www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v. 30, n. 157, 2026 | DOI: 10.69849/326jq518

Brasil jogos virtuais e sociedade: perspectivas criminológicas

Brazil virtual games and society: criminological perspectives

Ryan Alves Andrade[1]
Pedro Henrique Oliveira[2]
Marina Teodoro[3]

Resumo

O presente estudo tem como tema a análise dos jogos virtuais como ecossistemas sociotécnicos e os riscos criminológicos associados a esses ambientes. O objetivo geral consiste em examinar a inserção dos jogos virtuais na sociedade sob uma perspectiva criminológica, avaliando as condições que favorecem a ocorrência de delitos e a eficácia das respostas do sistema penal brasileiro. Como objetivos específicos, busca-se: (i) analisar a evolução histórica dos jogos digitais e seu papel na construção de identidades na subcultura gamer; (ii) identificar oportunidades criminógenas e riscos psicossociais com base na Teoria das Atividades Rotineiras e na Prevenção Situacional do Crime; e (iii) avaliar a aplicabilidade da legislação penal brasileira e os limites da responsabilidade das plataformas digitais. O problema da pesquisa consiste em verificar se o ordenamento jurídico penal brasileiro é suficiente para enfrentar os crimes praticados em jogos virtuais ou se há necessidade de reformulação diante das particularidades das provas digitais e das novas oportunidades de delito. Conclui-se que os jogos virtuais ultrapassam o entretenimento, configurando-se como espaços relevantes de interação social, mas também propícios a práticas ilícitas. Embora o ordenamento jurídico brasileiro se mostre, em regra, adequado para o enfrentamento desses crimes, sua efetividade é limitada por desafios probatórios e pela complexidade da cooperação internacional. Assim, a proteção nesses ambientes demanda uma abordagem integrada, que combine a atuação penal com medidas preventivas das plataformas, educação digital e articulação entre setor público e privado, a fim de garantir segurança sem comprometer a natureza lúdica dos jogos.

Palavras-Chave: Criminologia; Crimes digitais; Jogos virtuais.

[1] Discente da Universidade Evangélica de Goiás Campus Ceres – Ceres- GO- Brasil
[2] Coautor Docente da Universidade Evangélica de Goiás Campus Ceres- Ceres- GO- Brasil, Email: Pedro.oliveira@docente.unievangelica.edu.br
[3] Coorientadora Docente da Universidade Evangélica de Goiás Campus Ceres- Ceres- GO- Brasil, Email: marina.teodoro@docente.unievangelica.edu.br

Abstract

The present study focuses on the analysis of virtual games as sociotechnical ecosystems and the criminological risks associated with these environments. The general objective is to examine the integration of virtual games into society from a criminological perspective, assessing the conditions that favor the occurrence of crimes and the effectiveness of the Brazilian criminal justice system's responses. The specific objectives are: (i) to analyze the historical evolution of digital games and their role in identity construction within the contemporary gamer subculture; (ii) to identify criminogenic opportunities and psychosocial risks based on the Routine Activities Theory and Situational Crime Prevention; and (iii) to evaluate the applicability of Brazilian criminal law and the limits of the liability of digital platforms. The research problem consists of determining whether the current Brazilian criminal legal framework is sufficient to address crimes committed in virtual gaming environments or whether reform is needed due to the particularities of digital evidence and new crime opportunities. It is concluded that virtual games go beyond mere entertainment, becoming important spaces for social interaction, while also being conducive to illicit practices. Although the Brazilian legal system is generally adequate to address such crimes, its effectiveness is limited by evidentiary challenges and the complexity of international cooperation. Therefore, effective protection in these environments requires an integrated approach that combines criminal enforcement with preventive measures by platforms, digital education, and coordination between the public and private sectors, in order to ensure safety without compromising the ludic nature of games.

Keywords: Criminology; Cybercrime; Virtual games.

1. Introdução

Os jogos virtuais, historicamente compreendidos como uma expressão cultural e simbólica inerente à humanidade, evoluíram de simples atividades lúdicas para complexos ecossistemas digitais de interação social e construção de identidade.

Com o avanço tecnológico iniciado na década de 1950 e a subsequente popularização dos consoles e da internet, tais práticas migraram para o espaço digital, consolidando no Brasil uma robusta subcultura gamer que transcende o entretenimento individual para refletir dinâmicas da vida real em ambientes hiperconectados.

Todavia, embora proporcionem autonomia e pertença, essa evolução tecnológica trouxe consigo desafios éticos e jurídicos significativos, uma vez que a mesma arquitetura que fomenta a convivência também expõe os utilizadores a riscos crescentes em um espaço social híbrido e complexo.

Nesse contexto, observa-se que os ambientes de jogos se tornaram espaços sociotécnicos propícios à manifestação de diversas práticas ilícitas, tais como fraudes patrimoniais, aliciamento (grooming) e comportamentos tóxicos, especialmente em virtude do anonimato relativo e da baixa responsabilização dos agentes.

Diante dessa realidade, o problema de pesquisa central deste estudo reside em verificar se o ordenamento jurídico penal brasileiro atual é suficiente para enfrentar os crimes praticados em ecossistemas de jogos virtuais ou se a volatilidade das provas digitais e as novas oportunidades situacionais de delito demandam uma reforma na dogmática e na regulação das plataformas.

Com o intuito de abordar tal problemática, este trabalho estabelece como objetivo geral analisar a inserção dos jogos virtuais na sociedade sob uma ótica criminológica, avaliando as condições que possibilitam o surgimento de riscos e a eficácia das respostas do sistema penal nacional

Para alcançar este propósito, definem-se três objetivos específicos: primeiramente, examinar a evolução histórica dos jogos digitais e a formação das funções sociais e identitárias na subcultura gamer contemporânea; em segundo lugar, identificar e descrever as principais oportunidades criminógenas e riscos psicossociais presentes nos ambientes virtuais à luz da Teoria das Atividades Rotineiras e da Prevenção Situacional do Crime; e, por fim, avaliar a aplicabilidade da legislação penal brasileira vigente e os limites da responsabilidade jurídica e deveres de cuidado das plataformas digitais frente aos delitos informáticos.

2. Jogos Virtuais E Sociedade: Perspectivas Criminológicas

Inicialmente, cumpre destacar que os jogos, mesmo antes do ambiente digital, constituem manifestação cultural inerente à experiência humana, presente desde as civilizações antigas. Conforme Huizinga (2019), o jogo configura-se como atividade cultural e espaço simbólico por meio do qual o indivíduo estabelece regras, representa papéis e experimenta liberdade dentro de limites voluntariamente aceitos, transcendendo a mera noção de lazer.

Com o avanço da eletrônica e da informática, os jogos migraram do espaço físico para o digital. Entre as décadas de 1950 e 1960, universidades norte-americanas desenvolveram simuladores digitais, como jogos de xadrez e batalhas espaciais. Já na década de 1970, consoles como o Atari foram introduzidos no mercado (Mota, 2023).

Na década de 1980, empresas como Nintendo e Sega consolidaram personagens e narrativas que redefiniram a cultura digital (Reis, 2021). Nos anos 1990, a expansão dos computadores pessoais e da internet possibilitou jogos em rede, transformando significativamente a experiência coletiva e o ecossistema dos jogos virtuais (Barauna, 2021).

No Brasil, o desenvolvimento dos jogos digitais acompanhou o avanço tecnológico, contribuindo para a formação de uma ampla comunidade gamer e consolidando o país como relevante polo cultural e criativo, impulsionado pela internet, jogos gratuitos e influência de

streamers (Cetic.br, 2024). Contudo, essa evolução também introduziu novos desafios de natureza ética, psicológica e jurídica.

Nesse contexto, os jogos virtuais configuram um espaço social híbrido, no qual elementos lúdicos e reais se interrelacionam, transformando formas de comunicação, competição e convivência (Huizinga, 2019; Barauna, 2021). Jogar, portanto, ultrapassa o entretenimento individual, constituindo meio de interação social, expressão identitária e reflexo da realidade (Castro, 2021).

Diante desse panorama, o presente capítulo analisa a inserção dos jogos virtuais na sociedade sob a perspectiva criminológica, abordando riscos, patologias, condições de surgimento, bem como oportunidades e desafios decorrentes da hiperconectividade.

2.1 Subculturas digitais e funções sociais dos jogos eletrônicos

Os jogos eletrônicos surgiram com finalidade primordial de entretenimento, proporcionando experiências imersivas em universos fictícios. No Brasil, esse processo teve início com o Telejogo, dispositivo da década de 1970 que oferecia modalidades como Paredão, Tênis e Futebol, antecedendo a chegada do Atari (Mota, 2023).

Os jogos online distinguem-se dos primeiros videogames ao possibilitarem interação global entre usuários, além da incorporação de itens colecionáveis e bens virtuais com valor econômico, comercializados em plataformas digitais (Cabral, 2022).

Atualmente, tais jogos transcendem o lazer, configurando-se também como espaços corporativos e de networking. Destacam-se os MMORPGs, nos quais há interação contínua em ambientes persistentes, possibilitando a formação de comunidades complexas (Barauna, 2021). Nesses ambientes, desenvolvem-se relações profissionais, parcerias comerciais e oportunidades de trabalho, sendo constantemente exercitadas habilidades como liderança, comunicação e cooperação (Barauna, 2021).

Além disso, esses espaços funcionam como redes sociais imersivas, permitindo intercâmbio de experiências, conhecimentos e contatos, ampliando conexões pessoais e profissionais (Barauna, 2021). Paralelamente, constituem ambientes de construção identitária e expressão cultural, possibilitando a experimentação de papéis e estilos de vida (Reis, 2021).

Segundo Castro (2021), o crescimento do número de jogadores no Brasil consolidou os jogos eletrônicos como uma subcultura própria, denominada subcultura gamer, impulsionada pela popularização dos videogames e pelo avanço tecnológico. Essa subcultura abrange comunidades online, eventos, competições e produção de conteúdo, influenciando diversos setores sociais, como música, moda e economia (Castro, 2021).

Conforme Huizinga (2019), o jogo perpassa múltiplas esferas da vida social, incluindo religião, arte e política, constituindo elemento fundamental da cultura. Melo (2024) complementa ao afirmar que práticas lúdicas antecedem a própria cultura interativa, sendo utilizadas historicamente como forma de entretenimento.

Nesse sentido, os jogos eletrônicos representam uma evolução dessas práticas, funcionando como espaços simbólicos de refúgio e controle, proporcionando sensação de autonomia ao jogador (Melo, 2024). Todavia, tais ambientes também apresentam riscos, como fraudes, assédio, cyberbullying e grooming, o que evidencia a necessidade de medidas preventivas e de conscientização (Bispo, 2024).

2.2 Da psicologia à criminalidade: compreendendo riscos nos jogos eletrônicos

A análise dos jogos eletrônicos demanda abordagem interdisciplinar, envolvendo psicologia, sociologia digital e criminologia. Do ponto de vista clínico, destaca-se a necessidade de diferenciar o uso intenso do transtorno por jogos eletrônicos (gaming disorder), incluído na CID- 11, caracterizado por perda de controle, priorização do jogo e continuidade apesar de prejuízos (WHO, 2020). Ressalta-se que tal diagnóstico é restrito a casos com prejuízo funcional, evitando a estigmatização do hábito de jogar.

No que tange à relação entre jogos violentos e comportamento agressivo, a literatura apresenta resultados divergentes. Estudo da Universidade de Oxford não identificou relação significativa (Przybylski; Weinstein, 2019), enquanto meta-análise prospectiva apontou associação positiva, ainda que modesta (Prescott; Sargent; Hull, 2018). Assim, a análise deve considerar fatores individuais, contextuais e estruturais (Drummond et al., 2020).

Em jogos competitivos online, o anonimato e a baixa responsabilização favorecem comportamentos tóxicos, como assédio e insultos, prejudicando a cooperação (Kwak; Blackburn, 2014/2015). Pesquisas recentes indicam a necessidade de medidas estruturais, como moderação automatizada e sistemas de reputação (Wijkstra et al., 2024; Frommel et al., 2024).

No campo psicossocial, o cyberbullying associa-se à ansiedade, depressão e isolamento, especialmente entre jovens (Mestre-Bach; Potenza et al., 2025). Fatores como competição intensa e normas permissivas ampliam esses riscos (Hu; Huang; Zhang, 2025).

Dados brasileiros indicam alta incidência de experiências ofensivas entre crianças e adolescentes, reforçando a necessidade de acompanhamento e educação digital (Cetic.br, 2024; 2025). Paralelamente, observa-se aumento de denúncias relacionadas à exploração sexual e deepfakes (SaferNet, 2025).

Nesse cenário, destacam-se três frentes criminológicas: (i) grooming, com criação de vínculos para exploração (Thorn, 2024/2025; EUROPOL, 2024); (ii) sistemas de monetização como loot boxes, associados a comportamentos de risco (Zendle; Cairns, 2019; Spicer et al., 2022); e (iii) fraudes e lavagem de dinheiro envolvendo bens virtuais (EUROPOL, 2024).

Diante disso, recomenda-se adoção de medidas como verificação etária, controles parentais, autenticação em dois fatores e sistemas antifraude (ITU/UNICEF, 2020). No plano normativo, observa-se tendência internacional de regulação baseada em avaliação de riscos e proteção de usuários, exemplificada pelo Online Safety Act (OFCOM, 2024/2025).

2.3 Análise criminológica dos riscos dos jogos digitais

A criminologia fornece arcabouço teórico para compreender a ocorrência de crimes em ambientes virtuais, destacando-se a Teoria das Atividades Rotineiras (TAR) e a Prevenção Situacional do Crime (PSC). A TAR estabelece que o crime ocorre quando há convergência entre ofensor motivado, alvo adequado e ausência de guardião eficaz (Cohen; Felson, 1979). Tal dinâmica é recorrente em jogos online, nos quais alvos incluem contas, itens virtuais e usuários (Yar, 2005; Caplan; Kennedy; Miller, 2011).

A PSC, por sua vez, propõe estratégias voltadas à redução de oportunidades criminosas, como aumento de esforço e riscos, redução de recompensas e eliminação de justificativas (Cornish; Clarke, 2003; Clarke, 1997; Pinheiro, 2025). Dentre as principais oportunidades criminógenas, destaca-se o anonimato associado à baixa responsabilização, que favorece práticas como assédio, doxing e swatting (Armini, 2025). Relatórios indicam aumento desses delitos e recomendam protocolos preventivos (DHS, 2024; FBI, 2008).

Outra frente refere-se a fraudes e invasões de contas (ATO), viabilizadas por técnicas como phishing e uso de bots, demandando medidas como autenticação multifator e monitoramento (EUROPOL, 2024; IMPERVA, s.d.). Soma-se que sistemas de monetização baseados em aleatoriedade apresentam riscos de aproximação com jogos de azar, especialmente entre jovens (Spicer et al., 2022; UKGC, 2024).

A exploração sexual infantil em ambientes digitais constitui preocupação central, com aumento de práticas de grooming e uso de tecnologias emergentes (EUROPOL, 2024), exigindo medidas de proteção como verificação etária e canais de denúncia (ITU/UNICEF, 2020).

No Brasil, o Marco Civil da Internet, a LGPD e o ECA estruturam a proteção de usuários, especialmente crianças e adolescentes (Brasil, 2014; 2018; 1990). Ademais, crimes financeiros podem ocorrer por meio da conversão de ativos virtuais, demandando aplicação de diretrizes internacionais (FATF, 2021; 2023; 2024). Nesse contexto, a prevenção deve basear-se em

governança de plataformas, segurança por design e educação digital, alinhando-se a padrões internacionais (OFCOM/Online Safety Act; ITU/UNICEF, 2020).

3. A Imputabilidade Penal No Ordenamento Jurídico Nacional

Com a consolidação dos jogos virtuais, práticas como fraudes, furtos de contas e golpes passaram a configurar crimes digitais, frequentemente transnacionais, exigindo cooperação internacional para investigação e responsabilização. Nesse contexto, destaca-se a Convenção de Budapeste (Decreto nº 11.491/2023), que fortalece o enfrentamento desses delitos.

A imputabilidade penal exige a verificação da responsabilidade do agente com base na culpabilidade, dolo e culpa. No Brasil, menores de 18 anos são inimputáveis (art. 27 do Código Penal), sendo submetidos às medidas do Estatuto da Criança e do Adolescente, o que é relevante diante da participação de jovens em jogos virtuais. O Código Penal, embora concebido em contexto analógico, permite o enquadramento de condutas digitais em tipos penais já existentes, como estelionato, furto mediante fraude, apropriação indébita e invasão de dispositivo informático.

A legislação especial tem sido atualizada, como na Lei 14.155/2021, que agravou penas para fraudes eletrônicas. O ambiente de jogos online apresenta fatores que favorecem crimes digitais, como alto volume de transações, assimetria informacional e lacunas regulatórias. A análise da responsabilidade penal também considera a dinâmica psicológica dos jogos, que pode aumentar a vulnerabilidade de determinados usuários, especialmente menores, sem afastar os princípios penais.

A responsabilidade por condutas ilícitas envolve o agente, o usuário e as plataformas digitais, que possuem deveres de segurança e cooperação. A responsabilização das plataformas é objeto de debate, especialmente quanto aos limites entre responsabilidade civil e penal. A imputação penal depende da comprovação de risco juridicamente proibido, eventual posição de garantidor e omissão penalmente relevante, observando os limites constitucionais da responsabilidade penal.

3.1 Crimes relacionados a jogos virtuais: tipificações no Código Penal e legislação especial

A expansão dos ambientes digitais possibilitou a prática de crimes cibernéticos a partir de qualquer jurisdição, com repercussão em diferentes países, inclusive no Brasil (Gomes; Medrado; Gama, 2024). Fraudes, extorsões e golpes patrimoniais passaram a ser executados por meio de

plataformas virtuais, exigindo adaptação do Direito Penal a condutas praticadas em ambiente desterritorializado, mas com efeitos concretos sobre bens jurídicos nacionais.

No plano da lei penal no espaço, o Código Penal adota a teoria da ubiquidade, considerando o crime praticado tanto no local da ação ou omissão quanto no local do resultado (art. 6º) (Brasil, 1940). Tal critério permite a incidência da lei penal brasileira em fraudes estruturadas em ambiente virtual transnacional, desde que o resultado ocorra em território nacional.

O principal desafio, nesse contexto, reside na definição de jurisdição e na necessidade de cooperação internacional para identificação de autores e obtenção de provas (Gomes; Medrado; Gama, 2024). Tais dificuldades são especialmente relevantes em jogos virtuais, nos quais servidores, plataformas e usuários frequentemente se distribuem por múltiplos países. Importa ressaltar que tais obstáculos não decorrem de insuficiência normativa, mas de limitações operacionais na investigação e na cooperação internacional (Gomes; Medrado; Gama, 2024).

A Lei 14.155/2021 promoveu alterações relevantes, aumentando penas e introduzindo qualificadoras para crimes como furto mediante fraude eletrônica e invasão de dispositivo informático (Brasil, 2021; Figueiredo, 2021). Ademais, disciplinou a competência territorial do estelionato eletrônico, fixando o foro no domicílio da vítima. Essa inovação facilita o acesso à Justiça em casos de golpes praticados em jogos virtuais, permitindo que a vítima acione o sistema judicial em sua localidade, ainda que o agente esteja em outra jurisdição (Figueiredo, 2021).

A jurisprudência do Superior Tribunal de Justiça consolidou esse entendimento, reconhecendo o domicílio da vítima como critério determinante de competência em casos de estelionato eletrônico (CC 181.726/PR; CC 178.697/PR). No plano material, condutas como golpes em jogos virtuais podem ser enquadradas no crime de estelionato (art. 171), ainda que envolvam moedas digitais ou itens virtuais com valor econômico (Costa, 2023). De igual modo, furtos de contas, apropriação de bens digitais e invasão de perfis podem configurar furto mediante fraude, apropriação indébita ou invasão de dispositivo informático, conforme o caso.

A proteção penal abrange bens digitais com valor econômico, demonstrando que o ambiente virtual não constitui espaço imune à incidência do Direito Penal (Costa, 2023). Precedentes do Superior Tribunal de Justiça, como o HC 351.013/BA, evidenciam que a invasão de dispositivos pode constituir meio executivo para crimes patrimoniais mais amplos, raciocínio aplicável a fraudes em contas de jogos e ativos digitais. Segundo Guilherme (2022), a estrutura de plataformas de jogos — com inventários digitais, carteiras eletrônicas e sistemas de negociação — favorece a prática de golpes, embora tais condutas possam ser adequadamente enquadradas nos tipos penais existentes.

No tocante às loot boxes, embora não se enquadrem formalmente como jogos de azar, sua regulação pode ocorrer por meio do Código de Defesa do Consumidor e do Estatuto da Criança e do Adolescente, especialmente quando direcionadas a públicos vulneráveis (Santos; Magalhães Filho, 2024). Assim, a resposta jurídica adequada não reside na expansão indiscriminada do Direito Penal, mas na aplicação criteriosa dos tipos existentes, em observância ao princípio da intervenção mínima.

3.2 Dolo, culpa e a conduta do jogador em crimes relacionados a jogos virtuais

A imputação penal no ambiente digital exige análise rigorosa do elemento subjetivo, especialmente do dolo, da culpa e do erro de tipo, distinguindo situações de atuação consciente daquelas marcadas por desconhecimento técnico. O dolo manifesta-se de forma evidente em condutas como invasão de contas, uso de malwares e fraudes em moedas digitais, sendo frequentemente demonstrado pelo modo de execução, repetição de condutas, uso de perfis falsos e ocultação de rastros (Silva, 2022).

Por outro lado, o uso inadvertido de ferramentas digitais pode configurar erro de tipo (art. 20, CP), afastando o dolo, desde que comprovada a ausência de compreensão sobre o funcionamento e o potencial lesivo do instrumento. Já o erro de proibição (art. 21, CP) recai sobre a ilicitude da conduta, não sendo escusável o desconhecimento da lei (Brasil, 1940).

Sustenta-se que o reconhecimento do erro de tipo digital deve ocorrer apenas quando houver dúvida concreta quanto à percepção do agente, considerando sua experiência e o contexto da conduta. O denominado “dolo digital” evidencia-se em situações de planejamento e uso consciente de ferramentas ilícitas (Costa, 2023). Em geral, crimes envolvendo itens virtuais, NFTs e moedas digitais apresentam dolo, caracterizado pela intenção de obtenção de vantagem ilícita mediante fraude (Guilherme, 2022).

A Lei 14.155/2021 reforça essa compreensão ao qualificar fraudes eletrônicas e aumentar penas, reconhecendo a maior potencialidade lesiva do meio digital (Figueiredo, 2021). Por outro lado, a vulnerabilidade do usuário, especialmente em razão de fatores psicológicos dos jogos, pode contribuir para a ocorrência do delito, sem, contudo, afastar a responsabilidade do agente (Ferreira; Sartes, 2018).

A imprudência da vítima não exclui o dolo do autor, embora possa ser considerada na análise da dinâmica causal e da previsibilidade do resultado (Comitê Gestor da Internet no Brasil; NIC.br, 2012). Assim, a imputação deve ser realizada caso a caso, considerando capacidade técnica, contexto e informações disponíveis, sem presunção automática de ilicitude ou exclusão de responsabilidade.

3.3 Responsabilidade jurídica das plataformas frente a crimes no ambiente digital

A responsabilidade das plataformas digitais deve ser analisada de forma diferenciada nos planos civil, regulatório e penal, evitando a conversão automática de deveres de cuidado em imputação criminal. As plataformas possuem deveres relevantes, como moderação de conteúdo, preservação de registros e cooperação com autoridades. O Supremo Tribunal Federal, ao interpretar o art. 19 do Marco Civil da Internet, estabeleceu parâmetros para responsabilização civil, sem instituir responsabilidade penal automática.

Eventuais falhas no cumprimento desses deveres geram, em regra, responsabilidade civil ou administrativa, sendo a responsabilização penal excepcional e condicionada à demonstração de requisitos específicos. No plano penal, a imputação exige a comprovação de posição de garantidor, omissão juridicamente relevante, possibilidade concreta de agir e nexo causal com o resultado (art. 13, § 2º, CP).

A atuação das plataformas também é relevante na preservação de provas digitais, como registros de acesso e transações, essenciais à persecução penal (Comitê Gestor da Internet no Brasil; NIC.br, 2012). Embora a arquitetura dos sistemas possa facilitar a prática de crimes, a responsabilização penal depende da demonstração de que a empresa criou ou incrementou risco juridicamente proibido.

Mecânicas como loot boxes podem gerar responsabilização civil ou regulatória, especialmente quando afetam públicos vulneráveis, mas não ensejam automaticamente responsabilidade penal. No ordenamento brasileiro, a responsabilidade penal da pessoa jurídica é restrita, exigindo análise da conduta de agentes individuais que tenham contribuído para o resultado ilícito. A dimensão transnacional impõe ainda deveres de cooperação por parte das plataformas, sem afastar o caráter excepcional da responsabilização penal.

4. Criminalidade E Jogos Digitais: Desafios E Respostas Do Sistema Penal

O debate contemporâneo oscila entre visões reducionistas que associam diretamente os jogos à criminalidade e perspectivas que os tratam como ambientes neutros. Ambas se mostram insuficientes. Impõe-se, portanto, uma análise fundada nas dinâmicas sociais, nas estruturas tecnológicas das plataformas e nas formas concretas de vitimização.

Condutas como furto de contas, chantagem, aliciamento de menores e perseguição produzem efeitos reais, inclusive de natureza patrimonial e psicológica. Nesse contexto, a análise desenvolve-se a partir de três eixos: (i) práticas ilícitas e seus impactos; (ii) dificuldades

probatórias em cenários transnacionais; e (iii) o papel do Estado na prevenção, regulação e proteção de usuários, bem como os deveres das plataformas digitais.

4.1 Crimes virtuais com repercussão no mundo real: casos paradigmáticos

Os jogos online devem ser compreendidos como ecossistemas digitais complexos, que integram múltiplas funcionalidades comunicacionais e interativas, tais como chats por texto e voz, interação entre usuários desconhecidos, transmissões em tempo real, perfis persistentes e circulação de bens virtuais. Tais elementos conferem a esses ambientes a natureza de espaços sociotécnicos de convivência, ampliando significativamente o potencial de interação social lícita.

Entretanto, essa mesma complexidade funcional e a elevada densidade de interações também favorecem a instrumentalização desses ambientes para a prática de ilícitos, como assédio, fraudes, perseguição (stalking) e exploração de indivíduos em situação de vulnerabilidade, especialmente crianças e adolescentes (OFCOM, 2025; UNICEF, 2025).

O debate público e jurídico frequentemente incorre em simplificações, ora atribuindo aos jogos relação causal direta com a criminalidade, ora qualificando-os como ambientes neutros. Todavia, análise tecnicamente adequada indica que o risco não reside no jogo em si, mas nas arquiteturas de interação, nas funcionalidades comunicacionais e nos mecanismos de sociabilidade digital disponibilizados pelas plataformas (UNICEF, 2025).

A UNICEF ressalta que jogos online não constituem, por si, causa de comportamentos violentos, mas reconhece que suas ferramentas podem ser utilizadas de forma abusiva, viabilizando dinâmicas de aproximação indevida, manipulação psicológica e aliciamento de menores, o que exige abordagem regulatória centrada na governança dessas interações (UNICEF, 2025).

Em linha semelhante, a OFCOM identifica que a multiplicidade de formas de contato entre usuários, como chats, lobbies e transmissões, pode ser explorada por ofensores, especialmente na ausência de mecanismos eficazes de moderação e proteção (OFCOM, 2025). Entre os casos paradigmáticos, destaca-se a sextorsão. Pesquisa da Thorn (2025) indica que 24% dos jovens entrevistados sofreram extorsão sexual antes dos 18 anos, com maior incidência entre jovens LGBTQIA+. Tais práticas geram impactos profundos, incluindo medo, isolamento, chantagem recorrente e prejuízos à vida escolar e familiar (Thorn, 2025; UNICEF, 2025).

Outro exemplo relevante refere-se ao uso de deepfakes sexuais. Levantamento da SaferNet Brasil identificou, em 2025, 16 casos em 10 estados, envolvendo 72 vítimas, evidenciando impactos diretos na reputação, saúde mental e convivência social (SaferNet Brasil,

2025). Esses casos demonstram que o ambiente digital não constitui esfera dissociada da realidade, mas reconfigura práticas tradicionais de violência, ampliando sua velocidade, alcance e permanência. A circulação de conteúdos manipulados, por exemplo, afeta diretamente bens jurídicos como honra, dignidade e integridade psíquica (SaferNet Brasil, 2025; UNICEF, 2025).

Dados da OFCOM indicam que quase metade dos adolescentes manifesta preocupação com trolling em jogos online, enquanto 45% relatam comportamentos abusivos e 37% mencionam práticas de griefing (OFCOM, 2025). O relatório Childhood in a Digital World aponta que experiências abusivas online apresentam associação significativa com ansiedade, autolesão e ideação suicida, ao passo que o tempo de tela, isoladamente, possui impacto reduzido (UNICEF, 2025).

No âmbito patrimonial, bens digitais como contas, skins e moedas virtuais adquiriram valor econômico relevante. O relatório IOCTA 2024 destaca a persistência de fraudes, phishing e engenharia social voltados à apropriação desses ativos (EUROPOL, 2024). A EUROPOL também indica que práticas como grooming e extorsão sexual frequentemente se iniciam em plataformas digitais, incluindo jogos, por meio de aproximação gradual e construção de confiança (EUROPOL, 2024; OFCOM, 2025).

Diante disso, tais condutas devem ser compreendidas como reconfigurações de práticas ilícitas já conhecidas, potencializadas por características próprias do ambiente digital, como anonimato relativo, escalabilidade e permanência dos registros (UNICEF, 2025; EUROPOL, 2024; Thorn, 2025).

4.2 Dificuldades probatórias e cooperação internacional na persecução penal

Embora a materialidade dos crimes digitais seja cada vez mais evidente, a produção probatória permanece como principal obstáculo à persecução penal. A prova digital caracteriza-se por volatilidade, dispersão e dependência de infraestrutura privada, permitindo rápida eliminação de vestígios e limitação temporal de registros (Council of Europe, 2025; EUROJUST, 2024).

Nos jogos online, tais dificuldades são ampliadas pela fragmentação das interações, que frequentemente se distribuem por múltiplas plataformas e serviços, como chats internos, aplicativos de voz, redes sociais e sistemas de pagamento, aumentando o risco de perda de evidências (EUROJUST, 2025; OFCOM, 2025). Assim, os entraves à persecução penal decorrem, em regra, não da insuficiência normativa, mas da assimetria entre a rapidez da prática delitiva e a capacidade institucional de resposta (EUROJUST, 2024).

A jurisprudência do Superior Tribunal de Justiça evidencia a adaptação do sistema jurídico a esse cenário. No CC 181.726/PR, firmou-se a competência do domicílio da vítima em

casos de estelionato eletrônico, reconhecendo as especificidades da criminalidade digital (STJ, 2021; Brasil, 2021). No RHC 123.424/MT, a Corte reafirmou a relevância penal da invasão de dispositivo informático, ao mesmo tempo em que exigiu fundamentação adequada para medidas cautelares (STJ, 2020). Já no RHC 76.324/DF, declarou ilícita a obtenção de dados sem autorização judicial, reforçando a necessidade de respeito às garantias fundamentais (STJ, 2017).

Esses precedentes demonstram que a persecução penal digital deve conciliar eficiência investigativa com observância rigorosa do devido processo legal e da legalidade probatória.

A internalização da Convenção de Budapeste (Decreto nº 11.491/2023) representa avanço significativo ao estabelecer mecanismos de cooperação internacional e preservação expedita de dados (Brasil, 2023; Council of Europe, 2025). O Segundo Protocolo Adicional e a Convenção da ONU sobre Cibercrime ampliam esses instrumentos, buscando superar a morosidade dos modelos tradicionais de cooperação (United Nations, 2025; EUROJUST, 2025). Ainda assim, a efetividade depende de adaptação institucional, capacitação técnica e padronização de procedimentos investigativos.

A prova digital exige rigor metodológico em todas as etapas, incluindo coleta, preservação e análise, sendo elementos como logs, metadados, IPs e registros financeiros essenciais à reconstrução fática (INTERPOL, 2019). Nesse contexto, as plataformas digitais desempenham papel central na preservação de evidências, sem que isso implique responsabilidade penal automática. A imputação depende da verificação de omissão penalmente relevante, posição de garantidor e criação de risco juridicamente proibido (STF, 2025; Brasil, 2023).

A teoria da imputação objetiva, conforme Roxin (2009), permite delimitar a responsabilidade penal com base na criação de riscos não permitidos e na proteção de bens jurídicos. Todavia, as dificuldades probatórias não se resolvem por expansão penal, mas por fortalecimento institucional, investimento técnico e aprimoramento da cooperação internacional (EUROJUST, 2025; INTERPOL, 2019).

4.3 O papel do Estado na prevenção de crimes relacionados a jogos digitais

A repressão penal, embora necessária, mostra-se insuficiente para enfrentar os riscos dos ecossistemas digitais, especialmente quando envolvem crianças e adolescentes. A prevenção assume, portanto, papel central (UNICEF, 2025; OFCOM, 2025). Essa prevenção deve ser orientada por evidências, evitando pânico moral e abordagens genéricas. Estudos indicam que experiências abusivas têm maior impacto do que o tempo de uso de tecnologia (UNICEF, 2025).

No Brasil, a prevenção exige integração entre educação digital, regulação de plataformas, fortalecimento investigativo e apoio às vítimas. A Política Nacional de Educação Digital (Lei nº 14.533/2023) constitui instrumento relevante ao promover a formação de usuários conscientes, capazes de identificar riscos e agir de forma segura (Brasil, 2023). Dados da TIC Kids Online Brasil evidenciam alta exposição de crianças e adolescentes a conteúdos comerciais e estratégias de persuasão digital, o que reforça a necessidade de proteção qualificada (CETIC.br, 2025).

A Lei nº 15.211/2025 (Estatuto Digital da Criança e do Adolescente) amplia a proteção ao estabelecer critérios aplicáveis a serviços digitais acessíveis ao público infantojuvenil, independentemente da localização do fornecedor (Brasil, 2025). A atuação estatal passa, assim, a incorporar o princípio da prevenção por design, exigindo que plataformas adotem medidas de proteção desde sua estrutura. Experiências internacionais, como as diretrizes da OFCOM, indicam a necessidade de avaliação de riscos e adoção de medidas proporcionais, incluindo mecanismos de denúncia, proteção de privacidade e controle de interações (OFCOM, 2025).

Contudo, a responsabilização penal das plataformas deve permanecer excepcional, condicionada à demonstração de dever jurídico específico, omissão relevante e contribuição para o risco. A prevenção também deve contemplar suporte às vítimas, incluindo assistência psicológica, orientação jurídica e canais acessíveis de denúncia (Thorn, 2025; UNICEF, 2025). Ademais, a natureza transnacional desses ambientes exige cooperação internacional e compartilhamento de boas práticas regulatórias (Council of Europe, 2025).

5. Metodologia

Este estudo adotou como metodologia a revisão bibliográfica de natureza qualitativa e caráter descritivo. Para a construção da pesquisa, foram utilizados artigos científicos, monografias de bacharelado, documentos institucionais e relatórios técnicos relacionados à temática dos jogos virtuais, cibercriminalidade e as implicações jurídicas no ordenamento brasileiro

As buscas foram realizadas em bases de dados como o Google Acadêmico, além de repositórios institucionais de universidades, sites oficiais de órgãos de inteligência e segurança (como Europol e SaferNet) e portais de jurisprudência do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ). Foram considerados trabalhos e dispositivos normativos publicados no período de 1940 a 2026, abrangendo desde a base da legislação penal clássica até relatórios de tendências e leis digitais recentes.

Como critérios de inclusão, elencaram-se aqueles disponíveis na íntegra, publicados em língua portuguesa ou inglesa e que abordassem diretamente a criminologia aplicada aos jogos

eletrônicos, a prevenção situacional de crimes digitais ou a responsabilidade jurídica das plataformas virtuais.

Como critérios de exclusão, foram desconsiderados resumos, publicações duplicadas nas bases de dados e estudos que não apresentavam relação direta com o objetivo da pesquisa ou que focavam exclusivamente em aspectos técnicos de programação sem relevância jurídica

6 Resultados e Discussão

A análise desenvolvida ao longo dos capítulos evidencia que os jogos digitais devem ser compreendidos como ambientes sociotécnicos complexos, nos quais se articulam dimensões culturais, econômicas e jurídicas.

Conforme apontado por Huizinga (2019), o jogo já constituía elemento estruturante da cultura, e sua transposição ao meio digital ampliou significativamente seu alcance social (Barauna, 2021; Castro, 2021). Nesse sentido, os resultados indicam que os jogos virtuais não se limitam ao entretenimento, mas funcionam como espaços de interação social, construção identitária e circulação de bens com valor econômico.

A consolidação da chamada subcultura gamer reforça essa compreensão, demonstrando que os jogos digitais reproduzem e transformam dinâmicas sociais existentes (Castro, 2021). Esse achado permite afastar tanto a visão determinista que associa jogos à criminalidade quanto a perspectiva de neutralidade absoluta, indicando que os riscos decorrem das formas de interação e

das estruturas das plataformas, e não do jogo em si (UNICEF, 2025; OFCOM, 2025).

Sob a ótica criminológica, a aplicação da Teoria das Atividades Rotineiras demonstrou que os ambientes de jogos online favorecem a convergência entre ofensores motivados, alvos acessíveis e ausência de controle eficaz, especialmente em contextos de anonimato e baixa responsabilização (Cohen; Felson, 1979; Yar, 2005). Paralelamente, a Prevenção Situacional do Crime evidencia que medidas como autenticação reforçada, moderação ativa e redução de oportunidades podem mitigar tais riscos (Clarke, 1997; Cornish; Clarke, 2003).

No plano psicossocial, os resultados confirmam que não há consenso científico sobre a relação direta entre jogos violentos e comportamento agressivo, sendo a influência mediada por fatores individuais e contextuais (Przybylski; Weinstein, 2019; Prescott; Sargent; Hull, 2018). Em contrapartida, há evidências consistentes de que experiências negativas em ambientes digitais, como cyberbullying e assédio, estão associadas a impactos relevantes na saúde mental,

especialmente entre jovens (Mestre-Bach; Potenza et al., 2025; UNICEF, 2025). Assim, o risco central não está no uso da tecnologia, mas na exposição a interações abusivas.

No âmbito jurídico-penal, os resultados demonstram que o ordenamento brasileiro possui instrumentos suficientes para o enfrentamento de crimes praticados em jogos virtuais. Condutas como fraude, invasão de contas e apropriação de bens digitais podem ser enquadradas em tipos penais já existentes, como estelionato e invasão de dispositivo informático (Costa, 2023; Brasil, 1940). A Lei nº 14.155/2021 reforça essa adequação ao atualizar e qualificar tais condutas no contexto digital (Figueiredo, 2021).

Nesse sentido, confirma-se que o desafio não reside na ausência de tipificação, mas na correta aplicação das normas existentes a novas formas de execução delitiva (Gomes; Medrado; Gama, 2024). A jurisprudência do Superior Tribunal de Justiça também evidencia essa adaptação interpretativa, especialmente quanto à competência territorial e à caracterização de crimes eletrônicos (STJ, 2021).

A análise da imputabilidade penal indica que os critérios clássicos de dolo, culpa e erro de tipo permanecem plenamente aplicáveis ao ambiente digital, embora exijam interpretação sensível às especificidades tecnológicas (Silva, 2022). O dolo manifesta-se com clareza em fraudes estruturadas e reiteradas, enquanto o erro de tipo deve ser reconhecido apenas em situações de efetivo desconhecimento técnico relevante (Costa, 2023).

Outro resultado importante refere-se à responsabilidade das plataformas digitais. Verificou- se que tais agentes desempenham papel central na organização das interações e na gestão de riscos, possuindo deveres de moderação, segurança e cooperação (Comitê Gestor da Internet no Brasil; NIC.br, 2012). Contudo, a responsabilização penal deve permanecer excepcional, condicionada à demonstração de posição de garantidor, omissão relevante e nexo com o resultado, nos termos da teoria da imputação objetiva (Roxin, 2009; Brasil, 1940).

No campo da persecução penal, os resultados indicam que o principal obstáculo reside na prova digital, caracterizada por volatilidade, dispersão e dependência de provedores privados (EUROJUST, 2024; Council of Europe, 2025). A dificuldade de coleta e preservação de evidências, especialmente em contextos transnacionais, evidencia que os entraves são operacionais e técnicos, e não normativos.

A internalização da Convenção de Budapeste representa avanço relevante ao estabelecer mecanismos de cooperação internacional e preservação de dados, contribuindo para maior eficiência investigativa (Brasil, 2023; Council of Europe, 2025). Ainda assim, sua efetividade depende de capacitação institucional e integração entre órgãos nacionais e internacionais (EUROJUST, 2025).

No âmbito preventivo, os resultados demonstram que a repressão penal, isoladamente, é insuficiente para enfrentar os riscos dos jogos digitais. A literatura aponta a necessidade de políticas públicas integradas, envolvendo educação digital, regulação de plataformas e proteção de usuários vulneráveis (UNICEF, 2025; OFCOM, 2025). No Brasil, iniciativas como a Política Nacional de Educação Digital e o Estatuto Digital da Criança e do Adolescente indicam avanço na adoção de uma abordagem preventiva (Brasil, 2023; 2025).

7. Conclusão

Depreende-se que os jogos virtuais consolidaram-se como ecossistemas sociotécnicos complexos, transcendendo o mero entretenimento para se tornarem espaços fundamentais de interação social, construção de identidade e networking.

Todavia, essa mesma arquitetura que fomenta a autonomia e o pertencimento também cria janelas de oportunidade para diversas práticas ilícitas, evidenciando que os riscos nestes ambientes não decorrem exclusivamente do conteúdo, mas sim das oportunidades situacionais proporcionadas pelo anonimato, pela baixa responsabilização e pela ausência de guardiões eficazes

Nesse sentido, a aplicação da Teoria das Atividades Rotineiras e da Prevenção Situacional do Crime demonstrou ser um caminho eficaz para compreender a dinâmica delitiva no universo gamer, permitindo identificar como ofensores motivados exploram alvos adequados em áreas de baixa vigilância, como chats e mercados de itens virtuais. Verificou-se que fenômenos como o aliciamento (grooming), fraudes patrimoniais (ATO) e a toxicidade são problemas persistentes que exigem uma resposta multidisciplinar, integrando criminologia, psicologia e governança técnica

Quanto ao problema de pesquisa, este estudo conclui que o ordenamento jurídico brasileiro é, em regra, suficiente para enfrentar os crimes praticados em jogos virtuais. A legislação penal vigente, robustecida por leis como a Lei 14.155/2021, mostra-se apta a abarcar condutas como estelionato eletrônico e invasão de dispositivo informático sem a necessidade da criação apressada de novos tipos penais

Contudo, o maior desafio para a eficácia do Direito Penal não reside na norma em si, mas na dificuldade probatória, na volatilidade dos vestígios digitais e na complexidade da cooperação internacional em crimes transnacionais. Ademais, a responsabilidade das plataformas digitais deve ser pautada por deveres de cuidado e pelo conceito de safety by design, implementando mecanismos preventivos que dificultem a prática delitiva desde a concepção do sistema

Embora as plataformas não devam ser punidas criminalmente de forma automática por atos de terceiros, elas ocupam uma posição de garantidoras que as obriga a cooperar com as autoridades e a moderar riscos previsíveis, especialmente no que tange à proteção de públicos vulneráveis.

Sustenta-se que a proteção efetiva no ambiente digital depende de um modelo híbrido que combine a repressão penal subsidiária com políticas públicas de educação digital e regulação administrativa, como as previstas na Política Nacional de Educação Digital e no ECA Digital. Somente através da articulação entre governança privada, fiscalização estatal e capacitação técnica dos órgãos de investigação será possível preservar o caráter lúdico dos jogos, garantindo, ao mesmo tempo, um ambiente seguro e conforme aos direitos fundamentais dos utilizadores

Referências

ARMINI, Matheus Gomes Vidigal. **Os crimes cibernéticos e seus impactos no ambiente digital das plataformas de jogos on-line**: uma análise sobre a prevenção de crimes e responsabilização do ofensor. 2025. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade de Direito de Vitória, Vitória, 2025. Disponível em: http://www.repositorio.fdv.br:8080/handle/fdv/1897. Acesso em: 6 abr. 2026.

BARAÚNA, Guilherme de Souza. **Metaverso:** como os jogos vão afetar a realidade. 2021. Disponível em: https://epsjv.phlnet.com.br/beb/textocompleto/mfn21789.pdf. Acesso em: 7 out. 2025.

BISPO, Bruno Raphael da Mata Silva. **Ferramenta de educação em segurança digital**: um jogo interativo com Pygame. 2024. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/8586. Acesso em: 7 out. 2025.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023.** Promulga a Convenção sobre o Crime Cibernético. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 17 mar. 2026.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Rio de Janeiro: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 6 mar. 2026.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Estatuto da Criança e do Adolescente. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 23 fev. 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 17 out. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 out. 2025.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Código Penal para dispor sobre crimes eletrônicos. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 17 mar. 2026.

BRASIL**. Lei nº 14.533, de 11 de janeiro de 2023**. Institui a Política Nacional de Educação Digital. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14533.htm. Acesso em: 17 mar. 2026.

BRASIL. **Lei nº 15.211, de 17 de setembro de 2025**. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-15.211-de-17-de-setembro-de-2025-656579619. Acesso em: 17 mar. 2026.

CAPLAN, J. M.; KENNEDY, L. W.; MILLER, J. Cyber-routine activity theory. **Oxford: Oxford University Press,** 2025. Disponível em: https://oxfordre.com. Acesso em: 17 out. 2025.

CASTRO, Célio Alves de et al. Comportamento do consumidor de jogos eletrônicos: um estudo bibliométrico. **Espacio Abierto,** v. 30, n. 3, p. 56–75, 2021. Disponível em: https://www.redalyc.org/journal/122/12268654003/12268654003.pdf. Acesso em: 7 out. 2025.

CETIC.BR. **TIC Kids Online Brasil 2024**: principais resultados. São Paulo: CGI.br/NIC.br, 2024. Disponível em: https://cetic.br. Acesso em: 17 out. 2025.

CETIC.BR. **TIC Kids Online Brasil 2025**: principais resultados. São Paulo: CGI.br/NIC.br, 2025. Disponível em: https://cetic.br. Acesso em: 17 mar. 2026.

CLARKE, R. V. **Situational crime prevention:** successful case studies. 2. ed. Guilderland: Harrow and Heston, 1997.

COHEN, L. E.; FELSON, M. Social change and crime rate trends: a routine activity approach. **American Sociological Review**, v. 44, n. 4, p. 588–608, 1979.

CORNISH, D. B.; CLARKE, R. V. Twenty-five techniques of situational crime prevention. **Phoenix:** ASU, 2003.

COSTA, Carlos Eduardo Gontijo. **Cibercriminalidade: os crimes cibernéticos e os limites da punibilidade no ambiente virtual.** 2023. Trabalho de Conclusão de Curso – Pontifícia Universidade Católica de Minas Gerais, Arcos, 2023. Disponível em: https://bib.pucminas.br. Acesso em: 25 nov. 2025.

DRUMMOND, A. et al. Do longitudinal studies support long-term relationships between violent video game use and aggression among youth? **Royal Society Open Science,** 2020.

EUROPOL. Internet organised crime threat assessment (IOCTA) 2024**. Luxemburgo:** Publications Office of the European Union, 2024. Disponível em: https://www.europol.europa.eu. Acesso em: 17 mar. 2026.

FIGUEIREDO, Rudá. Crimes eletrônicos e Lei 14.155/2021. **Ministério Público do Estado da Bahia,** 2021.

FROMMEL, J. et al. Toxicity in online games. **Proceedings of the ACM**, 2024.

GOMES, Julio Cesar Lôbo da Costa; MEDRADO, Lucas Cavalcante; GAMA, Giliarde B. A. C. V. R. N. Crimes cibernéticos: desafios jurídicos. **Revista JRG de Estudos Acadêmicos**, v. 7, n. 15, 2024.

GUILHERME, Henrique Cabral. **Crimes digitais em jogos online e NFTs no século XXI**. 2022. Trabalho de Conclusão de Curso – Pontifícia Universidade Católica de São Paulo, São Paulo, 2022.

HU, Y.; HUANG, J.; ZHANG, Y. Cyberbullying in online games. **Technology, Mind, and Behavior,** 2025.

HUIZINGA, Johan. **Homo ludens:** o jogo como elemento da cultura. São Paulo: Perspectiva, 2019.

IMPERVA. **Bad bot report 2024.** 2024. Disponível em: https://www.imperva.com. Acesso em: 17 out. 2025.

INTERPOL. **Global guidelines for digital forensics laboratories**. 2019. Disponível em: https://www.interpol.int. Acesso em: 17 mar. 2026.

ITU; UNICEF. **Guidelines for industry on child online protection**. Geneva/New York, 2020.

KWAK, H.; BLACKBURN, J.; HAN, S. Exploring cyberbullying and other toxic behavior in team competition online games. **In: CHI PLAY. 2015.**

MELO, Amnon Gonçalves. **A tentativa de criminalização dos jogos eletrônicos no Brasil.** 2024. Trabalho de Conclusão de Curso – Universidade Federal de Alagoas, Maceió, 2024.

MESTRE-BACH, V.; POTENZA, M. N. Gamer cyberbullying: a narrative review. **Journal of Gambling Issues,** 2025.

MOTA, Thiago Henrique Santos. **A pirataria e o seu impacto no mercado de jogos digitais no Brasil.** 2023. Trabalho de Conclusão de Curso – Universidade Federal de Sergipe, 2023.

OFCOM. **Online safety and gaming.** Londres, 2024. Disponível em: https://www.ofcom.org.uk. Acesso em: 17 mar. 2026.

PINHEIRO, Emanuel Arcanjo Cabral Torres. **A prevenção da criminalidade juvenil**. Lisboa, 2025.

PRESCOTT, A. T.; SARGENT, J. D.; HULL, J. G. **Meta-analysis of violent video games and aggression.** PNAS, 2018.

PRZYBYLSKI, A. K.; WEINSTEIN, N. **Violent video game engagement and aggression.** Royal Society Open Science, 2019.

REIS, Patricia Rossi dos. **Interculturalidade e sustentabilidade.** 2021.

ROXIN, Claus. **A proteção de bens jurídicos como função do direito penal.** Porto Alegre: Livraria do Advogado, 2009.

SAFERNET BRASIL. **Nota técnica 02/2025**. Salvador, 2025. Disponível em: https://new.safernet.org.br. Acesso em: 17 out. 2025.

SANTOS, Francisco Matheus Damasceno dos; MAGALHÃES FILHO, Glauco Barreira. Loot boxes e regulação. **Revista Opinião Jurídica**, 2024.

SILVA, Tiago Augusto Nogueira da. **Direito cibernético**. 2022.

SPICER, S. G. et al. Loot boxes, problem gambling and mental health. **Addictive Behaviors**, 2022.

THORN. **Sexual extortion and young people.** 2025. Disponível em: https://info.thorn.org. Acesso em: 17 mar. 2026.

UNICEF. **Childhood in a digital world.** 2025. Disponível em: https://www.unicef.org. Acesso em: 17 mar. 2026.

WIJKSTRA, M. et al. **Toxic behavior in online video games**. ACM, 2024.

YAR, Majid. Theorizing cybercrime. **European Journal of Criminology**, 2005.

ZENDLE, D.; CAIRNS, P. **Video game loot boxes and gambling.** PLOS ONE, 2019.