsabilidade das plataformas não advém apenas da presença de um conteúdo ilícito isolado, mas da omissão estrutural em adotar medidas adequadas de prevenção.

Considera-se configurada a falha sistêmica quando o provedor deixa de implementar níveis elevados de segurança para impedir a circulação massiva das condutas criminosas graves, como atos antidemocráticos, terrorismo e, de forma alarmante, o induzimento ao suicídio ou à automutilação (Art. 122 do CP), frequentes em comunidades de "autoajuda negativa".

Além disso, o dever de cuidado proativo abrange crimes de ódio e a disseminação da pornografia infantil, focos centrais das investigações recentes sobre o Discord no Brasil, como o inquérito da Polícia Civil de São Paulo em 2025.

Diferentemente da visão passiva de 2014, o entendimento atual, reforçado pela Lei nº 15.211/2025, determina que a responsabilidade é presumida quando a arquitetura da plataforma favorece ilícitos. No caso do Discord, essa falha se materializa na ineficácia dos canais de denúncia, na falta de moderação sobre redes de *bots* e na priorização da criptografia em detrimento da segurança de menores.

Essa mudança impõe o conceito de *Safety by Design* (Segurança por Design): se o Discord lucra com o engajamento e assinaturas (Nitro), ele assume o risco do empreendimento e deve demonstrar o "melhor esforço tecnológico" para barrar abusos, não podendo mais socorrer-se da "blindagem" irrestrita do Artigo 19 do MCI.

Nesse cenário, surge uma distinção técnica crucial estabelecida pelo STF quanto aos "provedores neutros". Para serviços como e-mails e mensageiros interpessoais (WhatsApp ou Signal), a Corte manteve o regime de dependência da ordem judicial, justificando que a ausência de moderação algorítmica e indexação pública limita o controle dessas empresas. Contudo, o Discord permanece em uma "zona cinzenta".

Embora ofereça comunicações privadas, sua arquitetura baseia-se em servidores que hospedam milhares de membros e utilizam ferramentas de

automação, aproximando-o muito mais de uma rede social de hospedagem do que de um simples mensageiro neutro.

A zona cinzenta é dissipada pela Teoria do Risco do Empreendimento: ao fornecer infraestrutura para comunidades herméticas dedicadas ao ilícito e lucrar com esse ecossistema, a plataforma deixa de ser um "conduíte neutro" para se tornar uma facilitadora de interações complexas.

Portanto, conforme consolidado na jurisprudência, o Discord deve ser submetido ao regime de responsabilidade por falha sistêmica. A proteção dos direitos fundamentais, em especial do público infantojuvenil, sobrepõe-se à imunidade técnica. O vácuo normativo anterior foi preenchido por uma interpretação que exige que a inovação caminha lado a lado com a segurança, impedindo que o ambiente privado se torne um esconderijo para a impunidade digital.

5.4 A Autonomia Individual e Contratual como Fronteiras no Direito Digital

A evolução jurídica do Artigo 19 do Marco Civil da Internet, revela o persistente dilema entre a segurança coletiva e a liberdade individual. Embora a imposição de um "dever de cuidado" às plataformas busque sanar falhas sistêmicas, essa regulação deve ser interpretada à luz da autonomia individual, sob o risco de conduzir ao que Étienne de La Boétie define como "servidão voluntária".

Entende-se que, a sujeição de um povo ocorre não apenas pela força, mas quando o indivíduo se habitua à obediência passiva e abdica de sua própria liberdade em troca de uma falsa sensação de proteção. No contexto digital, essa abdicção se materializa na autonomia contratual exercida pelas plataformas, onde ao aceitar termos de uso genéricos e invasivos, o usuário exerce sua autonomia individual para aderir a um contrato de adesão que, muitas vezes, limita sua própria esfera de direitos. Transforma-se o usuário, outrora cidadão digital, em um sujeito tutelado, que aceita a "tirania dos algoritmos" e as normas privadas de empresas como o Discord, em nome de uma segurança que ele mesmo já não se sente capaz de prover.

Essa estrutura de monitoramento remete ao conceito de "panoptismo", explorado por Michel Foucault em Vigiar e Punir. Para Foucault, o controle social é exercido por dispositivos de visibilidade que garantem uma vigilância constante e invisível. Todavia, no Direito Civil Contemporâneo, a autonomia contratual das

plataformas não pode ser absoluta nem soberana sobre os direitos fundamentais. Se a alegoria do "Anel de Gíges", de Platão, demonstra que o anonimato pode corromper a justiça, a resposta jurídica equilibrada não reside na vigilância totalitária, mas na função social do contrato e na responsabilidade objetiva das empresas por falhas em seus ecossistemas de segurança.

Portanto, a superação do impasse nas plataformas digitais exige a transição da heteronomia para a autonomia. Conforme Immanuel Kant discute em *Fundamentação da Metafísica dos Costumes*, a "heteronomia" configura-se quando a vontade é determinada por leis externas, enquanto a "autonomia" é a capacidade da razão de ser lei para si mesma. O ordenamento jurídico deve, pois, intervir no dirigismo contratual para garantir que a autonomia contratual das Big Techs não anule a autonomia individual dos usuários. Deve-se punir a negligência das plataformas especialmente em casos graves de omissão no Discord sem, contudo, despojar o cidadão da sua autodeterminação informativa.

Somente ao fomentar a autonomia e o uso crítico da tecnologia conforme preconiza a Lei nº 15.211/2025 é que o Direito servirá como instrumento de liberdade. Do contrário, corre-se o risco de trocar a insegurança da rede por uma "servidão voluntária" tecnocrática, onde o controle técnico e os contratos de adesão substituem a ética individual e a justiça social.

6 CONSIDERAÇÕES FINAIS

A presente pesquisa permitiu concluir que a responsabilização das plataformas digitais, com foco específico no ecossistema do Discord, atravessa um momento de profunda redefinição teórica e jurisprudencial no Brasil. O percurso investigativo demonstrou que o modelo da responsabilidade civil passiva, estabelecido pelo Artigo 19 do Marco Civil da Internet, tornou-se insuficiente para lidar com a complexidade e a velocidade dos crimes cibernéticos contemporâneos, especialmente aqueles que vitimam públicos vulneráveis em ambientes herméticos.

Um dos pontos centrais desta análise, foi o tensionamento entre a autonomia individual e a autonomia contratual. Evidenciou-se que a autonomia individual do usuário, ao optar pelo ingresso em plataformas digitais, não pode ser interpretada como uma renúncia tácita à sua segurança ou à proteção dos seus direitos fundamentais. Paralelamente, a autonomia contratual das plataformas manifestada em seus Termos de Serviço e na liberdade de configurar arquiteturas de privacidade não constitui um poder absoluto. No Estado Democrático de Direito, a liberdade de empresa e o direito de contratar, devem estar submetidos à função social do contrato e ao princípio da dignidade da pessoa humana.

A investigação revelou que o Discord, ao utilizar uma estrutura de servidores privados e delegação de moderação, criou uma "zona cinzenta" que, por anos, foi explorada para a prática de ilícitos sob o manto da imunidade técnica. Todavia, a virada de paradigma operada pelo Supremo Tribunal Federal em 2025, por meio dos Temas 533 e 987, dissipou essa obscuridade ao consolidar o conceito de falha sistêmica. A responsabilidade da plataforma, portanto, deixa de ser meramente reativa e passa a ser proativa (*duty of care*). A omissão estrutural e a priorização do lucro em detrimento da segurança, configuram uma falha no serviço que atrai a responsabilidade objetiva da empresa.

Em suma, a autonomia não pode ser convertida em uma ferramenta de "servidão voluntária" ou em um escudo para a impunidade. O equilíbrio buscado pelo ordenamento jurídico brasileiro, reforçado pela Lei nº 15.211/2025, exige que as plataformas assumam o risco da sua atividade econômica. Conclui-se que a segurança jurídica no ambiente digital só será plenamente alcançada, quando a inovação tecnológica for mediada por um dirigismo contratual que proteja o cidadão

contra a tirania dos algoritmos e a negligência corporativa. O Direito, portanto, deve agir não para anular a autonomia, mas para garantir que ela se exerça em um ambiente seguro, ético e, acima de tudo, constitucional.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução de Virgílio Afonso da Silva. 2. ed. São Paulo: Malheiros, 2011.

ANES, Franciso. **Origem da internet: saiba como tudo começou**. *Inforchannel*, 11 nov. 2022. Disponível em: <https://inforchannel.com.br/2022/11/11/origem-da-internet-saiba-como-tudo-comecou/>. Acesso em: 03 out. 2025.

BINICHESKI, Paulo Roberto. A responsabilidade civil dos provedores de internet no Brasil. In: BINICHESKI, Paulo Roberto. **Responsabilidade civil dos provedores de internet: Direito comparado e perspectivas de regulamentação no direito brasileiro**. Curitiba: Juruá, 2011. Cap. 3, p. 199.

BONAVIDES, Paulo. **O Princípio Constitucional da Proporcionalidade e a Proteção dos Direitos Fundamentais**. Revista de Direito Administrativo, Rio de Janeiro, 2016.

BRASIL. Conselho Nacional de Justiça. **Portaria nº 291, de 17 de dezembro de 2020**. Institui o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário. Brasília: CNJ, 2020. Disponível em: <https://www.cnj.jus.br>. Acesso em: 24 abr. 2026.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República. Subchefia para Assuntos Jurídicos, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 8 out. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 24 abr. 2026.

BRASIL. **Lei nº 15.211, de 17 de setembro de 2025**. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Brasília, DF: Presidência da República, 2025. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm. Acesso em: 24 abr. 2026.

BRASIL. Ministério da Justiça e Segurança Pública. **MJSP e Discord debatem sobre segurança na rede social e aperfeiçoamento da colaboração com investigações**. Brasília, DF: MJSP, 14 jul. 2023. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/mjsp-e-discord-debatem-sobre-seguranca-na-rede-social-e-aperfeicoamento-da-colaboracao-com-investigacoes>. Acesso em: 20 ago. 2025.

BRASIL. Supremo Tribunal Federal. **RE 1.037.396 (Tema 987) e 1.057.258 (Tema 533): Responsabilidade de plataformas digitais por conteúdo de terceiros.**

Brasília, DF: STF, 26 jun. 2025. Disponível em:

https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Informac807a7710a768So ciedadeArt19MCI_vRev.pdf. Acesso em: 12 jun. 2025.

BRASIL. Supremo Tribunal Federal. **Tema de Repercussão Geral 533 (RE**

1.057.258) e Tema 987 (RE 1.037.396). Relatores: Min. Luiz Fux e Min. Dias Toffoli. Julgado em 26 de junho de 2025. Disponível em: <https://portal.stf.jus.br>. Acesso em: 24 abr. 2026.

CARVALHO, Juliano Maurício de; ARITA, Carmem Harumi; NUNES, Alesse de Freitas. **A política de implantação da Internet no Brasil.** [S. l.: s. n.], 1999. p. 2-5. Disponível em:

<https://d1wqtxts1xzle7.cloudfront.net/31062004/5be0d57f5fde664d948d9c2cbc80b619-libre.pdf?1392121352=&response-content-disposition=inline%3B+filename%3DA_politica_de_implantacao_da_Internet_no.pdf..>. Acesso em: 15 jun. 2025.

CETIC.BR. **Pesquisa TIC Kids Online Brasil 2024: Resumo Executivo.** São Paulo: Comitê Gestor da Internet no Brasil, 2024. Disponível em: <https://cetic.br>. Acesso em: 24 abr. 2026.

CETIC.BR. **Pesquisa TIC Kids Online Brasil 2025: Resumo Executivo.** São Paulo: Comitê Gestor da Internet no Brasil, 2025. Disponível em: <https://cetic.br>. Acesso em: 24 abr. 2026.

CORREIO BRAZILIENSE. **Polícia Civil de São Paulo abre inquérito contra o Discord.** Publicado em 07 de abril de 2025. Disponível em:

<https://www.correiobraziliense.com.br/brasil/2025/04/7104170-policia-civil-de-sao-paulo-abre-inquerito-contr-o-discord.html>. Acesso em: 24 abr. 2026.

CRUZ, Daniel Silveira. **‘Painéis’ no Discord escondem as mais perversas formas de crime contra crianças, diz policial infiltrada.** G1, Rio de Janeiro, 27 jul. 2025. Disponível em: <https://g1.globo.com/tecnologia/noticia/2025/07/27/painels-no-discord-escondem-as-mais-perversas-formas-de-crime-contr-a-criancas-diz-policial-infiltrada.ghml>. Acesso em: 12 out. 2025.

DISCORD INC. **DSA Transparency Report (2025).** Relatório de Transparência em conformidade com o Digital Services Act da União Europeia. Fevereiro de 2026. Disponível em: <https://discord.com/safety/transparency-report>. Acesso em: 24 abr. 2026.

DISCORD INC. **EU Terrorist Content Online Regulation Transparency Report.** Março de 2026 (período de referência: jan-dez 2025). Disponível em: <https://discord.com/safety/transparency-report>. Acesso em: 24 abr. 2026.

DISCORD INC. **Política de Privacidade**. Atualizada em 29 de agosto de 2025. Disponível em: <https://discord.com/privacy>. Acesso em: 24 abr. 2026.

DISCORD. **Discord Supplier Code of Conduct**. [S. l.]: Discord, [s. d.]. Disponível em: <https://support.discord.com/hc/en-us/articles/20506201198103--Discord-Supplier-Code-of-Conduct>. Acesso em: 10 out. 2025.

DISCORD. **Guidelines**. Data de vigência: 29 set. 2025. Disponível em: <https://discord.com/guidelines>. Acesso em: 10 out. 2025.

ESTEFENON, Susana Graciela Bruno; EISENSTEIN, Evelyn; ABREU, Cristiano Nabuco de (Orgs.). **Vivendo esse Mundo Digital: Impactos na Saúde, na Educação e nos Comportamentos Sociais**. São Paulo: Artmed Editora, 2013.

FOUCAULT, Michel. *Vigiar e punir: nascimento da prisão*. Tradução de Raquel Ramallete. 27. ed. Petrópolis: Vozes, 1987. Disponível em: https://professor.pucgoias.edu.br/SiteDocente/admin/arquivosUpload/17637/material/Foucault_Vigiar%20e%20punir%20I%20e%20II.pdf. Acesso em: 03 dez. 2025.

FREITAS, Daniel Santana de. **A estrutura da plataforma Discord como impulsionadora do discurso de ódio digital**. Orientador: Naiara Ferreira Martins. 2025. **53 f.** Trabalho de Conclusão de Curso (Pós-Graduação em Direito Digital: Inovação e Tecnologia) – Instituto CEUB de Pesquisa e Desenvolvimento, Centro Universitário de Brasília, Brasília, 2025. Disponível em: <https://repositorio.uniceub.br/jspui/bitstream/prefix/17759/1/52300946.pdf>. Acesso em: 15 out. 2025.

GOULART, Luiz Carlos Shishito; CORDOVA, Maiko Giordani dos Santos. **Ciberdelitos: uma análise jurídica dos crimes digitais**. São Paulo: Dialética, 2024.

KANT, Immanuel. **Fundamentação da Metafísica dos Costumes**. Lisboa: Edições 70, 1960.

LA BOÉTIE, Étienne de. **Discurso sobre a servidão voluntária**. Tradução de J. Cretella Jr. e Agnes Cretella. São Paulo: RT, 2009.

LAGRASTA, Valeria Ferioli. **Nota sobre o Marco civil da Internet e a inconstitucionalidade do art. 19 da Lei 12.965/14**. Revista de Direito do Consumidor, São Paulo: Revista dos Tribunais, v. 32, n. 148, p. 43-62, jul./ago. 2023. Disponível em: <https://bd.tjdft.jus.br/items/539306b9-7c7e-4d9c-b7fd-2637c89c22cf>. Acesso em: 20 set. 2025

LIMA, Jean Cesar Antunes. **O Anel de Giges – Anonimato, responsabilidade e justiça**. Acrópole, 8 ago. 2020. Disponível em: <https://acropole.org.br/artigos/simbolismo/o-anel-de-giges-anonimato-responsabilidade-e-justica/>. Acesso em: 25 set. 2025.

MADALENA, Juliano. **Regulação das fronteiras da internet: um primeiro passo para uma teoria geral do direito digital**. Revista dos Tribunais, São Paulo, n. 974, dez. 2016. Disponível em: <https://dspace.almg.gov.br/handle/11037/23021>. Acesso em: 3 ago. 2025.

MARIZ, Felipe Medeiros. **A abertura dos bueiros da Internet: Neonazismo e plataformas digitais no Brasil entre os anos de 2018-2022**. 94 f. Dissertação (Mestrado em Direito) – Programa de Pós-Graduação em Direito, Universidade Federal Rural do Semi-Árido, Mossoró, 2022. Disponível em: <https://repositorio.ufersa.edu.br/server/api/core/bitstreams/ad64a235-56b7-42de-8f93-8a262b880235/content>. Acesso em: 26 set. 2025.

MINISTÉRIO PÚBLICO FEDERAL. **Atuação do Ministério Público Federal no Combate aos Crimes Cibernéticos**. Brasília: MPF, 2025. Disponível em: <https://www.mpf.mp.br>. Acesso em: 24 abr. 2026.

MOCELLIN, Caroline. A responsabilidade civil dos provedores por danos decorrentes de conteúdo gerado por terceiro no Marco civil da Internet. **Revista de Direito Privado**, São Paulo: Revista dos Tribunais, v. 18, n. 83, p. 15-42, nov. 2017. Disponível em: <https://www.lexml.gov.br/urn:urn:lex:br:redes.virtual.bibliotecas:artigo.revista:2017;1001156777>. Acesso em: 22 ago. 2025.

MORAES, Alexandre de. **Direito constitucional**. 38. ed. rev., atual. e ampl. São Paulo: Atlas, 2022.

NOVELINO, Marcelo. **Direito Constitucional**. 8. ed. Rio de Janeiro: Forense; São Paulo: Método, 2016.

OLIVEIRA, Daniel Calegar. **Direitos Fundamentais e a Era Digital: Limites no Exercício dos Direitos Fundamentais e sua Aplicação na Internet**. Trabalho de Conclusão de Curso (Bacharelado em Direito). Manhuaçu: UNIFACIG, 2023.

POR QUE o Discord se tornou tão popular para crimes cibernéticos. Ministério Público do Estado de Mato Grosso, 18 jul. 2025. Fonte: Metrôpoles. Disponível em: <https://www.mpmt.mp.br/portalcao/news/1217/162511/por-que-o-discord-se-tornou-tao-popular-para-crimes-ciberneticos>. Acesso em: 1 out. 2025.

SAFERNET BRASIL. **Meninas em Rede: guia para fortalecimento de redes de proteção e apoio contra a violência online**. Organizadora: Juliana Cunha. Salvador, 2020. Disponível em: <https://new.safernet.org.br>. Acesso em: 24 abr. 2026.

SANTANA, Bianca Quitéria de Moura. **A (in)constitucionalidade do artigo 19 do Marco Civil da Internet: uma análise à luz do RE nº 1.037.396/SP**, Tema 987 do STF. Revista Universitária Brasileira, Recife, v. 3, n. 2, p. 1-96, abr. 2025. Disponível em: <https://www.revistaub.com/index.php/RUB/article/view/151/115>. Acesso em: 16 set. 2025.

SARLET, Ingo Wolfgang; SIQUEIRA, Andressa de Bittencourt. **O STF e a inconstitucionalidade parcial e progressiva do artigo 19 do Marco Civil da Internet**. ConJur, 15 ago. 2025. Disponível em: <https://www.conjur.com.br/2025-ago-15/o-stf-e-a-inconstitucionalidade-parcial-e-progressiva-do-artigo-19-do-marco-civil-da-internet/>. Acesso em: 28 set. 2025.

SCOFIELD, Laura; AGÊNCIA PÚBLICA. **Discord desobedece as próprias regras e permite conteúdo violento e extremista**. Núcleo, 17 abr. 2023. Disponível em: <https://nucleo.jor.br/reportagem/2023-04-17-discord-desobedece-as-proprias-regras-e-permite-conteudo-violento-e-extremista/>. Acesso em: 30 ago. 2025.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (Brasil). Departamento de Governança para o Combate à Fraude Cibernética. **Marco Civil da Internet: 11 anos garantindo direitos e moldando o futuro digital do país**. Brasília, DF: Serpro, 23 abr. 2025. Publicado em: Agência Gov. Disponível em: <https://agenciagov.ebc.com.br/noticias/202504/marco-civil-da-internet-11-anos-garantindo-direitos-e-moldando-o-futuro-digital-do-pais>. Acesso em: 11 out. 2025.

SILVA, Daniel Neves. Internet. Brasil Escola. Disponível em: <https://brasilecola.uol.com.br/informatica/internet.htm>. Acesso em: 5 ago. 2025.
SILVA, Inimar Júnior Oliveira. **Cibercrime e os seus Reflexos no Ordenamento Jurídico Brasileiro**. Monografia (Bacharelado em Direito). Paracatu: Centro Universitário Atenas, 2018.

STHEL, Fernanda Gonçalves. **Do virtual ao real: as interações dos grupos de radicalização online com os ataques em escolas no Brasil**. 130 f. Dissertação (Mestrado em Sociologia Política) – Programa de Pós-Graduação em Sociologia Política, Universidade Estadual do Norte Fluminense Darcy Ribeiro, Campos dos Goytacazes, 2025. Disponível em: <https://uenf.br/posgraduacao/sociologia-politica/wp-content/uploads/sites/9/2025/05/Dissertacao-Fernanda-Goncalves-Sthel.pdf>

TAVARES, Vitor. **Por que o Discord tem sido terreno fértil na internet para crimes de extremismo?** BBC News Brasil, 17 abr. 2023. Disponível em: <https://www.bbc.com/portuguese/articles/ckg2gdkq375o>. Acesso em: 20 ago. 2025.