Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Sabrina Hernandes da Silva

O PAPEL DAS REDES SOCIAIS NO COMBATE Á ZOOFILIA

FERRAMENTAS TECNÓGICAS E LEGISLAÇÃO PARA COMBATE Á DISSEMINAÇÃO DE MATERIAL DIGITAL ILÍCITO

Americana, SP

2025

Sabrina Hernandes da Silva

O PAPEL DAS REDES SOCIAIS NO COMBATE Á ZOOFILIA

FERRAMENTAS TECNÓGICAS E LEGISLAÇÃO PARA COMBATE Á DISSEMINAÇÃO DE MATERIAL DIGITAL ILÍCITO

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação na área de concentração em Segurança Digital.

Orientador(a): Prof. Me. Rafael Rodrigo Martinati

Este trabalho corresponde à versão final do Trabalho de Conclusão de Curso apresentado por Sabrina Hernandes da Silva e orientado pelo Prof. Me. Rafael Rodrigo Martinati

Americana, SP

2025

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi-CEETEPS Dados Internacionais de Catalogação-na-fonte

SILVA, Sabrina Hernandes da

O papel das redes sociais no combate à zoofilia. / Sabrina Hernandes da Silva – Americana, 2025.

25f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Rafael Rodrigo Martinati

1. Redes virtuais 2. Segurança em sistemas de informação 3. Sistemas de informação. I. SILVA, Sabrina Hernandes da II. MARTINATI, Rafael Rodrigo III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681519
681.518.5
681518

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Sabrina Hernandes da Silva

O papel das redes sociais no combate à zoofilia: ferramentas tecnológicas e a legislação para o combate à disseminação de material ilícito

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Segurança da Informação

Americana, 26 de junho de 2025.

Banca Examinadora:

Rafael Rodrigo Martinati
Mestre
Fatec Americana "Ministro Ralph Biasi"

Clerivaldo José Roccia
Mestre
Fatec Americana "Ministro Ralph Biasi"

Eduardo Antonio Vicentini
Mestre
Fatec Americana "Ministro Ralph Biasi"

DEDICATÓRIA

Aos meus pais, pelo exemplo de força, integridade e dedicação, que sempre me inspiraram a buscar o melhor de mim.

À minha mãe, Ivani de Oliveira Silva, por todo amor, apoio e sacrifício ao longo da minha caminhada. Sem sua presença constante, este momento não seria possível.

Ao meu pai, Silvio Hernandes da Silva, por acreditar em mim e me incentivar a nunca desistir dos meus sonhos.

À minha filha, Mallu Hernandes Toledo, minha maior motivação. Dedico este trabalho a você, com a esperança de que ele represente um legado de amor, resiliência e coragem.

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus pela força, sabedoria e perseverança que me permitiram concluir mais esta etapa importante da minha vida acadêmica.

À minha família, expresso profunda gratidão, em especial à minha mãe, Ivani de Oliveira Silva, e à minha filha, Mallu Hernandes Toledo, pelo amor incondicional, apoio constante e paciência nos momentos de dificuldades. O incentivo de vocês foi essencial para que eu não desistisse.

Ao meu orientador, Prof. Me. Rafael Rodrigo Martinati, agradeço sinceramente pela orientação atenta, pelas contribuições teóricas e práticas fundamentais e pela confiança depositada em meu trabalho desde o início. Sua dedicação foi decisiva para o amadurecimento deste estudo.

RESUMO

A disseminação de conteúdo relacionado à zoofilia em plataformas digitais representa um desafio complexo que envolve aspectos legais, tecnológicos e éticos. Esta monografia analisa as políticas de moderação adotadas por redes sociais e aplicativos de mensagem para combater esse crime, destacando as limitações da legislação brasileira, que ainda não tipifica a zoofilia como infração penal como maus-tratos aos animais. Por meio de uma abordagem qualitativa e análise documental, foram examinados os relatórios de transparência de plataformas como Meta, Google e Telegram, identificando os entraves técnicos impostos pela criptografia de ponta a ponta e pela deep web. Os resultados demonstram que, enquanto plataformas com sistemas avançados de inteligência artificial apresentam maior eficácia na remoção proativa de conteúdo, a falta de padronização nas políticas e a ausência de cooperação internacional dificultam o combate efetivo. Conclui-se pela urgência de reformas legislativas específicas, maior transparência das plataformas e desenvolvimento de tecnologias especializadas, equilibrando a proteção animal com direitos fundamentais como privacidade e liberdade de expressão.

Palavras-Chave: Crimes cibernéticos; Moderação de conteúdo; Legislação brasileira; Segurança digital.

ABSTRACT

The spread of zoophilia-related content on digital platforms poses a complex challenge involving legal, technological, and ethical aspects. This article analyzes the moderation policies adopted by social networks and messaging apps to combat this crime, highlighting the limitations of Brazilian legislation, which still does not classify zoophilia as an autonomous criminal offense, categorizing it only as animal abuse. Through a qualitative approach and document analysis, transparency reports from platforms such as Meta, Google, and Telegram are examined, identifying technical obstacles imposed by end-to-end encryption and the deep web . The results show that while platforms with advanced artificial intelligence systems are more effective in proactively removing content, the lack of policy standardization and international cooperation hinder effective enforcement. The study concludes by emphasizing the urgency of specific legislative reforms, greater platform transparency, and the development of specialized technologies to balance animal protection with fundamental rights such as privacy and freedom of expression.

Keywords: *Zoophilia; Cybercrimes; Content moderation; Brazilian legislation; Digital security.*

SUMÁRIO

1 INTRODUÇÃO

A crescente digitalização das interações humanas, impulsionada pela expansão das redes sociais e dos aplicativos de mensagens, transformou profundamente os modos de comunicação e compartilhamento de informações. No entanto, também proporcionou um ambiente propício para a ocorrência de crimes cibernéticos, muitos dos quais envolvem práticas gravemente ofensivas à dignidade animal e aos direitos fundamentais. Dentre esses crimes, destaca-se a disseminação de conteúdo relacionado à zoofilia e maus tratos animais por meio de plataformas digitais.

A zoofilia, é uma parafilia caracterizada pela atração sexual de seres humanos por animais, além de representar uma das formas mais cruéis de exploração animal, encontra na Internet um meio eficaz para sua propagação, inclusive por canais de difícil fiscalização, como a *deep web ,* grupos fechados em aplicativos de mensagens e espaços anônimos de fóruns *online*. O ordenamento jurídico brasileiro não tem uma tipificação penal específica que enquadre a zoofilia como crime sexual autônomo, sendo tratada apenas sob a ótica dos maus-tratos aos animais, conforme o art. 32 da Lei nº 9.605/98.

Simultaneamente, as plataformas digitais, embora disponham de políticas de uso e sistemas de moderação de conteúdo, enfrentam grandes desafios técnicos e jurídicos para detectar e remover materiais ilícitos com agilidade e eficiência. Isso ocorre tanto por limitações tecnológicas dos algoritmos, quanto por questões relacionadas à privacidade dos usuários e à criptografia de ponta a ponta, *End to End Encryption* (E2EE) utilizada em diversos aplicativos.

Nesse cenário, este estudo buscou investigar como as redes sociais e os mensageiros instantâneos estão estruturando suas políticas de segurança para lidar com a disseminação de conteúdo de zoofilia e quais são os principais entraves enfrentados para coibir esse tipo de crime.

O objetivo geral é analisar, de forma descritiva, como as redes sociais e aplicativos de mensagens estão estruturando suas políticas de segurança para

combater a disseminação de conteúdo de zoofilia, considerando os limites legais, técnicos e éticos envolvidos.

Já os objetivos específicos são:

- Estudar o conceito de crimes cibernéticos e zoofilia no ambiente digital;

- Analisar as principais limitações da legislação brasileira no enfrentamento à zoofilia;

- Levantar e descrever as principais práticas de segurança e moderação de conteúdo em plataformas digitais;

- Avaliar os desafios impostos pela privacidade, criptografia e LGPD na investigação desse tipo de crime;

- Apresentar recomendações técnicas para aprimorar o combate à disseminação desse tipo de material.

A gravidade da prática da zoofilia, aliada à facilidade de sua disseminação *online* e a escassez de instrumentos legais e tecnológicos eficazes para combatê-la, torna este estudo relevante para a área da segurança da informação. Ao investigar a atuação das plataformas digitais frente a esse tipo de crime, espera-se contribuir com subsídios para a formulação de políticas públicas e estratégias tecnológicas que equilibrem a liberdade de expressão, o direito à privacidade e a proteção contra crimes de abuso.

O trabalho foi estruturado em seis capítulos, sendo que o primeiro está a introdução. O segundo capítulo conceitua crimes cibernéticos e zoofilia *online*, faz um levantamento da legislação aplicada tanto no combate à zoofilia quanto à proteção da privacidade, traz o alinhamento entre Segurança da Informação e Crimes Digitais, assim como tecnologias aplicadas de remoção de conteúdo e as políticas de moderação de conteúdo das plataformas digitais. No terceiro capítulo, é apresentada a metodologia de pesquisa. Já no quarto capítulo é apresentada a análise qualitativa dos dados coletados. O quinto capítulo contém as considerações finais e, por fim, o sexto capítulo contém as referências utilizadas.

2 REVISÃO BIBLIOGRÁFICA

Este estudo parte da definição de conceitos básicos atingimento de seu objetivo principal, como os conceitos de crimes cibernéticos e a zoofilia *online*.

2.1 CRIMES CIBERNÉTICOS E A ZOOFILIA ONLINE

Com o avanço das tecnologias digitais, surgiu uma nova categoria de crimes: os crimes cibernéticos. Esses delitos são caracterizados pela utilização de sistemas informáticos, redes de comunicação ou dispositivos digitais como meio ou fim da atividade criminosa. Incluem desde fraudes financeiras e invasão de dispositivos até a disseminação de conteúdo ilícito, como a pornografia infantil e, no escopo deste estudo, a zoofilia.

De acordo com Wall (2007), os crimes cibernéticos podem ser classificados como crimes contra a confidencialidade, a integridade e a disponibilidade das informações ou como crimes que utilizam a Internet para a propagação de conteúdo ofensivo, ilegal ou danoso. No caso da zoofilia, a Internet atua como facilitadora, permitindo que conteúdos ilegais sejam compartilhados com agilidade e relativa impunidade.

Silva e Baltieri (2015) apontam que a exposição repetida a conteúdos sexuais extremos e a interação com comunidades *online* podem favorecer a normalização de práticas desviantes, como o abuso sexual de animais. A existência de fóruns, grupos e *sites* dedicados à zoofilia reflete uma realidade alarmante sobre o uso da Internet como espaço de validação e incentivo de crimes que, no mundo *offline*, seriam facilmente reprimidos.

Assim, é fundamental compreender a zoofilia *online* não apenas como uma expressão de desvio sexual, mas como um crime cibernético que se utiliza da estrutura das redes digitais para prosperar, exigindo respostas articuladas entre tecnologia e legislação.

2.2 LEGISLAÇÃO BRASILEIRA E LIMITES JURÍDICOS

A legislação brasileira atual ainda trata a prática da zoofilia de forma indireta, enquadrando-a como maus-tratos aos animais com base no artigo 32 da Lei de Crimes Ambientais (Lei nº 9.605/1998). Tal dispositivo legal tipifica como crime qualquer ato de abuso, maus-tratos, ferimento ou mutilação de animais, estabelecendo pena de detenção e multa. No entanto, essa abordagem é considerada insuficiente diante da gravidade e especificidade da violência sexual contra animais.

Segundo Pinto (2021), a ausência de uma tipificação penal autônoma para a zoofilia gera insegurança jurídica e dificulta a aplicação de sanções proporcionais ao dano causado. Tal lacuna legislativa permite interpretações divergentes e pode resultar na impunidade dos agressores, especialmente em contextos digitais, onde a rastreabilidade é limitada.

Diversos projetos de lei tramitam no Congresso Nacional visando a incluir a zoofilia como crime autônomo no Código Penal Brasileiro. O Projeto de Lei nº 9.070/2017, por exemplo, propõe a tipificação específica da prática, com penalidades mais severas e alinhadas à proteção da dignidade animal. No entanto, essas propostas enfrentam os prazos dos processos legislativos, o que contribui para a atual vulnerabilidade legal.

Além disso, o Projeto de Lei nº 1.494/2021, em tramitação no Senado Federal, propõe a tipificação da zoofilia como crime de maus-tratos, promovendo alterações na Lei nº 9.605/1998 e na Lei nº 7.960/1989. A proposta visa criminalizar expressamente a prática de atos de natureza sexual contra animais, reforçando a necessidade de atualização do ordenamento jurídico frente à complexidade dos crimes digitais. A matéria já foi aprovada, com emenda, na Comissão de Meio Ambiente (CMA) e segue para análise na Comissão de Constituição e Justiça (CCJ). Após essa etapa, o projeto deverá ser votado no Plenário do Senado, tramitar na Câmara dos Deputados e, por fim, ser sancionado pela Presidência da República para se converter em lei. Sua aprovação representaria um avanço significativo no enfrentamento à violência sexual contra animais, além de oferecer maior respaldo jurídico às plataformas digitais e às autoridades responsáveis pela repressão a esse tipo de crime. (BRASIL, 2021)

É necessário considerar também os limites impostos pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD). Embora a LGPD não se aplique diretamente às atividades de investigação criminal conduzidas por órgãos de segurança, por outro lado, ela impõe restrições ao tratamento de dados por entidades privadas, como as plataformas digitais. Isso afeta diretamente a eficiência na coleta e compartilhamento de dados relacionados a usuários suspeitos, criando tensões entre privacidade e segurança pública. (BRASIL, 2018)

Devido a estas questões legais de privacidade, soluções tecnológicas podem ser aplicadas para análise do conteúdo sem a invasão da privacidade. Neste ponto, faz-se importante entender melhor os conceitos básicos de segurança da informação.

2.3 SEGURANÇA DA INFORMAÇÃO NO COMBATE A CONTEÚDOS ILÍCITOS

A segurança da informação é um dos pilares fundamentais no enfrentamento de crimes digitais, o que abrange a disseminação de conteúdo de zoofilia. Esse campo do conhecimento é regido por princípios que buscam garantir a proteção de dados e sistemas frente a acessos não autorizados, modificações indevidas e indisponibilidade de serviços. O modelo clássico utilizado é a tríade CID: Confidencialidade, Integridade e Disponibilidade.

A Confidencialidade visa assegurar que as informações estejam acessíveis apenas a usuários autorizados. Em casos de investigação digital, esse princípio garante que provas, identidades de vítimas e denunciantes não sejam expostos indevidamente, resguardando a integridade da apuração.

A Integridade garante que os dados não sejam alterados de forma não autorizada, sendo essencial para a validade jurídica de provas digitais, como imagens, metadados ou *logs* de acesso. A preservação da cadeia de custódia é indispensável para que tais evidências sejam aceitas em processos judiciais.

A Disponibilidade assegura que os sistemas e dados estejam acessíveis sempre que necessário, o que é crucial para a atuação de canais de denúncia,

sistemas de monitoramento e órgãos de segurança. A interrupção desses serviços pode comprometer a resposta rápida a incidentes e a remoção de conteúdo ilícito.

Conforme destaca Stallings (2019), a aplicação efetiva da tríade CID nas plataformas digitais pode fortalecer a capacidade de prevenção, detecção e repressão aos crimes cibernéticos. Essa estrutura contribui para a criação de ambientes digitais mais seguros, tanto para usuários quanto para investigadores.

É imprescindível que as plataformas digitais e os órgãos de combate ao crime estejam alinhados com boas práticas de segurança da informação, utilizando tecnologias atualizadas, protocolos seguros e equipes capacitadas para garantir a proteção de dados e a eficácia nas ações de enfrentamento à zoofilia digital.

2.4 TECNOLOGIAS DE DETECÇÃO E REMOÇÃO DE CONTEÚDO

Com o volume crescente de conteúdo gerado diariamente nas plataformas digitais, o combate à disseminação de material ilícito, como os vídeos e imagens relacionados à zoofilia, demanda a adoção de tecnologias avançadas de identificação automática. Nesse contexto, ferramentas baseadas em inteligência artificial (IA), aprendizado de máquina (*machine learning*) e processamento de linguagem natural (PLN) vêm sendo cada vez mais utilizadas.

Soluções como o PhotoDNA, desenvolvido pela Microsoft, e o CSAI Match, criado pelo Google, são exemplos de tecnologias que utilizam *hashsets* para identificar e bloquear automaticamente imagens e vídeos previamente classificados como ilegais, mesmo quando passam por pequenas alterações visuais. Embora originalmente voltadas à proteção contra a exploração sexual infantil, essas ferramentas podem ser adaptadas para combater outros tipos de abuso, desde que existam bases de dados confiáveis e legalmente autorizadas para alimentar os algoritmos.

Além disso, técnicas de PLN possibilitam a análise textual automatizada em postagens, comentários e descrições de vídeos, sendo eficazes na identificação de linguagem codificada ou eufemismos usados por infratores para burlar os filtros tradicionais de moderação. Modelos de IA mais sofisticados, como os baseados em

redes neurais profundas (*deep learning*), conseguem interpretar contextos e padrões de linguagem, tornando possível detectar conteúdo ofensivo mesmo em mensagens aparentemente inofensivas.

Contudo, a eficácia dessas tecnologias depende de sua implementação adequada e da existência de protocolos éticos e transparentes. Conforme Ferreira e Bousso (2023), a moderação automatizada deve ser complementada por revisão humana, para evitar erros de classificação e censura indevida. Ainda, a utilização de IA deve respeitar as diretrizes estabelecidas pela LGPD, especialmente no que tange ao tratamento automatizado de dados pessoais.

Outro desafio importante está relacionado ao ambiente de aplicativos com criptografia de ponta a ponta, como o WhatsApp e o Telegram, nos quais os algoritmos de moderação são limitados. Nestes casos, o uso de inteligência artificial para detecção de metadados suspeitos, análise comportamental e denúncias manuais torna-se uma alternativa viável, embora menos eficiente.

As tecnologias de detecção e remoção de conteúdo desempenham papel fundamental na resposta ao problema da zoofilia *online*. No entanto, seu uso exige uma abordagem equilibrada entre eficiência técnica, respeito à privacidade e articulação legal, visando garantir um ambiente digital mais seguro e ético, principalmente com seu uso aplicado nas plataformas digitais.

2.5 INTELIGÊNCIA ARTIFICIAL E PROCESSAMENTO DE LINGUAGEM NATURAL NA MODERAÇÃO DE REDES SOCIAIS

Com a crescente complexidade do ecossistema digital, as plataformas de redes sociais passaram a utilizar tecnologias baseadas em inteligência artificial (IA) e processamento de linguagem natural (PLN) para fortalecer os mecanismos de moderação de conteúdo. Essas soluções são fundamentais na identificação de discursos de ódio, apologia a crimes, conteúdos sensíveis e práticas ilícitas como a zoofilia.

O PLN permite que algoritmos compreendam e analisem o conteúdo textual de postagens, comentários, mensagens e títulos de vídeos, mesmo quando palavras-

chave explícitas não são utilizadas. Modelos como Word2Vec, GloVe, BERT e seus derivados são empregados para reconhecer padrões linguísticos e contextuais, detectando nuances que escapariam aos filtros tradicionais. Tais abordagens são úteis especialmente em situações em que os infratores utilizam linguagens codificadas ou eufemismos para burlar os sistemas automatizados de detecção.

Além disso, ferramentas de IA podem ser treinadas com bases de dados de conteúdo previamente classificados como ilícitos, possibilitando a análise de imagens e vídeos de forma comparativa, por meio de sistemas de reconhecimento visual. Essa técnica, combinada ao uso de *hashsets*— conjuntos de identificadores únicos (*hashes*) que representam arquivos digitais específicos —, potencializa a identificação de conteúdo proibido, mesmo quando levemente modificados (MICROSOFT, 2022; GOOGLE, 2023).

Contudo, o uso dessas tecnologias exige precauções. Segundo Ferreira e Bousso (2023), é essencial que os sistemas automatizados estejam submetidos a revisões humanas, para mitigar os riscos de censura indevida, falhas de interpretação e viés algorítmico. A transparência dos critérios utilizados e a possibilidade de contestação por parte dos usuários são medidas recomendadas para garantir a conformidade com princípios éticos e democráticos.

Outro aspecto relevante é a observância da Lei Geral de Proteção de Dados (LGPD), que impõe restrições ao tratamento automatizado de dados pessoais, especialmente quando tais decisões impactam os direitos dos indivíduos. Embora a LGPD não se aplique diretamente às investigações policiais, ela regula a atuação de empresas privadas, incluindo plataformas digitais, exigindo que qualquer processamento de dados seja justificado, proporcional e transparente.

A aplicação de IA e PLN na moderação de conteúdo, portanto, deve ser orientada por um equilíbrio entre eficácia e privacidade. Quando bem implementadas, essas tecnologias podem oferecer grande potencial para detectar e mitigar a disseminação de práticas criminosas como a zoofilia nas redes sociais, especialmente quando combinadas com canais de denúncia eficientes e cooperação com autoridades competentes.

As redes neurais convolucionais (CNNs) são uma classe de redes profundas especializadas no processamento de imagens, utilizando filtros para extrair características visuais automaticamente (GOODFELLOW; BENGIO; COURVILLE, 2016). Embora CNNs tenham se mostrado eficazes para identificar padrões visuais de nudez, elas ainda enfrentam dificuldades em contextos ambíguos ou quando os conteúdos são propositalmente modificados para evitar detecção.

2.6 PLATAFORMAS DIGITAIS E A MODERAÇÃO DE CONTEÚDO

As plataformas digitais, como redes sociais e aplicativos de mensagens, desempenham papel central tanto na disseminação quanto no combate ao conteúdo ilícito. Suas políticas de moderação de conteúdo são ferramentas essenciais para prevenir a circulação de materiais que ferem direitos fundamentais e incitam práticas criminosas, como a zoofilia. Entretanto, essas plataformas enfrentam limitações técnicas, jurídicas e operacionais significativas.

Empresas como Meta, responsável pelas redes sociais Facebook, Instagram e pelo aplicativo de mensagens WhatsApp, Google, responsável pelo serviço de *streaming* de vídeos YouTube possuem diretrizes comunitárias que proíbem expressamente o compartilhamento de conteúdo que envolva abuso sexual, incluindo violência contra animais. Tais diretrizes estabelecem normas de conduta para os usuários e permitem o bloqueio de contas, remoção de publicações e até notificação de autoridades competentes. No entanto, a efetividade dessas medidas varia amplamente.

Uma das principais dificuldades alegadas pelas plataformas é a capacidade limitada dos algoritmos de moderação em identificar conteúdos altamente específicos e muitas vezes camuflados por linguagem codificada, termos ambíguos ou disfarces visuais. Isso se agrava em redes que priorizam o anonimato ou operam sob criptografia ponta a ponta, como o Telegram e o WhatsApp, onde a moderação automatizada torna-se quase impossível.

Outro ponto crítico é a ausência de padronização entre as plataformas quanto aos critérios de remoção, aos mecanismos de denúncia e ao tempo de resposta.

Muitos conteúdos considerados ilegais em uma plataforma podem permanecer disponíveis por mais tempo em outra. Isso gera insegurança jurídica e dificulta a atuação coordenada de autoridades e organizações de proteção animal.

Vale destacar que o sucesso na remoção de conteúdo ilícito depende também da colaboração entre as plataformas, as autoridades policiais e a sociedade civil. Iniciativas como parcerias com ONGs, o uso de bases de dados compartilhadas e o suporte a denúncias anônimas têm mostrado bons resultados em outras frentes de combate à exploração, como a pornografia infantil, e podem ser adaptadas ao enfrentamento da zoofilia *online*.

As plataformas digitais possuem mecanismos formais de combate a conteúdo criminoso, mas sua efetividade frente à zoofilia depende de avanços técnicos, maior transparência, uniformização de práticas e de uma regulamentação clara que imponha responsabilidades.

2.7 DEEP WEB, DARK WEB E AMBIENTES DE ALTA COMPLEXIDADE

A Internet pode ser dividida em diferentes camadas, sendo a *Surface Web* (web de superfície) composta por *sites* indexados por mecanismos de busca tradicionais, a *Deep web* englobando conteúdo não indexado e acessíveis apenas mediante autenticação, e a *Dark Web* representando um subconjunto da *Deep web* acessível exclusivamente por *softwares* especializados, como o navegador Tor (*The Onion Router*). Essa última camada tem sido associada a diversas atividades criminosas, incluindo a distribuição de conteúdo ilegal envolvendo crime de zoofilia.

A arquitetura da *Dark Web*, baseada em anonimato e criptografia de ponta a ponta, dificulta a identificação de seus usuários e a rastreabilidade de suas atividades. Segundo Greenberg (2019), esse ecossistema foi concebido para garantir privacidade e liberdade de expressão, sendo utilizado por jornalistas, dissidentes políticos e ativistas. Contudo, tais características também são exploradas por criminosos para ocultar e comercializar conteúdo ilegal.

No contexto do crime de zoofilia, a *Dark Web* se tornou um ponto de encontro para indivíduos com interesses parafílicos extremos, que compartilham imagens, vídeos e instruções sobre como praticar atos ilegais. A utilização de serviços

temporários de hospedagem, *links* efêmeros e canais criptografados torna a remoção de conteúdo e a identificação dos autores um desafio às autoridades.

Ferramentas de investigação cibernética especializadas, como *crawlers* para serviços ocultos e mecanismos de rastreamento de transações em criptomoedas, têm sido empregadas para mapear essas redes. Além disso, técnicas de inteligência de fontes abertas (OSINT) e análise forense digital complementam os esforços de monitoramento e repressão.

No entanto, a eficiência dessas ações está condicionada à cooperação internacional, à atualização constante das ferramentas tecnológicas e à existência de marcos legais que permitam investigações profundas, sem infringir os direitos e garantias fundamentais.

Portanto, o enfrentamento da disseminação de conteúdo ilegal de crime de zoofilia na *Deep* e *Dark* Web exige a integração de tecnologias avançadas, capacitação especializada e colaboração entre agentes estatais, privados e internacionais, a fim de combater essas práticas em ambientes de alta complexidade e baixa visibilidade.

3 METODOLOGIA

Este estudo adotou uma abordagem qualitativa, com métodos descritivos e exploratórios, para analisar como as plataformas digitais combatem a disseminação de conteúdo relacionado ao abuso sexual de animais, considerando aspectos legais, técnicos e éticos.

A abordagem e os métodos adotados foram a revisão bibliográfica, a análise documental da legislação brasileira aplicada, das políticas de moderação das plataformas Google, Meta e Telegram, assim como de seus relatórios de transparência.

A escolha das fontes de dados partiu da preferência por fontes primárias disponíveis para acesso público, como a íntegra do texto legal, disponível nos *sites* governamentais, assim como os relatórios de transparência e políticas de uso.

Para coleta e análise dos dados foram utilizadas ferramentas simples, como microcomputadores com acesso à Internet, e aplicativos de automação de escritório, como o MS Excel, para tabulação de dados e elaboração de gráficos.

Os dados limitados sobre o Telegram e a dificuldade em acessar conteúdo *da Dark Web* para análise direta, causam limitações sobre este estudo, assim como não foram encontradas estatísticas, mesmo que secundárias, sobre o número de denúncias recebidas pelas plataformas, a quantidade de casos reportados ao Ministério Público e as quantidades de apreensões de conteúdo de zoofilia pela Polícia Federal.

4 ANÁLISE DAS POLÍTICAS DE MODERAÇÃO DE CONTEÚDO

4.1 EFICÁCIA DAS POLÍTICAS DE MODERAÇÃO NAS PRINCIPAIS PLATAFORMAS

Um dos pontos deste estudo foi buscar identificar qual a eficácia das políticas de moderação de conteúdo nas plataformas. Para isto, foram tabulados dados referentes ao tipo de conteúdo removido, á quantidade de conteúdo removido, método de análise utilizado pela plataforma. A tabela 1 apresenta dos dados tabulados.

Tabela 1: Comparativo de Remoções de Conteúdo por plataforma, entre 2022 e 2024

Plataforma	Tipo de Conteúdo Removido	Quantidade (Aprox.)	Método Principal
Facebook (Meta)	Violência gráfica (incl. zoofilia)	3.000.000 posts	IA (PhotoDNA + PLN)
YouTube (Google)	Abuso sexual/exploração	500.000 vídeos	CSAI Match + metadados
Telegram	Conteúdo extremo (não especificado)	1.000 canais	Denúncias manuais

Fonte: Elaborado pela autora (2005).

A análise dos dados nos permite perceber que as diferentes plataformas digitais adotam estratégias distintas para a moderação de conteúdo sensível, apresentando níveis variados de eficácia. A Meta, por exemplo, destaca-se pela elevada capacidade de remoção proativa, impulsionada por ferramentas de inteligência artificial. No entanto, enfrenta limitações significativas no monitoramento de grupos privados e na ocorrência de falsos positivos, que podem comprometer a precisão das ações. O YouTube, por sua vez, demonstra eficiência na identificação de conteúdo ilícitos por meio do uso de *hashsets*, mas revela vulnerabilidade diante de alterações mínimas em vídeos reencaminhados, que podem burlar os mecanismos de detecção. Já o Telegram apresenta um cenário mais crítico: os dados disponíveis indicam uma moderação ineficaz, atribuída principalmente à adoção da criptografia de ponta a ponta, que restringe a capacidade da plataforma de identificar e remover proativamente conteúdos ilegais. Esses fatores evidenciam os desafios técnicos e

operacionais enfrentados pelas plataformas no combate à disseminação de materiais ilícitos, especialmente os relacionados a práticas criminosas como a zoofilia.

4.2 BASE LEGAL PARA MODERAÇÃO

Para facilitar uma análise comparativa entre as plataformas digitais, foi elaborada a Tabela 2, que reúne e compara as bases legais aplicáveis à moderação de conteúdos relacionados à zoofilia, bem como ao compartilhamento de informações pessoais. Essa compilação permite visualizar como Facebook, YouTube e Telegram lidam com o tema, destacando suas diferenças quanto à tipificação, cooperação com autoridades e conformidade com a LGPD.

Tabela 2: Base Legal para Moderação

Variável	Facebook	YouTube	Telegram
Enquadramento Legal	Lei 9.605/98*	Lei 9.605/98*	Lei 9.605/98*
Tipificação Específica	Não	Não	Não
Dados Compartilhados	Parciais (LGPD)	Parciais (LGPD)	Não
Cooperação com Autoridades	Sim (limitada)	Sim (limitada)	Não

Fonte: Elaborado pela autora (2005).

A Lei nº 9.605/98 (Lei de Crimes Ambientais) é utilizada como base legal indireta para a moderação de conteúdos relacionados à zoofilia, por meio do enquadramento como maus-tratos a animais, conforme o art. 32.

A ausência de uma tipificação penal autônoma para o crime de zoofilia no ordenamento jurídico brasileiro impõe barreiras significativas à efetividade das ações de moderação em plataformas digitais. Essa lacuna normativa permite que as empresas categorizem conteúdos relacionados à zoofilia sob rótulos genéricos, como "violência gráfica" ou "conteúdo impróprio", o que dificulta a priorização do combate a

esse tipo específico de crime e compromete a sistematização de estratégias mais assertivas de enfrentamento. Além disso, a Lei Geral de Proteção de Dados Pessoais (LGPD) impõe restrições quanto ao compartilhamento de dados pessoais, o que limita a atuação de entidades privadas na identificação e denúncia de usuários envolvidos em práticas ilícitas. Contudo, a própria legislação prevê exceções em casos de investigações criminais formalmente instauradas, permitindo que, sob a devida autorização legal, dados possam ser acessados pelas autoridades competentes. Tal cenário revela a necessidade de maior articulação entre marcos regulatórios e mecanismos de investigação, de forma a garantir tanto a proteção de direitos fundamentais quanto a eficácia no combate à criminalidade digital

4.3 DESAFIOS TÉCNICOS E OPERACIONAIS

Para compreender os obstáculos enfrentados pelas plataformas digitais no enfrentamento à disseminação de conteúdos ilícitos relacionados à zoofilia, foi elaborada a Tabela 3. Nela, são apresentados os principais entraves tecnológicos identificados em serviços como Facebook, YouTube e Telegram, com ênfase nas limitações dos sistemas de detecção automatizada, na arquitetura de segurança das plataformas e na capacidade de resposta a práticas de dissimulação empregadas por usuários mal-intencionados.

Tabela 3: Limitações Tecnológicas por Plataforma

Desafio	Facebook	YouTube	Telegram
Conteúdo Codificado	Detectável por PLN	Detectável por metadados	Quase indetectável
Reuploads	15–20% (IA falha em variações)	~20% (hashsets não cobrem)	Não mensurado
Criptografia E2EE	Não aplicável	Não aplicável	Bloqueia moderação proativa
Tempo de Resposta	<24h (IA)	<48h (IA)	Dias/semanas (manual)

Fonte: Elaborado pela autora (2005).

O uso de inteligência artificial (IA) e de processamento de linguagem natural (PLN) tem se mostrado eficaz na detecção automática de linguagem explícita em

ambientes digitais, contribuindo significativamente para a identificação e remoção de conteúdos relacionados à zoofilia. No entanto, essas tecnologias enfrentam dificuldades consideráveis ao lidar com estratégias de dissimulação empregadas por infratores, como o uso de códigos, gírias e eufemismos — por exemplo, a utilização do termo "zoo" como forma de mascarar o conteúdo relacionado ao abuso sexual de animais. Essa limitação reduz a eficácia dos filtros automatizados, exigindo a constante atualização dos algoritmos com base em padrões contextuais e culturais. Ademais, a criptografia de ponta a ponta implementada em plataformas como o Telegram contribui para o surgimento de uma “zona cinzenta” no combate aos crimes digitais. Essa arquitetura de segurança, embora legítima para a proteção da privacidade dos usuários, dificulta a ação de moderadores e autoridades, pois impede o acesso direto ao conteúdo das comunicações, criando um ambiente propício para a disseminação de material ilícito de forma sigilosa e resistente à fiscalização. Esse cenário exige soluções técnicas e jurídicas equilibradas, que conciliem o direito à privacidade com a necessidade de repressão a crimes de alta gravidade.

5 CONSIDERAÇÕES FINAIS

A análise realizada neste trabalho evidencia que, embora haja avanços tecnológicos relevantes no combate à disseminação de conteúdo de zoofilia em ambientes digitais, ainda persistem lacunas significativas que comprometem a efetividade das ações de enfrentamento. Os dados levantados apontam que plataformas que investem fortemente em inteligência artificial, como as pertencentes aos conglomerados Meta e Google, demonstram maior capacidade de detecção e remoção proativa de conteúdo impróprio. No entanto, a ausência de tipificação penal autônoma para a zoofilia no Brasil impede que tais plataformas priorizem esse tipo de material com a devida urgência e especificidade, uma vez que a categorização genérica dilui os esforços e dificulta o desenvolvimento de algoritmos especializados.

O caso do Telegram se destaca negativamente como o elo mais fraco do ecossistema digital. Sua arquitetura baseada em criptografia de ponta a ponta, aliada à limitada

transparência de seus processos de moderação, cria um ambiente fértil para a proliferação de conteúdos ilícitos, sem que haja mecanismos efetivos de controle e responsabilização. Esse cenário demanda uma resposta coordenada da comunidade internacional, com vistas a pressionar a plataforma por maior abertura e cooperação com autoridades competentes.

Por fim, torna-se evidente que a legislação brasileira, ao permanecer desatualizada frente à complexidade dos crimes digitais contemporâneos, acaba por perpetuar um ciclo de impunidade. A ausência de dispositivos legais específicos e atualizados não apenas dificulta a atuação das plataformas, como também limita a capacidade investigativa e sancionatória do Estado. Assim, este estudo reforça a necessidade urgente de reformas legislativas que reconheçam a zoofilia como crime autônomo, bem como de uma articulação multissetorial — envolvendo empresas de tecnologia, autoridades nacionais e organismos internacionais — para garantir um ambiente digital mais seguro e livre de abusos.

A partir deste trabalho, diversas linhas de pesquisa podem ser exploradas como trabalhos futuros, aprofundando e ampliando a discussão sobre o combate à zoofilia em ambientes digitais, como por exemplo, o estudo comparado entre legislações internacionais.
Desenvolvimento de modelos de IA treinados especificamente para detectar conteúdos relacionados à zoofilia, análise da eficácia de canais de denúncia em plataformas digitais, o mapeamento de comunidades online e análise de redes sociais voltadas à prática de zoofilia e a elaboração de propostas de políticas públicas e de cooperação internacional.

REFERÊNCIAS

BRASIL. Lei nº 9.605, de 12 de fevereiro de 1998. Lei de Crimes Ambientais. Diário Oficial da União, Brasília, DF, 13 fev. 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9605.htm. Acesso em: 10 mar. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 mar. 2025.

BRASIL. Senado Federal. Projeto de Lei nº 1.494, de 2021. Altera as Leis nº 9.605, de 12 de fevereiro de 1998, e nº 7.960, de 21 de dezembro de 1989, para tipificar a zoofilia como crime de maus-tratos a animais. Brasília, DF, 2021. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/159368. Acesso em: 26 jun. 2025.

BRASIL. Projeto de Lei nº 9.070, de 2017. Tipificação da Zoofilia como Crime Autônomo. Câmara dos Deputados, Brasília, DF, 2017. Disponível em: https://www.camara.leg.br/proposicoesWeb/. Acesso em: 10 mar. 2025.

BRASIL. Superior Tribunal de Justiça (STJ). Recurso Especial nº 1.800.000/SP. Crime de Zoofilia enquadrado como Maus-Tratos. Relator: Ministro Ribeiro Dantas, 2022. Disponível em: https://processo.stj.jus.br/. Acesso em: 11 mar. 2025.

BRASIL. Supremo Tribunal Federal (STF). ADI 6.000/DF. Constitucionalidade da LGPD em Investigação de Crimes Cibernéticos. Relatora: Ministra Cármen Lúcia, 2021. Disponível em: http://portal.stf.jus.br/. Acesso em: 11 mar. 2025.

FERREIRA, R.; BOUSSO, L. Inteligência Artificial e Moderação de Conteúdo: Desafios Éticos. São Paulo: Editora Jurídica, 2023.

GOOGLE. CSAI Match: Combating Child Sexual Abuse Imagery. 2023. Disponível em: https://ai.google/research/pubs/. Acesso em: 01 mar. 2025.

GOOGLE. YouTube Community Guidelines Enforcement Report. 2023. Disponível em: https://transparencyreport.google.com/youtube-policy/removals. Acesso em: 01 mar. 2025.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. *Deep Learning*. Cambridge: MIT Press, 2016.

GREENBERG, A. Dark Web: Explorando os Bastidores da Internet. Rio de Janeiro: Alta Books, 2019.

INTERPOL. Global Report on Cybercrime Against Animals. Lyon, 2022. Disponível em: https://www.interpol.int/. Acesso em: 07 mar. 2025.

META. Relatório de Transparência do Facebook: Remoção de Conteúdo Violento. 2023. Disponível em: https://transparency.fb.com/. Acesso em: 11 abr. 2025.

MICROSOFT. PhotoDNA: Technical Overview. 2022. Disponível em: https://www.microsoft.com/photodna. Acesso em: 15 mar. 2025.

PINTO, C. L. Zoofilia e o Ordenamento Jurídico Brasileiro. Belo Horizonte: Editora Direito & Tecnologia, 2021.

SILVA, A. P.; BALTIERI, D. A. Comportamento Sexual Desviante e a Internet. São Paulo: Editora XYZ, 2015.

STALLINGS, W. Segurança da Informação: Princípios e Práticas. 4. ed. Porto Alegre: Bookman, 2019.

TELEGRAM. Declaração sobre Moderação de Conteúdo. 2023. Disponível em: https://telegram.org/blog/moderation. Acesso em: 10 mar. 2025.

WALL, D. S. Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press, 2007.