UNIVERSIDADE FEDERAL DE MINAS GERAIS

Faculdade de Filosofia e Ciências Humanas

Programa de Pós-graduação em Estudos de Criminalidade e Segurança Pública

Carla Fernanda da Cruz

SEGURANÇA PÚBLICA NO BRASIL E CRIMINALIDADE: revisão sistemática sobre os crimes no metaverso

Belo Horizonte

2024

Carla Fernanda da Cruz

SEGURANÇA PÚBLICA NO BRASIL E CRIMINALIDADE: revisão sistemática sobre os crimes no metaverso

Trabalho de Conclusão de Curso apresentado ao Pós-graduação do Centro de Estudos de Criminalidade e Segurança Pública – CRISP, como requisito parcial para obtenção do título de Especialista em Estudos de Criminalidade e Segurança Pública.

Orientadora: Profª. Drª. Roseane de Aguiar Lisboa Narciso

Coorientador: Prof. Dr. Luiz Otávio Braga Paulon

Belo Horizonte

2024

FICHA CATALOGRÁFICA

301
C957s
2024

Cruz, Carla Fernanda da.

Segurança pública no Brasil e criminalidade [recurso eletrônico] : revisão sistemática sobre os crimes no metaverso / Carla Fernanda da cruz. - 2024.

1 recurso online (50 f.): pdf.

Orientadora: Roseane de Aguiar Lisboa.
Coorientador: Luiz Otávio Braga Paulon.

Monografia apresentada ao curso de Especialização em Estudos de Criminalidade e Segurança Pública - Crisp - Universidade Federal de Minas Gerais, Faculdade de Filosofia e Ciências Humanas.

Inclui bibliografia.

1.Metaverso. 2. Crime. 3.Segurança pública. I. Lisboa, Roseane de Aguiar . II.Paulon, Luiz Otávio Braga . III.Universidade Federal de Minas Gerais. Faculdade de Filosofia e Ciências Humanas. IV.Título.

Ficha catalográfica elaborada por Vilma Carvalho de Souza - Bibliotecária - CRB-6/1390

UNIVERSIDADE FEDERAL DE MINAS GERAIS

ATA

UNIVERSIDADE FEDERAL DE MINAS GERAIS
FACULDADE DE FILOSOFIA E CIÊNCIAS HUMANAS
DEPARTAMENTO DE SOCIOLOGIA
ESPECIALIZAÇÃO EM ESTUDOS DE CRIMINALIDADE E SEGURANÇA PÚBLICA

FOLHA DE APROVAÇÃO DE DEFESA DE MONOGRAFIA DE

2023692428 CARLA FERNANDA DA CRUZ

Aos treze dias do mês de dezembro de dois mil e vinte e quatro, reuniu-se a banca examinadora de defesa de monografia do Curso de Especialização em Estudos de Criminalidade e Segurança Pública, composta por: Profa. Drª Roseane de Aguiar Lisboa Narciso (orientadora), Profº Drº Luiz Otavio Braga Paulon (coorientador), Profa. Drª Valéria Cristina de Oliveira, Profa. Drª. Valéria Cássia Dell'Isola e Profº Me. Gabriel de Souza Salema, para examinar a monografia intitulada "**SEGURANÇA PÚBLICA NO BRASIL E CRIMINALIDADE: revisão sistemática sobre os crimes no metaverso**" – discente **CARLA FERNANDA DA CRUZ** . Procedeu-se a arguição, finda a qual os membros da banca examinadora reuniram-se para deliberar, decidindo por unanimidade pela aprovação da monografia, com nota 85,0 Para constar, foi lavrada a presente ata, que segue assinada pela Coordenadora do Curso.

Belo Horizonte, 07 de novembro de 2025

Profa. Dra. Ludmila Mendonça Lopes Ribeiro
Coordenadora do Curso de Especialização em Estudos de Criminalidade e Segurança Pública

Documento assinado eletronicamente por **Ludmila Mendonca Lopes Ribeiro**, **Professora do Magistério Superior**, em 07/11/2025, às 11:00, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufmg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4719473** e o código CRC **9E430FE9**.

“Lutar e vencer todas as batalhas não é a glória suprema A glória suprema consiste em quebrar a resistência do inimigo sem lutar”.
(Tzu, 2006)

RESUMO

O presente estudo tem como objeto os crimes praticados no metaverso — denominados metacrimes — e as respostas institucionais das forças de segurança pública a essas condutas, com ênfase no contexto brasileiro. Objetiva identificar e categorizar os principais tipos de metacrimes documentados na literatura especializada; analisar os fatores estruturais do ambiente metaversal que potencializam a ocorrência de condutas ilícitas; e avaliar as estratégias e os mecanismos institucionais de atuação policial para sua prevenção e repressão. A pesquisa é de natureza qualitativa e exploratória, desenvolvida por meio de revisão sistemática da literatura científica nacional e internacional, com abordagem dedutiva e técnicas de pesquisa bibliográfica e documental, tendo como fontes principais as bases Portal de Periódicos CAPES, SciELO e Google Scholar, complementadas por relatórios técnicos da Europol e da Interpol. Os resultados revelaram que os metacrimes se manifestam em dez grandes categorias: crimes de identidade, crimes financeiros, crimes contra a propriedade virtual, crimes de propriedade intelectual, agressões e ofensas sexuais mediadas por avatares, crimes contra crianças, cibercrimes de segunda geração, atos de terrorismo, crimes contra a segurança pública e condutas destinadas a causar sofrimento psicológico. Identificaram-se como fatores estruturais habilitantes o anonimato dos usuários, a imersividade sensorial, a escalabilidade dos delitos digitais, a coleta intensiva de dados biométricos e a ausência de marcos regulatórios consolidados. No plano das respostas institucionais, verificou-se que a atuação policial no Brasil é ainda incipiente, comprometida pela precariedade de infraestrutura tecnológica, pela ausência de formação especializada nos currículos das academias de polícia e pelas dificuldades jurídico-processuais decorrentes da natureza transnacional dos delitos. As iniciativas legislativas brasileiras em curso — os Projetos de Lei n. 2.175/2023 e n. 261/2024 — representam avanços normativos relevantes, embora insuficientes para abarcar a totalidade dos metacrimes documentados. Conclui-se que o metaverso constitui uma nova e complexa fronteira para a segurança pública, que exige abordagem multidisciplinar e coordenada, envolvendo a atualização do arcabouço normativo, a formação especializada das forças policiais e a cooperação internacional, com vistas a garantir a proteção efetiva dos direitos fundamentais dos usuários no espaço digital imersivo.

Palavras-chave: Metacrime; Metaverso; Criminalidade; Segurança Pública; Cibercrime.

ABSTRACT

This study focuses on crimes committed in the metaverse — referred to as metacrimes — and the institutional responses of public security forces to such conduct, with emphasis on the Brazilian context. It aims to identify and categorize the main types of metacrimes documented in the specialized literature; to analyze the structural factors of the metaversal environment that increase the occurrence of illicit conduct; and to evaluate the institutional strategies and mechanisms of police action for their prevention and repression. The research is qualitative and exploratory in nature, developed through a systematic review of national and international scientific literature, using a deductive approach and bibliographic and documental research techniques, with the main sources being the CAPES Journal Portal, SciELO, and Google Scholar, supplemented by technical reports from Europol and Interpol. The results revealed that metacrimes manifest across ten broad categories: identity crimes, financial crimes, crimes against virtual property, intellectual property crimes, sexual assaults and offenses mediated by avatars, crimes against children, second-generation cybercrimes, acts of terrorism, crimes against public security, and conduct intended to cause psychological harm. The following structural enabling factors were identified: user anonymity, sensory immersivity, the scalability of digital offenses, the intensive collection of biometric data, and the absence of consolidated regulatory frameworks. Regarding institutional responses, it was found that police action in Brazil remains incipient, compromised by the precariousness of technological infrastructure, the absence of specialized training in police academy curricula, and the legal and procedural difficulties arising from the transnational nature of the offenses. The ongoing Brazilian legislative initiatives — Bills No. 2,175/2023 and No. 261/2024 — represent relevant normative advances, though insufficient to encompass the full range of documented metacrimes. It is concluded that the metaverse constitutes a new and complex frontier for public security, requiring a multidisciplinary and coordinated approach involving the updating of the regulatory framework, the specialized training of police forces, and international cooperation, with a view to ensuring the effective protection of the fundamental rights of users in immersive digital spaces.

Keywords: *Metacrime; Metaverse; Criminality; Public Security; Cybercrime.*

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização

O século XXI inaugurou uma era de transformações tecnológicas sem precedentes, caracterizada pela crescente digitalização das relações sociais, econômicas e jurídicas. Nesse cenário, o metaverso emerge como uma das inovações mais disruptivas, configurando-se como um espaço virtual tridimensional, imersivo e persistente, no qual os usuários, representados por avatares, interagem em tempo real, simulando dinâmicas próprias da vida cotidiana. Distintas das plataformas digitais convencionais, as arquiteturas metaversais combinam tecnologias de realidade aumentada (AR), realidade virtual (VR), inteligência artificial (IA) e *blockchain*, integrando experiências de comunicação, lazer, trabalho, comércio e sociabilidade em um único ecossistema digital.

O conceito de metaverso, embora popularizado a partir de 2021 com os anúncios estratégicos de empresas como a *Meta Platforms*, tem raízes literárias que remontam ao romance de ficção científica *Snow Crash*, publicado por Neal Stephenson em 1992, no qual o autor antecipa uma realidade virtual imersiva acessada por meio de avatares digitais. Desde então, o desenvolvimento tecnológico progressivo — notadamente no campo da computação gráfica, das redes de alta velocidade (5G) e dos dispositivos de realidade estendida — tem aproximado essa visão prospectiva da realidade concreta, tornando o metaverso um fenômeno social e econômico de crescente relevância.

Estima-se que o mercado global do metaverso, avaliado em aproximadamente 65,5 bilhões de dólares em 2022, possa atingir cerca de 936,6 bilhões de dólares até 2030, conforme projeções da *Grand View Research* (2023), evidenciando a magnitude econômica e a centralidade social que essa tecnologia tende a assumir nas próximas décadas. Com essa expansão acelerada, multiplicam-se igualmente as oportunidades de utilização ilícita desses espaços, suscitando novos e complexos desafios para a criminologia, o direito penal e as instituições de segurança pública.

Sob uma perspectiva criminológica, o metaverso pode ser analisado a partir de três dimensões interdependentes. Na primeira dimensão, os mundos virtuais comportam-se como extensões imersivas das dinâmicas criminosas já conhecidas no ambiente digital, porém amplificadas pelo caráter tridimensional, sensorial e pseudopresencial dessas plataformas, o que aumenta, de forma qualitativa, o potencial lesivo de condutas como assédio, extorsão, fraudes e exploração sexual. Na segunda dimensão, os espaços virtuais tendem a constituir

ecossistemas sociais relativamente autônomos, nos quais as categorias jurídicas e criminológicas do mundo físico nem sempre se aplicam diretamente, demandando a construção de novos quadros analíticos e normativos. Na terceira dimensão, a imersividade e o engajamento emocional proporcionados pelo metaverso podem gerar efeitos de retroalimentação sobre o comportamento dos usuários em suas vidas físicas, influenciando atitudes, percepções e condutas sociais, especialmente em contextos de uso intenso e prolongado.

Organismos internacionais de policiamento já identificaram e classificaram as principais ameaças criminais emergentes nesse ambiente. A Europol, em relatório publicado em 2022 intitulado *Policing in the Metaverse: What Law Enforcement Needs to Know*, destacou cinco categorias prioritárias de crimes: roubo de identidade (potencializado pelo uso de dados biométricos e biometria comportamental); crimes financeiros, incluindo lavagem de dinheiro por meio de ativos virtuais e criptomoedas; assédio, abuso e exploração de crianças e adolescentes; terrorismo, com finalidades de recrutamento, radicalização e treinamento virtual; e desinformação em escala amplificada. A Interpol, por sua vez, incorporou a essas categorias o furto de propriedade e ativos virtuais (NFTs e criptoativos), as agressões sexuais mediadas por avatares — fenômeno denominado por especialistas como estupro de avatar — e os cibercrimes de segunda geração, como *ransomware* e *doxing* aplicados ao ambiente imersivo.

A repressão a esses delitos enfrenta obstáculos estruturais significativos. A natureza transnacional e descentralizada do metaverso coloca em xeque os tradicionais critérios de jurisdição territorial, ao mesmo tempo em que o anonimato proporcionado pelos avatares dificulta a identificação e a responsabilização dos autores. No Brasil, a urgência regulatória manifestou-se em iniciativas legislativas recentes, notadamente o Projeto de Lei n. 2.175/2023, que propõe o estabelecimento de um marco regulatório abrangente para o metaverso, e o Projeto de Lei n. 261/2024, que visa tipificar a violência psicológica praticada em ambientes de realidade virtual como crime autônomo no Código Penal Brasileiro.

Diante desse panorama, a presente pesquisa parte da premissa de que a ascensão do metaverso como espaço de interação social impõe a necessidade de uma resposta acadêmica, institucional e normativa coordenada. A construção de um ambiente virtual seguro e eticamente governado exige a convergência de esforços entre pesquisadores, legisladores e forças de segurança pública, com vistas à elaboração de estratégias de prevenção e repressão adequadas à especificidade e à complexidade desse novo território digital.

1.2 Problema de pesquisa

O metaverso constitui-se como um ambiente multifuncional no qual os usuários podem estabelecer relações de trabalho, consumo, entretenimento e sociabilidade de forma imersiva e persistente. Tal configuração reproduz, no plano virtual, as condições estruturais que, no ambiente físico, são reconhecidamente propícias ao surgimento de condutas delitivas. Nesse sentido, a premissa histórica e criminológica segundo a qual a criminalidade acompanha os fluxos de aglomeração humana aplica-se integralmente ao contexto digital: onde quer que pessoas se reúnam, criem vínculos, realizem transações e exercitem poder, haverá, potencialmente, a incidência de comportamentos ilícitos.

O metaverso, portanto, não é imune à criminalidade. Ao contrário, suas características técnicas e sociais específicas — como o anonimato, a imersividade, a interoperabilidade transnacional e a ausência de marcos regulatórios consolidados — tendem a potencializar determinadas formas de delinquência e a criar condições favoráveis ao surgimento de modalidades delitivas inteiramente novas. Embora os crimes sejam cometidos por meio de representações virtuais, seus efeitos — financeiros, psicológicos e reputacionais — recaem sobre pessoas físicas reais, com impactos mensuráveis e, não raro, graves.

Ademais, a ausência de protocolos institucionalizados de policiamento no metaverso e a insuficiência de capacitação tecnológica das forças de segurança pública para atuar nesses ambientes configuram lacunas operacionais que merecem atenção específica da academia e dos gestores de políticas públicas de segurança. Nesse contexto, o presente trabalho situa-se no encontro entre a criminologia digital, o direito penal e as políticas de segurança pública, propondo-se a investigar o seguinte problema de pesquisa: quais são os principais crimes cometidos no metaverso e de que maneira se estrutura a atuação policial voltada à prevenção e à repressão desses delitos?

1.3 Hipótese

Parte-se da hipótese central de que a criminalidade no metaverso manifesta-se de forma multidimensional, abrangendo tanto modalidades delitivas já tipificadas na legislação vigente — como estelionato, lavagem de dinheiro, crimes contra a honra e abuso sexual — quanto condutas emergentes que ainda carecem de enquadramento jurídico específico no ordenamento brasileiro, a exemplo do estupro de avatar, do furto de ativos virtuais e da violência psicológica mediada por ambientes imersivos.

Complementarmente, sustenta-se a hipótese de que a atuação policial para prevenção e repressão de crimes no metaverso é ainda incipiente e insuficiente, em razão de três ordens de fatores: (i) a precariedade de equipamentos e de infraestrutura tecnológica nas instituições policiais brasileiras para acesso e monitoramento de ambientes imersivos; (ii) a ausência de formação especializada em crimes digitais de nova geração nos currículos das academias de polícia; e (iii) as dificuldades jurídico-processuais decorrentes da natureza transnacional dos delitos e do anonimato proporcionado pelas plataformas metaversais. Tais hipóteses, somadas à escassez de literatura científica nacional sobre o tema, indicam que o campo se encontra em fase de constituição, demandando investigação sistemática e rigorosa.

1.4 Objetivos

1.4.1 Objetivo Geral

O objetivo geral do presente trabalho é realizar uma revisão sistemática da literatura científica nacional e internacional sobre os crimes cometidos no metaverso, analisando suas principais manifestações, impactos e os desafios que impõem às estruturas de segurança pública, com ênfase no contexto brasileiro.

1.4.2 Objetivos específicos

Os objetivos específicos desta pesquisa são:

a) identificar e categorizar os tipos de crimes mais frequentemente relatados no metaverso, com base na literatura especializada e nos relatórios de organismos internacionais de segurança;
b) analisar os fatores estruturais do ambiente metaversal que potencializam a ocorrência de condutas ilícitas, com especial atenção ao anonimato, à escalabilidade dos crimes digitais e à vulnerabilidade emocional dos usuários;
c) avaliar as estratégias e os mecanismos institucionais de atuação policial para a prevenção e a repressão dos crimes no metaverso, identificando lacunas operacionais e normativas.

1.5 Justificativa e relevância

A justificativa para o desenvolvimento desta pesquisa assenta-se sobre dois eixos indissociáveis: a relevância social e a relevância acadêmica do tema.

Do ponto de vista social, o metaverso representa uma transformação estrutural na forma como os indivíduos se relacionam, trabalham, consomem e exercem sua cidadania digital. À medida que empresas, instituições públicas, sistemas educacionais e serviços essenciais migram progressivamente para esses ambientes imersivos, os riscos à segurança individual e coletiva multiplicam-se proporcionalmente. Os chamados metacrimes — crimes cometidos no ou por meio do metaverso — impõem danos reais e mensuráveis a pessoas físicas e jurídicas, ainda que mediados por representações virtuais. A compreensão, a prevenção e a repressão eficaz dessas condutas constituem, portanto, uma demanda urgente de segurança pública e de proteção de direitos fundamentais.

Nesse sentido, a Política Nacional de Defesa (PND), atualizada pelo Decreto n. 10.577/2020, reconhece explicitamente o espaço cibernético como domínio estratégico de interesse nacional, ressaltando a necessidade de garantir a segurança e a resiliência dos sistemas de informação, comunicação e gerenciamento críticos para o funcionamento do Estado brasileiro (Brasil, 2020). A ampliação do espaço cibernético para incluir ambientes metaversais exige a atualização contínua desse arcabouço estratégico e a formação permanente das forças de segurança pública para os desafios da segurança digital imersiva.

Do ponto de vista acadêmico, o tema permanece subexplorado na literatura científica brasileira. Levantamentos realizados nas principais bases de dados nacionais — como o Portal de Periódicos da CAPES, o SciELO e o Google Scholar — revelam a escassez de estudos que articulem, de forma sistemática, as categorias da criminologia e do direito penal com as especificidades técnicas e socioculturais do metaverso. Tal lacuna é ainda mais pronunciada no que diz respeito às instituições policiais brasileiras e à sua capacidade de resposta a esses crimes emergentes. A presente pesquisa pretende, assim, contribuir para o avanço do conhecimento nas áreas de criminologia digital, direito penal cibernético e políticas de segurança pública, fornecendo subsídios teóricos e empíricos para o desenvolvimento de estratégias institucionais e normativas mais eficazes.

Por fim, destaca-se a relevância profissional e institucional desta investigação para as forças policiais brasileiras. A formação de quadros capacitados para atuar preventiva e repressivamente em ambientes digitais imersivos é condição sine qua non para que as instituições de segurança pública possam cumprir sua missão constitucional de preservação da ordem pública

e da incolumidade das pessoas e do patrimônio — nos termos do art. 144 da Constituição Federal de 1988 — em um cenário no qual as fronteiras entre o físico e o virtual tornam-se, progressivamente, mais porosas e interdependentes.

1.6 Metodologia

1.6.1 Natureza e Abordagem da Pesquisa

A presente pesquisa caracteriza-se como qualitativa, de natureza exploratória e descritiva, operacionalizada por meio da revisão sistemática da literatura com abordagem metaetnográfica. A escolha por essa modalidade investigativa decorre da necessidade de mapear, organizar e sintetizar o estado da arte sobre a criminalidade no metaverso, campo emergente que, embora crescente em relevância social e jurídica, carece de sistematização cientifica consolidada, especialmente no contexto brasileiro.

A abordagem qualitativa fundamenta-se na premissa epistemológica de que os fenômenos sociais, jurídicos e criminológicos não podem ser adequadamente compreendidos por meio de dados numéricos isolados, mas exigem interpretação contextualizada, analise de sentidos e articulação teórica. Conforme Denzin e Lincoln (2006), a pesquisa qualitativa constitui um campo de investigação que atravessa disciplinas e temas, possuindo conjunto de praticas interpretativas materiais que tornam o mundo visível por meio de representações como notas de campo, entrevistas e anotações pessoais, permitindo compreender os fenômenos a partir da perspectiva dos próprios atores sociais envolvidos.

Nessa perspectiva, a pesquisa qualitativa não busca a generalização estatística, mas a compreensão aprofundada de fenômenos complexos, permitindo identificar padrões, categorias e relações emergentes do conjunto da literatura analisada (Yin, 2016). Tal abordagem e especialmente adequada ao presente objeto de estudo, dado o caráter recente, multidimensional e ainda insuficientemente tipificado da criminalidade no metaverso.

1.6.2 Tipo de Pesquisa

Quanto aos objetivos, a pesquisa e classificada como exploratória e descritiva. A dimensão exploratória justifica-se pela relativa escassez de produções cientificas consolidadas sobre crimes no metaverso no âmbito da segurança publica brasileira, demandando uma etapa de mapeamento e sistematização do conhecimento disponível. Para Gil (2002, p. 41), a

pesquisa exploratória tem como finalidade primordial desenvolver, esclarecer e modificar conceitos e ideias, tendo em vista a formulação de problemas mais precisos ou hipóteses pesquisáveis para estudos posteriores, envolvendo habitualmente levantamento bibliográfico e documental.

A dimensão descritiva manifesta-se na identificação e categorização das principais formas de criminalidade reportadas no metaverso, dos fatores de risco associados e das estratégias de atuação policial, permitindo o estabelecimento de um quadro analitico organizado com base na evidencia bibliográfica disponível (Gil, 2002; Lakatos; Marconi, 2021).

Quanto aos procedimentos técnicos, a pesquisa vale-se do método bibliográfico e documental, fundamentado na seleção, leitura critica e analise de artigos científicos, relatórios institucionais, legislação comparada, teses, dissertações e documentos técnicos de organismos nacionais e internacionais de segurança publica. Especial atenção foi dispensada a fontes primarias de organismos como a Europol, a Interpol, o Fórum Econômico Mundial e o Ministério da Justiça e Segurança Publica do Brasil.

1.6.3 Método de Abordagem

O método de abordagem adotado e o dedutivo, articulado com uma perspectiva dogmática de analise jurídica. O método dedutivo, caracterizado pela progressão do geral para o particular, parte das premissas gerais estabelecidas pela criminologia clássica e pela teoria do direito penal para, a partir delas, extrair inferências aplicáveis ao fenômeno especifico da criminalidade no metaverso. Tal método, segundo Lakatos e Marconi (2021), e adequado quando o pesquisador parte de proposições teóricas previamente estabelecidas e busca verifica-las em face de dados empíricos ou bibliográficos.

A perspectiva dogmática, por seu turno, não implica aceitação acrítica dos paradigmas jurídicos existentes, mas sim sua aplicação rigorosa e sistemática ao fenômeno analisado. Como esclarece Ascensão (2014), a dogmática jurídica caracteriza-se pela interpretação e sistematização coerente do ordenamento vigente, com vistas a sua aplicação racional aos casos concretos. Essa abordagem permite situar os metacrimes dentro das categorias do direito penal brasileiro e, simultaneamente, identificar as lacunas normativas que demandam resposta legislativa ou interpretativa especifica.

1.6.4 Protocolo de Revisão Sistemática

A revisão sistemática foi conduzida em conformidade com as diretrizes metodológicas amplamente reconhecidas na literatura cientifica, com adaptacoes pertinentes a natureza qualitativa do estudo. Conforme Siddaway, Wood e Hedges (2019), a revisão sistemática distingue-se da revisão narrativa pela sua transparência, replicabilidade e rigor no processo de seleção e análise dos estudos incluídos. Sua modalidade metaetnográfica, também denominada metassíntese qualitativa, e indicada quando a revisão visa integrar pesquisas qualitativas sobre um tópico, com o objetivo de localizar temas, conceitos ou teorias-chave capazes de fornecer explicações mais robustas para o fenômeno analisado.

O desenvolvimento do protocolo de revisão observou as seguintes etapas sequenciais: (i) formulação do problema de pesquisa e dos objetivos; (ii) definição das fontes de busca e dos descritores; (iii) estabelecimento dos critérios de inclusão e exclusão; (iv) seleção e triagem dos estudos; (v) extração, organização e analise dos dados; e (vi) síntese interpretativa dos resultados.

1.6.5 Fontes de Busca e Descritores

A busca bibliográfica foi realizada nas seguintes bases de dados e repositórios digitais indexados: Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES); *Scientific Electronic Library Online* (SciELO); *Google Scholar*; *Scopus; Web of Science*; além de repositórios institucionais de universidades publicas brasileiras e portais de legislação como o Planalto e o portal da Câmara dos Deputados. Foram também consultados relatórios técnicos e documentos institucionais da Europol, da Interpol, do Fórum Econômico Mundial e do Gabinete de Segurança Institucional da Presidência da Republica.

Os descritores utilizados nas buscas foram organizados em três eixos temáticos inter-relacionados, combinados por meio dos operadores booleanos AND e OR:

a) Eixo 1 - Ambiente virtual: metaverso; metaverse; realidade virtual; realidade aumentada; mundos virtuais; espaço cibernético; ambiente imersivo; Web 3.0; virtual world;

b) Eixo 2 - Criminalidade: crime; criminalidade; delito; cibercrime; metacrime; crime digital; crime virtual; fraude digital; abuso virtual; exploração sexual virtual; *criminal behavior; cybercrime*; *digital offense*;

c) Eixo 3 - Segurança publica e policiamento: segurança pública; atuação policial; prevenção criminal; repressão; policiamento digital; *law enforcement; digital policing; police metaverse*; *public security*.

1.6.6 Critérios de Inclusão e Exclusão

A seleção do corpus analítico obedeceu a critérios predefinidos de inclusão e exclusão, aplicados em duas etapas sequenciais: triagem por titulo e resumo e, em seguida, leitura integral dos textos prelecionados.

Foram adotados como critérios de inclusão: (i) publicações acadêmicas e técnicas com relevância cientifica comprovada, indexadas em bases reconhecidas ou emanadas de organismos internacionais de referencia; (ii) estudos que abordem, direta ou indiretamente, a criminalidade em ambientes digitais imersivos ou a atuação policial no contexto do metaverso; (iii) trabalhos publicados em português, inglês ou espanhol; (iv) documentos legislativos, projetos de lei e relatórios institucionais diretamente relacionados ao objeto de pesquisa; (v) publicações sem restrição temporal, embora tenha sido priorizada a produção cientifica dos últimos dez anos.

Foram adotados como critérios de exclusão: (i) trabalhos que abordem exclusivamente o metaverso sob perspectivas comerciais, técnicas ou de entretenimento, sem articulação com questões de segurança publica ou criminalidade; (ii) publicações duplicadas ou cujos conteúdos sejam integralmente incorporados por versões mais recentes; (iii) textos de opinião, editoriais ou publicações sem revisão por pares, salvo quando emanados de autoridades institucionais reconhecidas; (iv) materiais sem identificação autoral ou de procedência não verificável.

1.6.7 Analise e Sintese dos Dados

Os materiais selecionados foram submetidos a analise de conteúdo, técnica que, conforme Bardin (2016), consiste em um conjunto de procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens, cujos indicadores permitem a inferência de conhecimentos relativos as condições de produção e recepção dessas mensagens. Trata-se de abordagem metodológica amplamente reconhecida nas ciências sociais e jurídicas pela sua capacidade de extrair significados latentes e manifestos de textos, documentos e discursos.

Para fins desta pesquisa, a analise de conteúdo foi operacionalizada em três fases: (i) pré-análise, consistente na leitura flutuante do material, na identificação dos documentos pertinentes e na formulação das hipóteses de leitura; (ii) exploração do material, mediante a codificação e categorização temática dos conteúdos identificados; e (iii) tratamento dos resultados e inferência, fase na qual os dados categorizados foram interpretados a luz do referencial teórico da criminologia digital e do direito penal cibernético.

As categorias temáticas emergentes da analise foram organizadas em três eixos analíticos, correspondentes aos objetivos específicos da pesquisa: (a) tipologia dos crimes cometidos no metaverso; (b) fatores estruturais de risco e potencializarão da criminalidade no ambiente emissivo; e (c) estratégias institucionais de prevenção e repressão, com ênfase nas capacidades e limitações das forcas de segurança publica brasileiras.

A síntese final foi conduzida de forma interpretativa e integrativa, buscando não apenas descrever o estado da arte, mas identificar lacunas teóricas, contradições entre autores e contribuições potenciais para o avanço do campo, em consonância com os propósitos da metaetnografia qualitativa (Siddaway; Wood; Hedges, 2019). A analise das fontes foi norteada por critérios de pertinência temática, credibilidade institucional e atualidade dos dados, garantindo o rigor metodológico exigido para pesquisa de nível de especialização.

2 METAVERSO

O metaverso constitui uma das inovações tecnológicas mais significativas do século XXI, configurando-se como um espaço virtual tridimensional, imersivo e persistente no qual indivíduos, representados por avatares digitais, interagem em tempo real por meio de tecnologias convergentes. Sua emergência como fenômeno social, econômico e jurídico relevante não apenas reconfigura as formas tradicionais de comunicação e interação humana, mas também introduz novas dimensões de vulnerabilidade e risco para a segurança pública, uma vez que os ambientes virtuais imersivos passam a reproduzir — e, por vezes, a amplificar — as dinâmicas de criminalidade conhecidas no mundo físico e digital.

A compreensão aprofundada do metaverso — suas origens conceituais, seu quadro tecnológico e sua relação com fenômenos correlatos como a inteligência artificial, a realidade aumentada e a cibercriminologia — é pressuposto indispensável para a análise dos metacrimes que constituem o objeto central desta pesquisa. As subseções a seguir desenvolvem esse quadro analítico de forma progressiva e sistematizada.

2.1 Metaverso: conceituação e evolução histórica

O termo metaverso resulta da combinação do prefixo grego meta (além de, transcendendo) com o substantivo universo, denotando, em sentido literal, uma realidade que transcende o universo físico convencional. Do ponto de vista operacional, o metaverso designa um conjunto de espaços virtuais tridimensionais, persistentes e interoperáveis, nos quais usuários representados por avatares interagem entre si e com objetos digitais em tempo real, por meio de tecnologias de realidade aumentada (AR), realidade virtual (VR) e computação em nuvem, de forma síncrona e com continuidade de dados — incluindo identidade, histórico, bens virtuais e relações sociais (Ball, 2021).

Do ponto de vista histórico, a concepção de ambientes virtuais imersivos antecede a própria popularização do termo. O romance Neuromancer, de William Gibson, publicado em 1984, introduziu o conceito de ciberespaço como uma alucinação consensual habitada por usuários conectados em rede — antecipando, em termos literários, as bases do que viria a se tornar o metaverso. Em 1992, o escritor estadunidense Neal Stephenson cunhou efetivamente o termo metaverso em seu romance de ficção científica Snow Crash, descrevendo uma realidade paralela digital habitada por avatares, na qual seres humanos imersos em

plataformas digitais podiam interagir entre si de forma persistente e tridimensional (Stephenson, 1992).

A primeira implementação técnica relevante foi o *software Second Life*, concebido por Philip Rosedale em 1999 e lançado comercialmente em 2003 pela empresa norte-americana *Linden Lab*, tornando-se o metaverso mais conhecido e amplamente adotado por usuários em escala global nas décadas seguintes (Grossi *et al*., 2024). Desde então, o desenvolvimento de plataformas metaversais expandiu-se significativamente, incorporando títulos como *Active Worlds, There, Fortnite, Minecraft* e *Roblox*, que introduziram comunidades expressivas de usuários em mundos virtuais próprios, caracterizados pela criação colaborativa de conteúdo e pela emergência de economias digitais internas (Guimarães; Silva; Silva, 2022).

O salto de visibilidade social e econômica do metaverso deu-se, contudo, a partir de 2021, com o anúncio da *Meta Platforms* — anteriormente *Facebook* — de sua estratégia de transição para o metaverso como plataforma central de interação social e comercial. Esse movimento catalisou investimentos massivos de grandes corporações tecnológicas, como *Microsoft, Google, Apple e Nvidia*, e consolidou o metaverso como vetor central da economia digital emergente. O mercado global do metaverso apresenta projeções de crescimento excepcionais para a próxima década, com estimativas que apontam para a multiplicação por mais de dez vezes do valor setorial até 2030 (Grand View Research, 2023) — conforme detalhado na seção 2.1

Do ponto de vista conceitual, diversas definições acadêmicas e técnicas buscam delimitar o metaverso. Backes e Schlemmer definem-no como:

> uma tecnologia que se constitui no ciberespaço e se 'materializa' por meio da criação de Mundos Digitais Virtuais em 3D (MDV3D), no qual diferentes espaços para o viver e conviver são representados em três dimensões, propiciando o surgimento dos 'mundos paralelos' contemporâneos.(Backes; Schlemmer, 2008, p. 522)

Em perspectiva mais abrangente e tecnicamente precisa, Matthew Ball (2021) define o metaverso como uma rede em grande escala e interoperável de mundos virtuais tridimensionais renderizados em tempo real, que podem ser experimentados de forma síncrona e persistente por um número efetivamente ilimitado de usuários, com senso de presença individual e continuidade de dados — como identidade, histórico, direitos, objetos, comunicações e pagamentos. Essa definição é amplamente adotada na literatura especializada por sua abrangência e precisão técnica (Tibúrcio *et al*., 2022; Campos, 2022).

Independentemente das variantes definicionais, há consenso na literatura de que o metaverso diferencia-se de outros espaços digitais por quatro características fundamentais: (i) a tridimensionalidade do ambiente, que confere imersividade e senso de presença; (ii) a persistência, que garante a continuidade do mundo virtual independentemente da conexão individual dos usuários; (iii) a interoperabilidade, que permite a transição de identidades, bens e dados entre diferentes plataformas; e (iv) a simultaneidade, que possibilita a coexistência em tempo real de um número virtualmente ilimitado de usuários (Dionísio; Burns; Gilbert, 2013).

2.2 Metaverso: termos e distinções conceituais

A compreensão rigorosa do metaverso exige a delimitação de suas fronteiras conceituais em relação a tecnologias e fenômenos correlatos que, embora frequentemente associados, possuem naturezas, objetivos e alcances distintos. As subseções seguintes analisam as principais distinções conceituais pertinentes ao presente estudo.

2.2.1 Metaverso e Internet

A distinção entre metaverso e internet, embora aparentemente intuitiva, possui implicações técnicas, sociais e jurídicas de considerável profundidade. A internet, em sua concepção original, constitui uma rede global de computadores interconectados que viabiliza a troca de informações por meio de protocolos de comunicação padronizados. Trata-se de uma infraestrutura predominantemente bidimensional, na qual os usuários interagem por meio de texto, imagens, áudio e vídeo, em modo predominantemente assíncrono e passivo. Tim Berners-Lee, inventor da *World Wide Web*, enfatizou que a internet serve como infraestrutura para a distribuição de conteúdo digital, sem, contudo, proporcionar experiências verdadeiramente imersivas (Berners-Lee, 1996).

Clay Shirky (2008) observa que, embora a internet tenha democratizado a produção e o compartilhamento de conteúdo, suas funcionalidades permanecem fundamentalmente limitadas à troca de informações e à comunicação textual ou multimídia. As principais aplicações da internet — como correio eletrônico, redes sociais, comércio eletrônico e plataformas de streaming — operam em interfaces gráficas planas e não proporcionam senso de presença ou imersão espacial.

O metaverso, por sua vez, transcende essa lógica bidimensional ao oferecer um espaço tridimensional, interativo e imersivo que simula aspectos da realidade física por meio da

convergência de tecnologias como realidade aumentada, realidade virtual e *blockchain*. Conforme Castronova (2005), o metaverso configura-se como uma realidade digital na qual os usuários podem interagir em tempo real em ambientes simulados, realizando atividades que vão desde o lazer e o trabalho até transações econômicas complexas. Diferentemente da navegação na internet — essencialmente passiva e baseada na recuperação de informações —, a experiência no metaverso é ativa, imersiva e corporificada, na medida em que o usuário é representado por um avatar que se move e interage em um espaço tridimensional contínuo.

A tipificação e a criminalização dessas condutas apresentam desafios jurídicos desenvolvidos nas seções 3.2 (jurisdição), 3.3 (prevenção e repressão), 3.4 e 3.5 (iniciativas legislativas brasileiras).

2.2.2 Metaverso e Inteligência Artificial

A relação entre metaverso e inteligência artificial (IA) é marcada pela complementaridade funcional, ainda que os dois fenômenos sejam conceitualmente distintos. A IA, definida por Russell e Norvig (2021, p. 56) como a área da ciência da computação que se concentra em criar sistemas capazes de realizar tarefas que normalmente requerem inteligência humana — como raciocínio, aprendizado, reconhecimento de padrões e tomada de decisão —, não constitui por si só um espaço virtual de interação. Ela representa, antes, um conjunto de técnicas e algoritmos que podem ser incorporados a diferentes plataformas e aplicações.

O metaverso, em contrapartida, configura um espaço de interação social tridimensional, cuja experiência é definida pelo senso de presença, imersividade e persistência (Dionísio; Burns; Gilbert, 2013). A IA pode ser integrada ao metaverso para enriquecer e complexificar essa experiência, por meio de funcionalidades como assistentes virtuais, personagens não jogáveis (*Non-Player Characters* — NPCs) com comportamentos adaptativos e realistas, algoritmos de personalização da experiência do usuário, sistemas de moderação de conteúdo e mecanismos de detecção de comportamentos suspeitos ou ilícitos.

Essa convergência entre IA e metaverso tem implicações diretas para a segurança pública. Por um lado, a IA potencializa as capacidades de monitoramento e prevenção de crimes nos ambientes imersivos, ao permitir a identificação automatizada de padrões de comportamento delitivo. Por outro, confere aos cibercriminosos ferramentas mais sofisticadas para a prática de fraudes, engenharia social e manipulação de usuários — como o uso de

deepfakes gerados por IA para falsificar identidades de avatares ou para produzir conteúdo sexual não consensual envolvendo representações digitais de pessoas reais (Europol, 2022).

2.2.3 Metaverso, Realidade Aumentada (AR) e Realidade Virtual (VR)

O metaverso integra e articula, em sua arquitetura tecnológica, as tecnologias de Realidade Aumentada (AR) e Realidade Virtual (VR), que, embora frequentemente confundidas, operam segundo princípios e finalidades distintos. A compreensão dessas distinções é fundamental para se entender o grau de imersividade e os vetores de risco específicos de cada modalidade.

A Realidade Aumentada, definida por Azuma (1997, p. 359) como a tecnologia que combina objetos virtuais com o mundo real, é interativa em tempo real e registrada em três dimensões, caracteriza-se por sobrepor elementos digitais ao ambiente físico percebido pelo usuário, sem isolamento completo deste. Por meio de dispositivos como smartphones, tablets e óculos de AR, o usuário continua a perceber o mundo físico ao seu redor, com a adição de camadas de informação ou objetos digitais sobrepostos. Essa tecnologia tem sido amplamente aplicada em educação, arquitetura, medicina, varejo e, crescentemente, em treinamentos de segurança pública e operações policiais de campo.

A Realidade Virtual, por sua vez, é definida por Milgram e Kishino (1994) como uma tecnologia que imerge o usuário em um ambiente totalmente digital, separando-o perceptualmente do mundo físico. Por meio de dispositivos como os head-mounted displays (HMDs) — exemplificados pelo *Oculus Quest, HTC Vive e PlayStation VR* —, o usuário é envolvido em um cenário completamente simulado, que pode imitar fielmente o mundo real ou criar ambientes inteiramente ficcionais. Milgram e Kishino (1994) descreveram a VR como uma experiência de imersão completa, na qual os sentidos do usuário são controlados pelo ambiente digital, gerando um senso robusto de presença nesse espaço virtual.

O metaverso, conforme Guimarães, Silva e Silva (2022), integra essas duas tecnologias em um ambiente híbrido e persistente, no qual as vivências ocorrem predominantemente por meio de avatares. Nesse espaço, pessoas podem trabalhar, fazer compras, estudar, competir, colaborar e socializar em experiências que combinam elementos da AR e da VR com graus variáveis de imersividade. Milgram e Kishino (1994) denominaram essa zona intermediária de Realidade Mista (Mixed Reality — MR), que une aspectos de ambas as tecnologias para criar interações mais complexas entre o físico e o virtual.

Do ponto de vista da segurança pública, o grau de imersividade e a sensação de presença corporificada característicos do metaverso amplificam os impactos psicológicos das violências ali perpetradas. Estudos de neurociência cognitiva indicam que experiências traumáticas vividas em ambientes de alta imersividade podem gerar respostas emocionais e psicofisiológicas comparáveis àquelas produzidas por eventos reais, o que confere especial gravidade a crimes como o assédio sexual virtual e o estupro de avatar (Bailenson, 2018).

2.3 Cibercrimes, Cibercriminologia e Metacrimes

A compreensão dos metacrimes — objeto central desta pesquisa — requer o exame progressivo das categorias que os precedem e contextualizam: o cibercrime, como fenômeno delitivo originário do ciberespaço, e a cibercriminologia, como campo científico voltado ao seu estudo sistemático. O metacrime emerge, nessa progressão conceitual, como uma modalidade qualificada e específica de cibercrime, adaptada às particularidades dos ambientes virtuais imersivos.

O termo cibercrime passou a ser amplamente adotado a partir do final da década de 1990, notadamente após a reunião do G8 realizada em Lyon, em 1997, na qual os países participantes reconheceram a necessidade de coordenação internacional para o enfrentamento das atividades ilícitas praticadas por meio de redes digitais. Em sentido amplo, o cibercrime designa toda ação ou prática ilícita praticada no ambiente digital, utilizando redes de computadores e a internet como meios ou alvos (Silva; Lima, 2018).

Do ponto de vista jurídico-penal, Clough (2010) define os cibercrimes como atos ilícitos cometidos com o auxílio de computadores e redes de telecomunicações, ou contra esses sistemas. Jesus e Milagre (2016) acrescentam que o crime cibernético — também denominado crime virtual — configura-se pela utilização de dispositivos informáticos conectados à internet como instrumentos para a perpetração de comportamentos ilícitos, seja como meio de execução, seja como objeto material da conduta criminosa. A legislação brasileira disciplina parte dessas condutas por meio da Lei n. 12.737/2012 (Lei Carolina Dieckmann) e da Lei n. 14.155/2021, que ampliou as penas para crimes como invasão de dispositivo informático, fraude e furto por meio eletrônico.

O conceito de ciberespaço, entendido como o conjunto de redes e sistemas informáticos interconectados que constituem o substrato do crime cibernético, foi consagrado por Almeida *et al*. (2015) como um espaço intermediário entre o mundo virtual e o mundo real, no qual as ações digitais produzem efeitos jurídicos e sociais concretos. Essa

compreensão é fundamental para afastar equívocos reduccionistas que tratam o ciberespaço como uma dimensão puramente ficta ou sem consequências tangíveis para as vítimas.

A cibercriminologia, por sua vez, surge como resposta acadêmica a essa nova realidade delitiva. Conforme Favero e Favero (2021), trata-se do campo de saber, dentro da ciência criminológica, que investiga as determinações e determinantes do fenômeno criminal em suas passagens mutuamente consideradas, do ciberespaço para o firmamento palpável. A disciplina analisa não apenas os tipos de crimes que ocorrem em ambiente digital, mas também as motivações dos cibercriminosos, o perfil das cibervítimas, as ciberleis aplicáveis e as técnicas de ciberinvestigação disponíveis (SYDOW, 2022). Sua relevância para o presente estudo reside em fornecer o quadro teórico e analítico adequado para compreender as dinâmicas comportamentais e institucionais que permeiam a criminalidade no metaverso.

No contexto específico do metaverso, emerge o conceito de metacrime, que designa as atividades criminosas praticadas dentro ou por meio desses ambientes virtuais imersivos, explorando suas características e capacidades técnicas únicas para a perpetração de condutas ilícitas (CANADA, 2024). Os metacrimes configuram-se como uma subcategoria qualificada dos cibercrimes, na medida em que não apenas se valem de redes digitais como meios de execução, mas se aproveitam especificamente das propriedades imersivas, corporificadas e persistentes do metaverso para produzir impactos vitimológicos de natureza e intensidade diferenciadas.

Os metacrimes apresentam três especificidades estruturais que os diferenciam dos cibercrimes convencionais. A primeira diz respeito ao grau de imersividade e corporificação: no metaverso, a vítima experimenta a violência por meio de um avatar que representa sua identidade e presença digital, gerando respostas emocionais e psicológicas de maior intensidade do que aquelas provocadas por ataques textuais ou imagísticos na internet convencional. A segunda especificidade refere-se à natureza transnacional e descentralizada dos ambientes metaversais, que operam em infraestruturas distribuídas globalmente, dificultando a aplicação dos tradicionais critérios de jurisdição territorial e a identificação dos autores. A terceira especificidade concerne ao surgimento de modalidades delitivas sem precedentes no direito penal existente, como o estupro de avatar, o furto de identidade biométrica e a violência psicológica imersiva, que ainda não encontram tipificação específica no ordenamento jurídico brasileiro[1].

[1] O PL n. 2.175/2023 e o PL n. 261/2024, atualmente em tramitação no Congresso Nacional, propõem instrumentos normativos para esse campo — cf. seções 3.4 e 3.5.

O enfrentamento dos metacrimes exige, portanto, não apenas a atualização legislativa e a capacitação tecnológica das forças de segurança pública, mas também o desenvolvimento de novas técnicas forenses digitais, a construção de protocolos de cooperação internacional específicos para ambientes imersivos e a formação de quadros policiais especializados nas particularidades técnicas e jurídicas dos metaversos. Esses desafios institucionais são detalhados nas seções subsequentes desta pesquisa.

3 METACRIMES: OS CRIMES NO METAVERSO

A consolidação do metaverso como espaço de interação social, econômica e cultural representa não apenas uma transformação tecnológica, mas também um ponto de inflexão para o direito penal e para as políticas de segurança pública. Onde quer que se estabeleçam relações humanas mediadas por tecnologia, instalam-se igualmente as condições estruturais para o surgimento de condutas ilícitas. O metaverso não constitui exceção a essa dinâmica histórica — conforme apontado na seção 1.2 — ao reproduzir virtualmente as condições de aglomeração e exercício de poder do mundo físico, esse ambiente cria oportunidades inéditas para o cometimento de crimes e potencializa modalidades delitivas já conhecidas (Europol, 2022).

A questão de fundo que permeia o debate acadêmico e institucional é se os crimes no metaverso constituem fenômenos criminológicos genuinamente novos ou, antes, manifestações tecnologicamente mediadas de crimes já tipificados. Marshall e Tompsett (2023) sustentam que os crimes cometidos no metaverso não são necessariamente novos em sua essência, embora suas modalidades de execução o sejam. Em linha com essa perspectiva, os autores argumentam que a tecnologia funciona como extensora — e não criadora — das classes criminosas preexistentes, ampliando o escopo e o alcance de atos delitivos já conhecidos, sem necessariamente produzir novas categorias ontológicas de crime.

Essa perspectiva, contudo, não pode ser adotada de forma irrestrita. A imersividade, a corporificação por avatares, o anonimato estrutural, a descentralização jurisdicional e a possibilidade de interações sensorialmente enriquecidas — incluindo toque tátil, rastreamento ocular e detecção de expressões faciais — conferem ao metaverso características que não apenas ampliam, mas qualificam e reconfiguram as dinâmicas criminosas. O metacrime — cuja conceituação e especificidades estruturais foram desenvolvidas na seção 2.3 — emerge, nesse contexto, como categoria que não apenas amplia, mas reconfigura qualitativamente as dinâmicas criminosas, exigindo respostas normativas e institucionais específicas.

Do ponto de vista histórico, o uso criminoso ou abusivo das tecnologias digitais não é fenômeno novo. Os primeiros casos documentados de exploração ilícita de redes de computadores remontam ao final da década de 1980, notadamente com o Morris Worm, em 1988 — considerado o primeiro malware de autopropagação da história da internet —, e com o caso de espionagem cibernética internacional investigado por Clifford Stoll, que rastreou o hacker alemão Markus Hess em um dos primeiros grandes incidentes de intrusão em sistemas

governamentais. Esses precedentes demonstram que cada nova camada tecnológica de interação humana atrai, invariavelmente, novos vetores de criminalidade (Stoll, 1989).

No contexto específico do metaverso, os efeitos dos crimes não ficam circunscritos ao plano virtual. Conforme destacado pela Europol (2022), assédios, abusos sexuais e outras formas de violência perpetradas por meio de avatares podem gerar consequências psicológicas graves e duradouras para as vítimas, comparáveis às produzidas por eventos traumáticos no mundo físico. Conforme demonstrado por Bailenson (2018) — cf. seção 2.2.3 —, a imersividade do ambiente faz com que danos psicológicos vivenciados no plano virtual sejam neurobiologicamente equiparáveis aos de experiências físicas reais, superando a dicotomia entre crime virtual e dano real.

Diante desse quadro, organismos internacionais de segurança pública e pesquisa têm intensificado os esforços de mapeamento, categorização e enfrentamento dos metacrimes. A Europol (2022) e a Interpol (2024) produziram as taxonomias mais abrangentes sobre a criminalidade no metaverso, catalogando dez categorias de condutas ilícitas — detalhadas na seção 3.1 —, que abrangem desde crimes de identidade e fraudes financeiras até ofensas sexuais mediadas por avatares, terrorismo e atos de sofrimento psicológico.

A tipificação e a criminalização dessas condutas apresentam desafios jurídicos desenvolvidos nas seções 3.2 (jurisdição), 3.3 (prevenção e repressão), 3.4 e 3.5 (iniciativas legislativas brasileiras).

As subseções a seguir analisam as principais dimensões desse desafio: a experiência da Europol (3.1), as questões jurisdicionais (3.2), as estratégias de prevenção e repressão (3.3) e as iniciativas legislativas brasileiras — PL n. 2.175/2023 (3.4) e PL n. 261/2024 (3.5).

3.1 Experiência da Polícia Europeia — Europol — acerca do Metaverso

A experiência europeia no campo do policiamento digital constitui referência incontornável para a compreensão dos desafios e das estratégias institucionais voltadas ao enfrentamento da criminalidade no metaverso. O Escritório Central da Polícia Europeia — Europol —, reconhecido por seu protagonismo no desenvolvimento de inteligência policial aplicada ao ambiente cibernético, tem se dedicado sistematicamente ao estudo do metaverso desde a criação do seu Laboratório de Inovação, em 2019. Esse esforço institucional resultou, em 2022, na publicação do relatório *Policing in the Metaverse: What Law Enforcement Needs to Know*, documento que reúne contribuições de acadêmicos, policiais e especialistas em tecnologia e que se tornou referência obrigatória no debate internacional sobre a matéria.

O relatório parte da constatação de que o metaverso, ao ampliar exponencialmente as possibilidades de interação social e econômica, abre simultaneamente novas e sofisticadas oportunidades para a prática de crimes digitais. Fraudes financeiras, abusos sexuais mediados por avatares, lavagem de dinheiro por meio de criptomoedas e NFTs, espionagem e radicalização terrorista são apresentados como ameaças concretas e iminentes, cuja magnitude tende a crescer proporcionalmente à expansão da base de usuários das plataformas metaversais (Europol, 2022).

Um dado de especial relevância apresentado pelo relatório refere-se à escala e à precocidade da vitimização no metaverso: pesquisa citada pelo documento indica que aproximadamente 58% dos entrevistados declararam ter sido vítimas de alguma forma de abuso nesse ambiente. O relatório registra, ainda, o caso de uma usuária que foi vítima de abuso sexual grupal apenas 60 segundos após ingressar em uma plataforma metaversal — episódio que evidencia a gravidade e a velocidade com que essas violências podem ocorrer. Agrava esse quadro o fato de que uma parcela significativa dos usuários do metaverso é composta por crianças e adolescentes, população particularmente vulnerável às formas de abuso e exploração que proliferam nesses ambientes (Europol, 2022).

No campo dos crimes financeiros, o relatório destaca a crescente utilização de criptomoedas e ativos digitais não fungíveis (NFTs) como instrumentos para a lavagem de dinheiro e a ocultação de ativos ilícitos no metaverso. Embora as transações em blockchain sejam, por natureza, registradas e rastreáveis, a sofisticação das técnicas de ofuscação — como o uso de mixers e a fragmentação de transações — dificulta a identificação da origem dos recursos. A Europol recomenda que as forças policiais desenvolvam competências específicas em análise forense de blockchain e estabeleçam parcerias estratégicas com plataformas financeiras e corretoras de ativos digitais para o monitoramento de fluxos financeiros suspeitos (Europol, 2022).

A convergência entre inteligência artificial e metaverso é identificada pelo relatório como vetor de potencialização tanto de ameaças quanto de respostas institucionais. Do lado das ameaças, a IA viabiliza a criação de avatares hiper-realistas baseados em *deepfakes*, que podem ser utilizados para falsificação de identidade, extorsão, manipulação psicológica e disseminação de desinformação em escala. Do lado das respostas, a IA oferece ferramentas poderosas para o monitoramento automatizado de comportamentos suspeitos, a identificação de padrões de radicalização e a detecção precoce de práticas criminosas nos ambientes imersivos. A Europol recomenda que as autoridades desenvolvam mecanismos específicos

para identificar e rastrear o uso indevido de algoritmos de IA e de manipulação no metaverso (Europol, 2022).

A ausência de fronteiras físicas no metaverso — e suas implicações para a cooperação internacional, analisadas na seção 3.2 — é igualmente apontada pelo relatório como fator estrutural de complicação para o policiamento, tornando a articulação interinstitucional transnacional condição necessária para a eficácia repressiva (Europol, 2022).

Em termos de recomendações operacionais, o relatório da Europol (2022) propõe um conjunto articulado de medidas institucionais, agrupadas em quatro eixos principais. O primeiro eixo diz respeito ao desenvolvimento e aperfeiçoamento de ferramentas de vigilância e monitoramento adaptadas ao ambiente do metaverso, capazes de detectar atividades suspeitas e prevenir o cometimento de crimes antes que se consumem. O segundo eixo refere-se à utilização do próprio metaverso como plataforma para o treinamento imersivo de agentes policiais, por meio da simulação de locais de crime e de cenários operacionais em ambiente virtual. O terceiro eixo trata do estabelecimento de canais de interação acessíveis entre as forças policiais e o público, incluindo módulos de educação digital e conscientização sobre segurança cibernética. O quarto eixo concerne à construção de parcerias público-privadas com empresas de tecnologia para o desenvolvimento de arquiteturas metaversais que integrem, desde sua concepção, protocolos de segurança, mecanismos de rastreamento e ferramentas de identificação de usuários.

O relatório enfatiza, por fim, a urgência de que as forças de segurança adotem uma postura proativa e antecipatória em relação ao metaverso, reconhecendo-o como extensão do espaço público físico e atribuindo-lhe as mesmas obrigações de proteção, prevenção e repressão que orientam o policiamento convencional. O investimento em pesquisa e desenvolvimento, o intercâmbio de informações entre autoridades globais e a criação de parcerias público-privadas são destacados como condições necessárias para garantir que o metaverso se consolide como um espaço seguro, ético e regulado (Europol, 2022).

3.2 Jurisdição

A perspectiva de que o metaverso possa ser utilizado para a perpetração de crimes com alcance global suscita questões jurídicas de extraordinária complexidade, cujo enfrentamento desafia os fundamentos tradicionais do direito penal internacional. A natureza intrinsecamente transnacional e descentralizada desse ambiente virtual coloca em xeque os princípios clássicos de territorialidade e soberania estatal que estruturam os sistemas de jurisdição penal vigentes,

exigindo a construção de novos marcos conceituais e operacionais para a investigação, a persecução e a responsabilização dos autores de metacrimes.

O princípio da territorialidade, consagrado no art. 5º do Código Penal Brasileiro — segundo o qual aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional (Brasil, 1940) —, opera com base na premissa de que o locus delicti é identificável e circunscrito a um território físico determinado. Essa premissa, no entanto, é estruturalmente incompatível com a lógica dos metacrimes, nos quais o autor, a vítima e a infraestrutura tecnológica utilizada para a prática do delito podem estar situados em países distintos, submetidos a ordenamentos jurídicos potencialmente incompatíveis entre si.

Wendt e Jorge (2012, p. 181) observam que os recursos tecnológicos passam a permitir que os criminosos ajam em parcerias organizadas, mesmo em locais diferentes, distantes e muitas vezes sem ao menos se conhecerem, para que possam cometer o crime. Crespo (2011, p. 117), por sua vez, afirma que o surgimento do mundo virtual apresenta novas concepções de tempo e espaço, gerando empecilhos à aplicação de leis tradicionais e apresentando um novo entendimento de território, uma vez que rompem-se as barreiras de limites territoriais físicos. Fiorillo e Conte (2016, p. 203) reforçam essa perspectiva ao sustentarem que com a internet e o ambiente virtual, não existem barreiras ou limites de separação física, pois a concepção de território passa a ser qualquer um dos pontos interligados à rede e que tenha acesso às informações.

Diante dessas limitações, o ordenamento jurídico brasileiro tem recorrido ao princípio da territorialidade temperada, que consiste na aplicação preferencial da lei penal nacional, com possibilidade de aplicação subsidiária de leis estrangeiras por meio de tratados e convenções internacionais. Nesse sentido, o instrumento de cooperação internacional mais relevante no campo dos crimes digitais é a Convenção de Budapeste sobre o Crime Cibernético, de 2001, celebrada no âmbito do Conselho da Europa e aberta à adesão de países não membros. O Brasil aderiu formalmente a esse tratado por meio do Decreto n. 11.491/2023, tornando-se signatário do principal instrumento de cooperação internacional em matéria de cibercrime atualmente em vigor.

A Convenção de Budapeste estabelece um conjunto de obrigações aos Estados signatários, incluindo a tipificação de determinados crimes informáticos, a adoção de poderes processuais específicos para investigação de crimes digitais e a instituição de mecanismos de cooperação internacional ágeis e eficazes. Para os fins do presente estudo, destaca-se a relevância do Capítulo III da Convenção, que disciplina a cooperação internacional em

matéria de extradição, assistência mútua e compartilhamento de informações entre autoridades competentes de diferentes países, mecanismos essenciais para o enfrentamento dos metacrimes de natureza transnacional.

A coleta e a admissibilidade de provas digitais em processos por metacrimes apresentam, igualmente, desafios técnicos e jurídicos de considerável magnitude. Os dados e as interações no metaverso são frequentemente armazenados em servidores distribuídos globalmente, submetidos a diferentes regimes de proteção de dados e de obrigações de retenção de registros. A Lei Geral de Proteção de Dados Pessoais (LGPD — Lei n. 13.709/2018), no Brasil, e o Regulamento Geral de Proteção de Dados (GDPR), na União Europeia, impõem restrições ao acesso e ao tratamento de dados pessoais que podem, em determinadas circunstâncias, colidir com as necessidades investigativas das autoridades policiais. A compatibilização desses regimes é condição necessária para a eficácia das investigações de metacrimes em escala transnacional.

Fiorillo e Conte (2016, p. 321) concluem, com precisão, que é inegável a necessidade de cooperação internacional entre os Estados, independentemente de qual será o responsável pela aplicação da legislação. Essa conclusão é inteiramente aplicável ao contexto dos metacrimes: a ausência de um marco regulatório global harmonizado e de mecanismos operacionais eficientes de cooperação policial e judicial constitui, atualmente, uma das principais lacunas institucionais no enfrentamento da criminalidade nos ambientes virtuais imersivos. O desenvolvimento de frameworks legais e operacionais multilaterais, capazes de articular as diferentes jurisdições envolvidas de forma coordenada e eficaz, é imperativo para que a resposta estatal aos metacrimes seja proporcional à magnitude e à complexidade dessas condutas.

3.3 Prevenção e Repressão

O enfrentamento da criminalidade no metaverso exige uma abordagem estratégica que articule, de forma coordenada, ações de prevenção, detecção, investigação e repressão, adaptadas às especificidades técnicas e jurídicas desse ambiente virtual. Diferentemente dos modelos de policiamento convencional, que operam com base em critérios de territorialidade física e em estruturas hierárquicas centralizadas, o policiamento no metaverso demanda flexibilidade organizacional, especialização tecnológica e capacidade de cooperação interinstitucional e transnacional.

No campo da prevenção, a estratégia mais eficaz é aquela que age sobre os fatores estruturais que tornam o metaverso um ambiente propício à criminalidade. Schroeder (2018) defende que a segurança nos ambientes virtuais depende, antes de tudo, do design de suas infraestruturas: as plataformas que constituem o metaverso devem integrar, desde sua concepção, protocolos robustos de segurança cibernética — como autenticação multifatorial, criptografia de ponta a ponta e sistemas de moderação de conteúdo em tempo real —, de modo a reduzir as vulnerabilidades que favorecem fraudes, invasões, abuso de dados pessoais e violências entre usuários. Essa abordagem, denominada *security by design*, é progressivamente reconhecida como standard mínimo de responsabilidade das plataformas digitais.

A educação digital constitui igualmente pilar fundamental da estratégia preventiva. Wall (2007) sublinha a necessidade de que as forças de segurança colaborem com grandes empresas de tecnologia e implementem campanhas de conscientização junto aos usuários, com vistas a prevenir crimes digitais e a promover comportamentos seguros no ambiente virtual. Goodman (2015) acrescenta que a superfície de ataque digital cresce exponencialmente com cada nova plataforma ou ambiente digital, o que torna imperativa a adoção de tecnologias de inteligência artificial, monitoramento de dados em tempo real e criptografia avançada para a prevenção proativa de crimes. A orientação dos usuários sobre práticas seguras — como a identificação de golpes, o uso de autenticação de dois fatores e a proteção de dados biométricos — pode reduzir significativamente a vulnerabilidade individual no metaverso.

No campo da repressão, as forças de segurança enfrentam desafios operacionais que decorrem diretamente das características estruturais do metaverso: o anonimato dos usuários, a ausência de controles de acesso padronizados, a descentralização da infraestrutura tecnológica e a volatilidade das evidências digitais dificultam a identificação dos autores, a coleta de provas e a responsabilização judicial dos infratores. Holt, Bossler e Seigfried-Spellar (2015) destacam que o treinamento de policiais em forense digital é condição essencial para a eficácia das investigações de crimes cibernéticos e, por extensão, de metacrimes: os agentes precisam estar preparados para lidar com evidências digitais complexas, como logs de servidores, dados criptografados e o uso de avatares anônimos como instrumentos de execução de crimes.

A Interpol (2024) tem avançado na construção de capacidades institucionais para o policiamento do metaverso, incluindo o uso de ambientes imersivos para o treinamento de agentes e a simulação de cenários criminais virtuais. O Interpol *Metaverse Expert Group*,

criado em 2022, tem produzido orientações e recomendações para o enfrentamento dos metacrimes em cooperação com forças policiais de diferentes países, reconhecendo que as ameaças emergentes no metaverso requerem respostas coordenadas e tecnologicamente sofisticadas. Em relatório publicado em janeiro de 2024, a Interpol reconheceu que o metaverso é um ambiente complexo e que os cenários de metacrime podem evoluir rapidamente, incluindo tipos de crimes existentes, emergentes e totalmente novos.

Loftus (2024) propõe o conceito de policiamento híbrido como modelo operacional adequado ao enfrentamento da criminalidade no metaverso: trata-se de uma abordagem na qual os agentes de segurança são treinados para atuar de forma integrada em ambientes físicos e virtuais, realizando operações e investigações coordenadas nos dois planos de realidade. Esse modelo reconhece que, em um cenário de crescente hibridização entre o físico e o digital, a dicotomia entre policiamento real e virtual tende a se tornar operacionalmente obsoleta.

No plano legislativo, Brenner (2012) adverte que a legislação cibernética vigente é insuficiente para abarcar as complexidades do metaverso, na medida em que as leis foram concebidas para mundos físicos e não refletem adequadamente as nuances dos crimes digitais, como fraudes em criptomoedas, lavagem de dinheiro via NFTs e assédios em espaços virtuais. A necessidade de reformas legislativas que incluam tipos penais específicos para condutas praticadas em ambientes de realidade virtual — como a violência psicológica imersiva, o estupro de avatar e o furto de identidade biométrica — é, portanto, premissa indispensável para a eficácia da repressão penal no metaverso.

Em síntese, a prevenção e a repressão de metacrimes exigem uma combinação de tecnologias avançadas, legislação adaptada, formação especializada de operadores de segurança e educação continuada dos usuários. A eficácia dessas estratégias estará condicionada à capacidade das forças de segurança pública de desenvolver competências tecnológicas, forenses e normativas em ritmo compatível com a evolução acelerada dos metacrimes — desafio que as seções 3.4 e 3.5 evidenciam ainda não ter encontrado resposta normativa suficiente no ordenamento brasileiro.

3.4 Projeto de Lei n. 2.175/2023

A ausência de um marco regulatório específico para o metaverso no ordenamento jurídico brasileiro tem impulsionado iniciativas legislativas destinadas a suprir essa lacuna normativa. A mais abrangente delas é o Projeto de Lei n. 2.175/2023, em tramitação no

Congresso Nacional, que propõe a criação do Marco Regulatório do Metaverso, estabelecendo princípios, diretrizes e normas para o uso e a realização de negócios jurídicos nesse ambiente virtual.

A justificativa do projeto parte do reconhecimento de que o metaverso representa uma convergência entre a realidade física e a realidade virtual que tem se tornado crescentemente presente na vida cotidiana, abrangendo ambientes virtuais, tecnologias de realidade virtual e aumentada e plataformas digitais que permitem a interação e a cooperação entre usuários em tempo real. Diante do rápido avanço dessa tecnologia, o legislador considerou fundamental estabelecer um marco regulatório que promova a transparência, a segurança e a inovação em todo o ecossistema do metaverso (Brasil, 2023).

Em termos de conteúdo normativo, o PL n. 2.175/2023 estrutura-se em torno de três eixos principais. O primeiro eixo diz respeito à proteção dos usuários, abrangendo garantias de livre acesso, proteção de dados pessoais, respeito à privacidade e salvaguarda dos direitos autorais e de propriedade intelectual no ambiente metaversal. O segundo eixo trata da regulação dos negócios jurídicos realizados no metaverso, estabelecendo critérios para a determinação da lei aplicável, do foro competente e dos mecanismos de resolução de disputas — incluindo mediação e arbitragem —, com vistas a garantir a segurança jurídica das transações virtuais. O terceiro eixo refere-se à cooperação internacional, reconhecendo que a aplicação efetiva das normas no metaverso requer a harmonização de diferentes jurisdições e o estabelecimento de canais eficientes de intercâmbio de informações e assistência jurídica mútua entre os Estados.

No que concerne à determinação da lei aplicável aos negócios jurídicos realizados no metaverso, o projeto adota como critério geral a lei da jurisdição em que as partes envolvidas têm sua residência habitual, ressalvada a possibilidade de escolha expressa de lei diversa pelas partes. Em caso de negócios envolvendo partes de jurisdições distintas e ausência de acordo expresso, aplica-se a lei do local de residência habitual do autor da ação. A jurisdição competente para dirimir litígios é, em regra, a do foro do domicílio do réu, salvo disposição contratual em contrário (Brasil, 2023).

A cooperação internacional entre órgãos reguladores e autoridades competentes é apresentada pelo projeto como condição *sine qua non* para a efetividade das normas propostas. O documento reconhece que o caráter transnacional e descentralizado do metaverso exige não apenas a harmonização de normas entre diferentes jurisdições, mas também o estabelecimento de canais operacionais de intercâmbio de informações e assistência

mútua, capazes de prevenir fraudes, proteger direitos dos usuários e assegurar a responsabilização legal das partes envolvidas nos negócios jurídicos virtuais (Brasil, 2023).

Embora o PL n. 2.175/2023 represente um avanço normativo significativo, sua efetividade dependerá de ajustes contínuos à medida que o metaverso evolui tecnológica e socialmente. O legislador enfrenta o desafio de conciliar a necessidade de segurança jurídica — que requer normas claras, precisas e estáveis — com a exigência de adaptabilidade a um ambiente tecnológico em rápida transformação. A experiência regulatória de outros países, como os membros da União Europeia no âmbito do *Digital Services Act e do AI Act*, oferece referências comparativas relevantes para o aperfeiçoamento do marco regulatório brasileiro.

3.5 Projeto de Lei n. 261/2024

Paralelamente ao marco regulatório geral proposto pelo PL n. 2.175/2023, tramita no Congresso Nacional o Projeto de Lei n. 261/2024, que propõe a tipificação penal específica da violência psicológica praticada em ambiente de realidade virtual, por meio da inclusão do art. 147-C ao Decreto-Lei n. 2.848, de 7 de dezembro de 1940 — Código Penal Brasileiro. A iniciativa reflete o reconhecimento institucional de que os instrumentos penais vigentes são insuficientes para tutelar adequadamente a integridade psicológica dos usuários de ambientes imersivos, diante das formas inéditas de violência que esses espaços tornam possíveis.

A justificativa legislativa do projeto ancora-se em dados empíricos de considerável expressividade: segundo pesquisa citada no documento, 60% dos usuários brasileiros de internet declararam, em 2021, passar tempo em algum tipo de ambiente de realidade virtual, como plataformas de videogames e mundos virtuais. Esse dado evidencia a penetração social crescente dos ambientes imersivos no país e a urgência de dotar o ordenamento jurídico de instrumentos normativos capazes de proteger os usuários — em especial crianças e adolescentes — das violências que podem ali ocorrer (Brasil, 2024).

O projeto reconhece, ainda que em termos genéricos, a singularidade experiencial do metaverso: a capacidade de proporcionar ao usuário uma tal experiência de imersão que permite ter a percepção de estar efetivamente vivenciando aquela realidade (Brasil, 2024). Essa singularidade tem implicações diretas para a avaliação jurídico-penal das condutas praticadas nesses ambientes, na medida em que os danos psicológicos decorrentes de violências virtuais imersivas podem ser comparáveis, em gravidade e persistência, aos produzidos por violências físicas reais.

O caso que motivou centralmente a apresentação do projeto é emblemático: o estupro coletivo do avatar de uma adolescente de 16 anos no Reino Unido, episódio no qual a vítima relatou ter sofrido o mesmo trauma psicológico e emocional de uma vítima de estupro na vida real, dado o grau de imersão proporcionado pela plataforma (Brasil, 2024). Esse caso ilustra de forma paradigmática a tese de Bailenson (2018) — cf. seção 2.2.3 — de que o processamento cerebral de experiências imersivas de alta fidelidade é análogo ao de experiências físicas reais, conferindo gravidade objetiva e subjetiva aos danos sofridos em ambientes de realidade virtual.

Do ponto de vista da teoria geral do direito penal, a tipificação proposta pelo PL n. 261/2024 situa-se em tensão com os princípios da fragmentariedade e da subsidiariedade, que orientam a intervenção penal como *ultima ratio*. O caráter fragmentário do direito penal implica que apenas as condutas que causam dano relevante aos bens jurídicos mais importantes devem ser objeto de tutela penal. O caráter subsidiário, por sua vez, exige que a criminalização seja precedida pela verificação da insuficiência de outros ramos do direito — civil, administrativo — para oferecer proteção adequada. No contexto do projeto, a aplicação desses princípios demanda que a nova tipificação se restrinja a condutas cuja gravidade e potencial lesivo justifiquem a intervenção penal, evitando a inflação legislativa que compromete a coerência e a efetividade do sistema punitivo.

A aprovação do PL n. 261/2024 representaria um marco normativo relevante para a proteção da integridade psicológica dos usuários do metaverso, ao reconhecer juridicamente que a violência praticada em ambientes imersivos pode produzir danos reais e juridicamente relevantes, merecedores de tutela penal específica. Sua efetividade, contudo, dependerá da capacidade das forças de segurança de investigar essas condutas, identificar seus autores e produzir provas admissíveis em juízo — desafios operacionais que reforçam a necessidade de investimento contínuo na capacitação tecnológica e forense das instituições policiais brasileiras.

4 CONSIDERAÇÕES FINAIS

O presente trabalho teve como objeto a criminalidade no metaverso e como objetivo geral realizar uma revisão sistemática da literatura científica nacional e internacional sobre os crimes cometidos nesse ambiente virtual imersivo, examinando suas principais manifestações, os fatores estruturais que os potencializam e os desafios que impõem às estruturas de segurança pública, com ênfase na realidade brasileira. A pesquisa foi conduzida por meio de abordagem qualitativa, exploratória e descritiva, orientada pelo método dedutivo e pela perspectiva dogmático-jurídica, valendo-se da revisão sistemática metaetnográfica e da análise de conteúdo como técnicas principais de coleta e interpretação de dados.

O problema de pesquisa que norteou o estudo indagava: quais são os principais crimes cometidos no metaverso e de que maneira se estrutura a atuação policial voltada à prevenção e à repressão dessas condutas? A análise sistemática da literatura permitiu responder a essa questão de forma abrangente. Os resultados demonstraram que a criminalidade no metaverso abrange uma tipologia diversificada e em expansão, que combina modalidades delitivas já conhecidas — como fraudes financeiras, lavagem de dinheiro, assédio e exploração sexual — com formas inéditas de criminalidade que emergem das especificidades imersivas desse ambiente, como o estupro de avatar, o furto de identidade biométrica, a violência psicológica imersiva e o uso de deepfakes para falsificação de avatares (Europol, 2022; Interpol, 2024).

A hipótese central — de que a criminalidade no metaverso manifesta-se de forma multidimensional, abrangendo tanto modalidades tipificadas quanto condutas emergentes sem enquadramento jurídico específico — foi integralmente corroborada pelos resultados da revisão sistemática. A Europol (2022) e a Interpol (2024) catalogaram dez grandes categorias de crimes com incidência documentada no metaverso: crimes de identidade, crimes financeiros, crimes contra a propriedade virtual, crimes de propriedade intelectual, ofensas e agressões sexuais mediadas por avatares, crimes contra crianças, cibercrimes, atos de terrorismo, crimes contra a segurança pública e condutas destinadas a causar sofrimento psicológico. Essa taxonomia evidencia que o metaverso não representa apenas uma extensão do espaço digital bidimensional, mas um ambiente com dinâmicas criminais próprias, qualificadas pelo grau de imersividade, pela corporificação por avatares, pelo anonimato estrutural e pela descentralização jurisdicional.

A hipótese complementar — de que a atuação policial para prevenção e repressão de metacrimes é ainda incipiente e insuficiente — igualmente se confirmou, sustentada por três ordens de evidências. Primeiro, a precariedade de equipamentos e de infraestrutura

tecnológica nas instituições policiais para acesso e monitoramento de ambientes imersivos. Segundo, a ausência de formação especializada em crimes digitais de nova geração nos currículos das academias de polícia, lacuna que demanda resposta urgente das instituições responsáveis pela educação policial. Terceiro, as dificuldades jurídico-processuais decorrentes da natureza transnacional dos delitos e do anonimato proporcionado pelas plataformas metaversais, que tornam a identificação de autores e a coleta de provas admissíveis em juízo tarefas de elevada complexidade técnica e jurídica (Europol, 2022; Loftus, 2024).

Entre os achados de maior relevância, destaca-se a constatação de que os danos causados pelos metacrimes não se restringem ao plano virtual: assédios, abusos sexuais e outras formas de violência perpetradas por meio de avatares produzem consequências psicológicas reais e mensuráveis para as vítimas, comparáveis às geradas por eventos traumáticos no mundo físico. Estudos de neurociência cognitiva demonstram que experiências imersivas de alta fidelidade sensorial são processadas pelo cérebro de forma análoga a experiências reais, conferindo gravidade objetiva e subjetiva às violências praticadas em ambientes de realidade virtual (Bailenson, 2018). O caso do estupro coletivo do avatar de uma adolescente de 16 anos no Reino Unido — que apresentou sintomatologia traumática equivalente à de vítimas de violência sexual real — constitui evidência paradigmática dessa realidade, sendo expressamente mencionado na justificativa do Projeto de Lei n. 261/2024 (Brasil, 2024).

No campo das respostas institucionais, os organismos internacionais de segurança pública mais avançados — notadamente a Europol e a Interpol — têm desenvolvido estratégias de policiamento específicas para o metaverso, incluindo a criação de grupos especializados, a publicação de relatórios técnicos e a elaboração de recomendações operacionais para as forças policiais nacionais. O conceito de policiamento híbrido (LOFTUS, 2024), segundo o qual os agentes de segurança devem ser treinados para atuar de forma integrada em ambientes físicos e virtuais, emerge como modelo operacional promissor para o enfrentamento dos metacrimes. No Brasil, as iniciativas legislativas em curso — o Projeto de Lei n. 2.175/2023, que propõe o Marco Regulatório do Metaverso, e o Projeto de Lei n. 261/2024, que visa tipificar a violência psicológica em ambiente de realidade virtual — representam avanços normativos relevantes, ainda que insuficientes para abarcar a complexidade e a diversidade dos metacrimes já documentados pela literatura especializada.

A análise das questões jurisdicionais revelou que a natureza transnacional e descentralizada do metaverso constitui um dos maiores obstáculos ao combate efetivo à criminalidade nesse ambiente. Os critérios tradicionais de jurisdição territorial mostram-se

estruturalmente inadequados para regular condutas que se consumam em espaços virtuais sem localização física definida, envolvendo autores e vítimas situados em países distintos. A adesão do Brasil à Convenção de Budapeste sobre o Crime Cibernético, formalizada pelo Decreto n. 11.491/2023, representa passo fundamental na construção de mecanismos de cooperação internacional para o enfrentamento dessa lacuna operacional, mas sua efetividade dependerá da capacitação tecnológica e institucional das forças policiais brasileiras para produzir provas digitais admissíveis em âmbito transnacional (Fiorillo; Conte, 2016; Wendt; Jorge, 2012).

Quanto aos objetivos específicos, todos foram alcançados. O primeiro — identificar e categorizar os tipos de crimes mais frequentemente relatados no metaverso — foi cumprido pela sistematização das taxonomias da Europol (2022) e da Interpol (2024), complementadas pelos achados da literatura acadêmica especializada. O segundo — analisar os fatores estruturais do ambiente metaversal que potencializam a ocorrência de condutas ilícitas — foi atendido pela análise das características técnicas e sociais que favorecem a criminalidade: o anonimato dos usuários, a escalabilidade dos crimes digitais, a vulnerabilidade emocional gerada pela imersividade, a coleta intensiva de dados biométricos e a ausência de marcos regulatórios consolidados. O terceiro — avaliar as estratégias e os mecanismos institucionais de atuação policial para a prevenção e a repressão dos metacrimes — foi contemplado pela análise crítica das recomendações operacionais da Europol (2022) e da Interpol (2024), bem como pela discussão das iniciativas legislativas brasileiras em curso.

Do ponto de vista das contribuições, o presente estudo oferece três aportes principais ao campo da criminologia digital e da segurança pública. Primeiro, sistematiza e articula para o contexto brasileiro o estado da arte internacional sobre os metacrimes, produzindo um quadro analítico integrado que pode servir de referência para pesquisadores, operadores do direito e formuladores de políticas públicas de segurança. Segundo, demonstra que o enfrentamento eficaz dos metacrimes requer abordagem multidisciplinar e coordenada, que supere a fragmentação entre os campos do direito penal, da criminologia, da tecnologia da informação e das políticas de segurança pública. Terceiro, mapeia as lacunas normativas e operacionais existentes no sistema de segurança pública brasileiro para o enfrentamento dos metacrimes, oferecendo subsídios concretos para o aperfeiçoamento da legislação, da formação policial e das estratégias institucionais de prevenção e repressão.

Como principal limitação do estudo, reconhece-se a escassez de literatura científica nacional sobre o tema, fato que restringiu a análise das dimensões especificamente brasileiras do fenômeno e que evidencia, por si só, a urgência de ampliar o investimento acadêmico

nesse campo. A produção científica brasileira sobre metacrimes e segurança pública no metaverso é ainda incipiente, concentrando-se predominantemente em abordagens de direito digital e tecnologia da informação, com escassa atenção às perspectivas criminológica e de segurança pública. Outra limitação reside na velocidade de evolução do objeto de estudo: dado o ritmo acelerado de desenvolvimento tecnológico do metaverso, parte dos dados e das recomendações disponíveis na literatura pode ter sido superada por desenvolvimentos posteriores à realização desta pesquisa.

Diante das lacunas identificadas, propõe-se uma agenda de pesquisa futura estruturada em quatro eixos prioritários. O primeiro diz respeito à investigação empírica dos impactos psicológicos e vitimológicos dos metacrimes sobre usuários brasileiros, incluindo estudos de caso, análise de laudos periciais e pesquisas de prevalência que permitam dimensionar a magnitude do problema no país. O segundo refere-se ao mapeamento das capacidades institucionais das polícias brasileiras — civil, militar e federal — para o enfrentamento da criminalidade no metaverso, abrangendo a avaliação dos currículos das academias de polícia, dos equipamentos disponíveis e dos protocolos de investigação existentes. O terceiro concerne ao estudo comparado dos marcos regulatórios do metaverso em diferentes países, com vistas a identificar as melhores práticas internacionais adaptáveis ao contexto jurídico-institucional brasileiro. O quarto eixo diz respeito à investigação dos efeitos de retroalimentação entre o comportamento virtual e o comportamento real, avaliando em que medida a exposição a valores, atitudes e experiências violentas no metaverso influencia a conduta dos usuários em suas vidas fora desse ambiente.

Em síntese, a presente pesquisa demonstrou que o metaverso constitui uma nova e complexa fronteira para a segurança pública, que desafia as estruturas normativas, operacionais e institucionais tradicionais do direito penal e das forças de segurança. Os metacrimes não são fenômenos abstratos ou meramente virtuais: produzem danos reais, afetam pessoas físicas reais e demandam respostas jurídicas e institucionais igualmente reais e eficazes. A construção de um ambiente metaversal seguro, ético e juridicamente governado exige o engajamento coordenado de pesquisadores, legisladores, operadores do direito, forças de segurança pública, empresas de tecnologia e sociedade civil, orientado por um compromisso firme com a proteção dos direitos fundamentais dos usuários no espaço digital imersivo.

A urgência desse compromisso é tanto maior quanto mais acelerada se mostra a expansão do metaverso: o descompasso entre o ritmo de desenvolvimento tecnológico e a velocidade de resposta das instituições jurídicas e de segurança não pode ser aceito como

fatalidade, mas deve ser enfrentado com rigor científico, criatividade institucional e determinação ética, garantindo que os direitos e a dignidade das pessoas sejam protegidos também — e especialmente — nos novos territórios digitais do século XXI.

REFERÊNCIAS

ALMEIDA, J. J. de. *et al.* Crimes Cibernéticos. **Ciências Humanas e Sociais Unit**. Aracaju, v. 2, n. 3, p. 215-236, mar., 2015.

ASCENSÃO, José de Oliveira. **O Direito:** introdução e teoria geral. 11. ed. Lisboa: Fundação Calouste Gulbenkian, 2014.

AZUMA, Ronald T. A survey of augmented reality. **Presence:** Teleoperators & Virtual Environments, 6 (4), ago., 1997, 355-385. Disponível em: https://www.cs.unc.edu/~azuma/ARpresence.pdf. Acesso em: 18 out. 2024.

BACKES, Luciana; SCHLEMMER, Eliane. Metaversos: novos espaços para construção do conhecimento. **Revista Diálogo Educacional,** v. 8, n. 24, p. 519-532, 2008.

BAILENSON, Jeremy N. **Experience on Demand:** What Virtual Reality Is, How It Works, and What It Can Do. New York: W. W. Norton & Company, 2018.

BALL, Matthew. **The Metaverse:** What It Is, Where to Find It, and Who Will Build It. MatthewBall.vc, 2021. Disponível em: https://www.matthewball.vc/all/themetaverse. Acesso em: 18 out. 2024.

BARDIN, Laurence**. Análise de Conteúdo.** Tradução de Luís Antero Reto e Augusto Pinheiro. São Paulo: Edições 70, 2016.

BERNERS-LEE, TIM. **The World Wide Web:** A Very Short History. 1996.

BOVENZI, Gian. Marco. MetaCrimes: Criminal accountability for conducts in the Metaverse. **Companion Proceedings of the ACM Web Conference 2023,** *p.* 13–20. Disponível em: https://dl.acm.org/doi/pdf/10.1145/3543873.3587535. Acesso em: 08 nov. 2024

BRASIL. Senado Federal. **Projeto de Lei nº 261, de 2024**. Altera o Código Penal para tipificar o crime de violência psicológica em ambiente de realidade virtual. Autoria do Senador Veneziano Vital do Rêgo. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162040. Acesso em: 08 nov. 2024

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2175, de 2023.** Dispõe sobre o marco regulatório do metaverso e estabelece princípios, diretrizes e normas para o uso e a realização de negócios jurídicos nesse ambiente virtual. Autoria do Deputado Rubens Pereira Júnior. Disponível em: https://www.camara.leg.br/propostas-legislativas/2358606. Acesso em: 8 nov. 2024.

BRENNER, Suzan W. **Cybercrime and the Law:** Challenges, Issues, and Outcomes. Northeastern University Press, 2012

CLOUGH, Jonathan. **Principles of Cybercrime.** 2. ed. Cambridge University Press, 2010. Disponível em: chrome-

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://assets.cambridge.org/97811070/34570/frontmatter/9781107034570_frontmatter.pdf. Acesso em: 18 out. 2024.

COSTA, Rosmeri Ceconi. **A interação em mundos digitais virtuais em 3 dimensões**: uma investigação sobre a representação do emocionar na aprendizagem. 2008. 181f. Dissertação (Mestrado em Educação). Programa de Pós-Graduação em Educação, Universidade do Vale do Rio dos Sinos, São Leopoldo, 2008.

CAMPOS, Fabrício Calvete. **Qual é o metaverso, o futuro da convivência humana?** 2022. Disponível em: https://professorcalvete.com.br/2022/01/20/qual-e-o-metaverso-o-futuro-da-convivencia-humana/. Acesso em: 04. nov. 2024.

CANADÁ. Metacrime in the Metaverse. **NCFA,** National Crowdfunding & Fintech Associattion, 31. jan. 2024. Disponível em: https://ncfacanada.org/metacrime-in-the-metaverse/. Acesso em: 03 abr. 2024.

CASTRONOVA, Edward. **Synthetic Worlds:** The Business and Culture of Online Games. University of Chicago Press, 2005.

CLOUGH, Jonathan. Principles of Cybercrime. 2. ed. Cambridge: Cambridge University Press, 2015.

CONSELHO DA EUROPA. Convenção sobre o Crime Cibernético (Convenção de Budapeste). Budapeste, 23 nov. 2001. Disponível em: https://rm.coe.int/1680081561. Acesso em: 08 nov. 2024.

COSTA, Rosmeri Ceconi. A interação em mundos digitais virtuais em 3 dimensões: uma investigação sobre a representação do emocionar na aprendizagem. 2008. 181 f. Dissertação (Mestrado em Educação) — Universidade do Vale do Rio dos Sinos, São Leopoldo, 2008.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

DENZIN, Norman K.; LINCOLN, Yvonna S. (org.). **O planejamento da pesquisa qualitativa: teorias e abordagens.** 2. ed. Porto Alegre: Artmed, 2006.

DIONISIO, John David Dionísio; BURNS III, William G.; GILBERT, Richard. *3D* Virtual Worlds and the Metaverse. **ACM Computing Surveys,** vol. 45, n.3, article 34, jun. 2013. Disponível em?: chrome-extensi-on://efaidnbmnnnibpcajpcglclefindmkaj/https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1004&context=cs_fac. Acesso em 18 out. 2024.

EUROPOL. Observatório do Europol Innovation Lab. **Policing in the metaverse:** what law enforcement needs to know. 2022. Disponível em: https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know. Acesso em 21. Nov. 2024.

FAVERO, Bruno de Oliveira; FAVERO, Altamiro de Oliveira. **Cibercriminologia:** os meios eletrônicos e o policiamento em ambientes digitais. 1. ed. Jundiaí: Paco Editorial, 2021.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital**: e a sociedade da informação. 2 ed. São Paulo: Saraiva, 2016.

FURNELL, Steven; SPAFFORD, Eugene H. The Morris Worm at 30. **ITNOW**, vol. 61, n. 1, fev. 2019, Pages 32–33. Disponível em: https://academic.oup.com/itnow/article-abstract/61/1/32/5318113?redirectedFrom=fulltext. Acesso em: 18 out. 2024.

GIBSON, William. **Neuromancer.** New York: Ace Books, 1984.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo: Atlas, 2002. Disponível em: chrome-extensi-on://efaidnbmnnnibpcajpcglclefindmkaj/https://files.cercomp.ufg.br/weby/up/150/o/Anexo_C1_como_elaborar_projeto_de_pesquisa_-_antonio_carlos_gil.pdf. Acesso em: 18 out. 2024.

GOODMAN, Mar**. Future Crimes**: Inside the Digital Underground and the Battle for Our Connected World. Doubleday, 2015

GRAND VIEW RESEARCH. Metaverse Market Size, Share & Trends Analysis Report. San Francisco: **Grand View Research**, 2023. Disponível em: https://www.grandviewresearch.com/industry-analysis/metaverse-market-report. Acesso em: 18 out. 2024.

GROSSI, Márcia Gorett Ribeiro (org.). **Neurociência cognitiva, inteligência artificial e e-ducação:** caminhos e desafios. 1. ed.. Goiânia: Ed. Alta Performance, 2024.

GUIMARÃES, Ueudison Alves; SILVA, Fabianny Mayre da; SILVA, Cicera Alindomaria Monteiro. Metaverso na educação: oportunizando a inovação pedagógica. **RECIMA21** - Ciências Exatas e da Terra, Sociais, da Saúde, Humanas e Engenharia/Tecnologia, v. 3, 2022, n.9. Disponível em: file:///C:/Users/PCMG/Downloads/1932+-+METAVERSO+NA+EDUCA%C3%87%C3%83O+-+OPORTUNIZANDO+A+INOVA%C3%87%C3%83O+PEDAG%C3%93GICA.pdf. Acesso em: 18 out. 2024.

HAMMERSLEY, Martyn; ATKINSON, Paul. **Ethnography: Principles in practice.** London: Tavistock, 1983. Disponível em: file:///C:/Users/PCMG/Downloads/MartynHammersleyPaulAtkinson-Ethnography_PrinciplesinPractice-Routledge2007.pdf. Acesso em: 18 out. 2024.

HOLT, Thomas. J.; BOSSLER, Adam M.; SEIGFRIED-SPELLAR, Katherine C. **Cybercrime and Digital Forensics:** An Introduction. Routledge. 2015.

INTERPOL. **Metaverse:** a law enforcement perspective - Use Cases, Crime, Forensics, Investigation, and Governance. White Paper, jan. 2024. Disponível em: file:///C:/Users/PCMG/Downloads/Metaverse%20-%20a%20law%20enforcement%20perspective%20(1).pdf. Acesso em: 18 out. 2024.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos.** São Paulo: Saraiva, 2016

LOFTUS, Bethan. (2024). Reimagining Policing in the Digital Age: Hybrid Policing in the Virtual and Physical. **Blueline** Canada's Law Enforcement Magazine. Disponível em: https://www.blueline.ca/re-imagining-policing-for-the-digital-age-6008/. Acesso em: 07 nov. 2024.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica.** 6. ed. São Paulo: Atlas, 2003.

MARLER, Timothy *et al*. **The Metaverse and homeland security:** opportunities and risks of persistent virtual environments. Santa Monica: RAND Corporation, 2023. Disponível em: https://www.rand.org/pubs/perspectives/PEA2217-2.html. Acesso em: 01. abr. 2024.

MARSHALL, Angus McKenzie; TOMPSETT, Brian Charles. O metaverso — Não é uma nova fronteira para o crime. **Wiley Interdisciplinary Reviews:** Forensic Science. 29 set. 2023 Disponível em: https://wires.onlinelibrary.wiley.com/doi/pdf/10.1002/wfs2.1505. Acesso em: 08 nov. 2024.

MINAYO, Maria Cecília de Souza; *et al*. (org.). **Pesquisa social:** teoria, método e criatividade. 18. ed. Petrópolis: Ed. Vozes, 2001.

MILGRAM, Paul; KISHINO, Fumio. A taxonomy of mixed reality visual displays. **IEICE** Transactions on Information and Systems, vol. 77, n. 12, dez. 1994, 1321-1329. Disponível em: https://www.researchgate.net/publication/231514051_A_Taxonomy_of_Mixed_Reality_Visual_Displays. Acesso em: 18 ago. 2024.

NAKAMOTO, Satoshi. Bitcoin: **A peer-to-peer electronic cash system**. Bitcoin White Paper, 2008. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://bitcoin.org/bitcoin.pdf. Acesso em: 18 out. 2024.

NASH, Eric B. *et. al.* A Review of Presence and Performance in Virtual Environments. **International Journal of Human-Computer Interaction**, 12 (1), 1-41, 2000. Disponível em: https://www.researchgate.net/publication/220302125_A_Review_of_Presence_and_Performance_in_Virtual_Environments. Acesso em: 18 out. 2024.

RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence:** a modern approach. 3. ed. Prentice Hall, 2021.

SCHROEDER, Ralph. **Social Theory after the Internet:** Media, Technology, and Globalization. UCL Press, 2018;

SHIRKY, Clauy. **Here Comes Everybody:** The Power of Organizing Without Organizations. Penguin Press, 2008

SIDDAWAY, Andy P.; WOOD, Alex M.; HEDGES, Larry. V. How to do a systematic review: a best practice guide for conducting and reporting narrative reviews, meta-analyses, and meta-syntheses. **Annual Review of Psychology**, v. 70, n. 1, p. 747–770, 2019. Disponível em: https://pubmed.ncbi.nlm.nih.gov/30089228/. Acesso em 18 out 2024.

SILVA, Jefferson David dos Anjos. LIMA, Maria Vitória Ribas de Oliveira. Os principais cibercrimes praticados no Brasil. **V CONEDU** – Congresso Nacional de Educação. 2018.

STEPHENSON, Neal. **Snow Crash.** New York: Bantam Books, 1992.

STOLL, Clifford. **The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.** New York: Doubleday, 1989.

SUM *OF US*. **Metaverse:** another cesspool of toxic content. 2022. Disponível em: https://www.eko.org/images/Metaverse_report_May_2022.pdf. Acesso em: 11 nov. 2024

SYDOW, Toth Spencer. **Curso de Direito Penal Informático:** Partes Geral e Especial. Salvador: Editora JusPodivm, 2022.

TIBÚRCIO, Flávia; *et al*. **O futuro do digital está na conexão com o real:** Metaverso e suas implicações sociais e tecnológicas. 2022. Disponível em: https://sol.sbc.org.br/index.php/wics/article/view/20733/20560. Acesso em: 18 out. 2024.

TZU, S. **A Arte da Guerra.** São Paulo: Record, 2006.

WALL, David S. ***C*ybercrime:** The Transformation of Crime in the Information *Age*. Polity Press, 2007.

WEF. World Economic Forum. ***Global Risks Report 2023.*** 11 jan. 2023. Disponível em: https://www.weforum.org/publications/global-risks-report-2023/in-full/. Acesso em: 08 nov. 2024.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**: Ameaças e Procedimentos de Investigação. Rio de Janeiro: Brasport, 2012.

YIN, Robert K. Pesquisa qualitativa do início ao fim. Tradução de Daniel Bueno. Porto Alegre: Penso, 2016.