UNIVERSIDADE FEDERAL DE MINAS GERAIS
Faculdade de Direito
Bacharelado em Ciências do Estado

Maria Eduarda Gazire de Abreu

CRIMINOLOGIA DIGITAL:
Perfis e fatores criminológicos por trás de delitos virtuais, crimes de ódio nas redes e impactos da LGPD

Belo Horizonte
2026

Maria Eduarda Gazire de Abreu

CRIMINOLOGIA DIGITAL:
Perfis e fatores criminológicos por trás de delitos virtuais, crimes de ódio nas redes e impactos da LGPD

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Federal de Minas Gerais como requisito parcial para obtenção de título de Bacharel em Ciências do Estado.

Orientador: Prof. Dr. Carlos Augusto Canêdo Gonçalves da Silva.

Belo Horizonte
2026

TRABALHO DE CONCLUSÃO DE CURSO

ATA DE DEFESA

No _____dia do mês de ____do ano de 20__, o/a **discente** _____, matriculado (a) sob o número de Registro Acadêmico _____, defendeu o Trabalho de Conclusão de Curso intitulado **"**_____**"**, tendo obtido a média __(_____).

Participaram da banca examinadora os membros abaixo indicados, que, por nada mais terem a declarar, assinam e datam a presente ata, a ser arquivada na pasta do (a) discente.

Belo Horizonte, ____de _____de 20___.

Orientador: _____, Nota ___(_____)

Examinador: _____, Nota ___(_____)

Examinador: _____*, Nota* ___*(*_____*)*

Aos meus pais,
Eduardo e Maria de Lourdes,
que foram o solo fértil
para que minha semente germinasse.

"O ciberespaço encoraja um estilo de relacionamento quase independente dos lugares geográficos (telecomunicações e telepresença) e da coincidência dos tempos (comunicação assíncrona) (...) a extensão do ciberespaço acompanha e acelera uma virtualização geral da economia e da sociedade"

Pierre Levy.

RESUMO

A crescente digitalização das relações sociais produziu profundas transformações nas dinâmicas de interação humana, circulação de informações e manifestação da criminalidade. Nesse contexto, surgem novos desafios para a criminologia, especialmente diante da expansão dos delitos virtuais, da disseminação de crimes de ódio nas redes sociais e das tensões decorrentes da proteção de dados pessoais em sociedades altamente conectadas. O presente trabalho tem por objetivo analisar criticamente os perfis e fatores criminológicos associados à criminalidade digital, investigando de que maneira as transformações tecnológicas influenciam a produção de comportamentos criminosos, os processos de radicalização online e a atuação dos mecanismos de controle social. Inicialmente, examina-se a evolução da criminologia diante da sociedade digital, com destaque para as contribuições das teorias da associação diferencial de Edwin H. Sutherland e da anomia de Robert K. Merton. Em seguida, analisa-se a influência das plataformas digitais, dos algoritmos de recomendação e do denominado capitalismo de vigilância. Posteriormente, investigam-se os crimes de ódio praticados em ambientes digitais, os fenômenos de polarização e radicalização online descritos por Cass Sunstein, bem como os desafios relacionados à liberdade de expressão e à responsabilização das plataformas digitais. Por fim, são examinados os impactos da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), especialmente no que se refere à proteção dos direitos fundamentais, aos limites da vigilância estatal e à compatibilização entre privacidade e persecução penal. Utilizando-se do método dedutivo e da pesquisa bibliográfica, conclui-se que a criminalidade digital não pode ser adequadamente compreendida apenas por fatores individuais relacionados ao infrator. As estruturas tecnológicas, os modelos econômicos das plataformas digitais e os mecanismos algorítmicos exercem influência significativa sobre a produção, disseminação e legitimação de comportamentos potencialmente criminosos. Conclui-se ainda que a proteção de dados pessoais representa instrumento indispensável à preservação das liberdades fundamentais na sociedade digital e que o enfrentamento da criminalidade virtual exige respostas interdisciplinares compatíveis com os princípios do Estado Democrático de Direito.

Palavras-chave: Criminologia Digital. Crimes de Ódio. Delitos Virtuais. Proteção de Dados. LGPD. Radicalização Online.

ABSTRACT

The growing digitalization of social relations has profoundly transformed human interaction, information circulation, and the manifestation of criminal behavior. In this context, new challenges arise for criminology, particularly regarding cybercrime, hate crimes on social media platforms, and the tensions associated with personal data protection in highly connected societies. This study aims to critically analyze the criminological profiles and factors related to digital criminality, investigating how technological transformations influence criminal behavior, online radicalization processes, and contemporary mechanisms of social control. Initially, the research examines the evolution of criminology in the digital age, emphasizing Edwin H. Sutherland's Differential Association Theory and Robert K. Merton's Anomie Theory. Subsequently, it analyzes the influence of digital platforms, recommendation algorithms, and the phenomenon known as surveillance capitalism. The study then investigates hate crimes committed in digital environments, the processes of online polarization and radicalization described by Cass Sunstein, and the challenges involving freedom of expression and platform accountability. Finally, it examines the impacts of the Brazilian General Data Protection Law (LGPD – Law No. 13,709/2018), particularly regarding the protection of fundamental rights, the limits of state surveillance, and the balance between privacy and criminal investigation. Using a deductive method and bibliographic research, the study concludes that digital criminality cannot be adequately explained solely by individual factors related to offenders. Technological structures, digital platform business models, and algorithmic mechanisms significantly influence the production, dissemination, and legitimization of potentially criminal behavior. It also concludes that personal data protection is an essential instrument for safeguarding fundamental freedoms in the digital age and that combating cybercrime requires interdisciplinary responses compatible with the principles of the Democratic Rule of Law.

Keywords: Digital Criminology. Hate Crimes. Cybercrime. Data Protection. LGPD. Online Radicalization.

SUMÁRIO

INTRODUÇÃO

A transformação tecnológica experimentada pela sociedade nas últimas décadas alterou profundamente as formas de comunicação, interação social, produção econômica e circulação de informações. O desenvolvimento da internet e a posterior consolidação das plataformas digitais produziram uma realidade caracterizada pela conectividade permanente, pela instantaneidade das comunicações e pela crescente dependência das tecnologias da informação. Nesse novo contexto, o ambiente digital deixou de representar mera ferramenta de comunicação para tornar-se um espaço central de convivência humana, capaz de influenciar comportamentos, opiniões e processos decisórios em escala global.

A expansão das tecnologias digitais trouxe consigo inúmeros benefícios sociais, econômicos e culturais. O acesso à informação tornou-se mais amplo, a comunicação passou a ocorrer em tempo real e novas oportunidades de desenvolvimento econômico surgiram a partir da digitalização das atividades produtivas. Entretanto, os mesmos instrumentos que ampliaram as possibilidades de interação humana também criaram condições favoráveis ao surgimento de novas formas de criminalidade.

Fraudes eletrônicas, invasões de sistemas informáticos, vazamentos de dados pessoais, ataques cibernéticos, perseguições virtuais, campanhas coordenadas de desinformação e crimes de ódio praticados em redes sociais passaram a integrar a realidade cotidiana das sociedades contemporâneas. Paralelamente, fenômenos como radicalização política, extremismo digital e manipulação algorítmica passaram a despertar crescente preocupação entre pesquisadores, autoridades públicas e organismos internacionais.

Diante desse cenário, tornou-se evidente que a compreensão da criminalidade contemporânea exige a superação de modelos analíticos construídos para uma realidade predominantemente analógica. Embora as teorias criminológicas clássicas continuem oferecendo importantes contribuições para a compreensão do comportamento criminoso, diversos fenômenos observados na sociedade digital revelam características que desafiam explicações centradas exclusivamente no indivíduo.

A internet não apenas criou novas oportunidades para a prática de delitos. Ela transformou os próprios mecanismos de socialização, aprendizagem e interação humana. Fóruns digitais, redes sociais, aplicativos de mensagens instantâneas e plataformas de compartilhamento de conteúdo passaram a desempenhar papel relevante na formação de identidades, crenças e comportamentos. Como consequência, fatores tecnológicos passaram a exercer influência significativa sobre a produção e reprodução da criminalidade.

Nesse contexto, emerge a denominada Criminologia Digital, campo de estudos voltado

à análise das relações entre tecnologia, comportamento humano e criminalidade. Diferentemente das abordagens tradicionais, a criminologia digital procura compreender de que forma os ambientes virtuais influenciam a prática de delitos, os processos de vitimização e os mecanismos contemporâneos de controle social.

A relevância desse debate torna-se ainda maior quando se observa o crescimento dos crimes de ódio praticados nas redes sociais. O ambiente digital ampliou significativamente o alcance de discursos discriminatórios direcionados a grupos definidos por critérios raciais, religiosos, étnicos, políticos ou relacionados à orientação sexual e identidade de gênero. A velocidade de circulação das informações e os mecanismos algorítmicos de recomendação potencializam a disseminação dessas mensagens, criando condições favoráveis à radicalização e ao fortalecimento de comunidades extremistas.

Ao mesmo tempo, a consolidação da economia digital intensificou a coleta e o tratamento de dados pessoais por empresas privadas e instituições públicas. A informação passou a ocupar posição estratégica na organização econômica contemporânea, transformando-se em um dos ativos mais valiosos da sociedade em rede. Como consequência, surgiram novas preocupações relacionadas à privacidade, à vigilância digital e à proteção dos direitos fundamentais.

Nesse contexto, a promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) representou um importante marco regulatório destinado a estabelecer limites jurídicos para a coleta, utilização e compartilhamento de informações pessoais. Contudo, a proteção de dados também passou a gerar novas discussões relacionadas à investigação criminal, ao monitoramento digital e aos limites da atuação estatal no combate à criminalidade virtual.

Diante dessas transformações, o presente trabalho busca responder ao seguinte problema de pesquisa: em que medida os delitos virtuais, os crimes de ódio praticados nas redes sociais e os desafios relacionados à proteção de dados pessoais exigem uma reformulação dos paradigmas criminológicos tradicionais?

Parte-se da hipótese de que a criminalidade digital não pode ser adequadamente compreendida apenas a partir das características individuais dos infratores. Sustenta-se que os próprios ambientes digitais, os mecanismos algorítmicos, a economia da atenção e o modelo econômico baseado na exploração de dados pessoais atuam como fatores criminógenos relevantes, influenciando comportamentos, ampliando oportunidades delitivas e favorecendo processos de radicalização.

O objetivo geral da pesquisa consiste em analisar criticamente os fatores

criminológicos associados aos delitos virtuais, aos crimes de ódio nas redes sociais e aos impactos da Lei Geral de Proteção de Dados na sociedade contemporânea.

Como objetivos específicos, pretende-se examinar a evolução da criminologia diante da sociedade digital; identificar os principais fatores criminológicos relacionados à prática de crimes virtuais; analisar os processos de radicalização online e disseminação do discurso de ódio; investigar a influência dos algoritmos na amplificação de comportamentos desviantes; e avaliar os impactos da proteção de dados pessoais para a persecução penal e para a preservação dos direitos fundamentais.

A pesquisa adota o método dedutivo e utiliza como principal técnica a revisão bibliográfica, com análise de obras relacionadas à criminologia, sociologia, proteção de dados, teoria do controle social e estudos sobre tecnologia. Também serão examinadas legislações, documentos institucionais e precedentes judiciais relevantes para a compreensão do tema.

A relevância do estudo justifica-se pela crescente centralidade da tecnologia nas relações sociais contemporâneas e pela necessidade de compreender como as transformações digitais influenciam a criminalidade, os mecanismos de controle social e a proteção das liberdades fundamentais. Em uma sociedade cada vez mais orientada por algoritmos e sistemas de processamento de dados, torna-se indispensável refletir criticamente sobre os limites do poder tecnológico e sobre os desafios impostos ao Estado Democrático de Direito.

Assim, a presente pesquisa pretende contribuir para a construção de uma abordagem criminológica compatível com as exigências da era digital, capaz de compreender não apenas quem pratica os delitos virtuais, mas também quais estruturas sociais, econômicas e tecnológicas influenciam sua ocorrência.

CAPÍTULO I – Criminologia digital e a transformação do fenômeno criminal

1.1 Da criminologia clássica à sociedade digital

A compreensão científica do crime sempre esteve intimamente relacionada ao contexto histórico, econômico e social em que se desenvolveu cada teoria criminológica. O fenômeno criminal não constitui uma realidade estática; ao contrário, sofre constantes transformações em razão das mudanças estruturais experimentadas pelas sociedades. Por essa razão, a criminologia, enquanto ciência empírica voltada ao estudo do crime, do criminoso, da vítima e dos mecanismos de controle social, precisou adaptar seus referenciais teóricos ao longo do tempo para compreender novas formas de manifestação da criminalidade.

As primeiras formulações sistemáticas sobre o crime surgiram ainda no contexto do Iluminismo, especialmente a partir da obra de Cesare Beccaria, “Dos Delitos e das Penas” (1764), o autor procurou racionalizar o sistema penal, criticando arbitrariedades e defendendo limites ao poder punitivo do Estado. A criminalidade era compreendida como resultado do exercício do livre-arbítrio por indivíduos capazes de avaliar racionalmente os custos e benefícios de suas ações.

A Escola Clássica possuía, portanto, uma concepção fortemente individualista do comportamento criminoso. O delito era visto como fruto de uma decisão consciente e racional tomada pelo agente. Consequentemente, a prevenção criminal deveria ocorrer por meio da certeza da punição e não de sua severidade.

Embora essa perspectiva continue exercendo influência significativa sobre os sistemas penais contemporâneos, sua capacidade explicativa mostra-se limitada diante de fenômenos complexos observados na sociedade digital. Diversos comportamentos praticados em ambientes virtuais não decorrem exclusivamente de decisões individuais plenamente racionais, mas também da influência de fatores tecnológicos, grupais e comunicacionais que alteram a percepção dos riscos e das consequências associados à prática criminosa.

No final do século XIX, a Escola Positivista promoveu importante mudança de paradigma ao deslocar o foco da análise para as características do próprio infrator. Cesare Lombroso, em “*L'Uomo Delinquente”* (1876), sustentou que determinados indivíduos apresentariam predisposições biológicas para a criminalidade. Posteriormente, Enrico Ferri em sua obra “*Sociologia Criminale*” (1892) ampliou essa compreensão ao incorporar fatores sociais e ambientais à análise criminológica.

Apesar de sua relevância histórica, as explicações positivistas também encontram limitações evidentes diante da criminalidade contemporânea. Os delitos virtuais frequentemente são praticados por indivíduos plenamente integrados à sociedade, com

elevado nível educacional e significativa capacidade técnica. A figura do cibercriminoso desafia diversos estereótipos tradicionalmente associados ao comportamento desviante.

Essa percepção foi antecipada por Edwin H. Sutherland ao desenvolver suas pesquisas sobre os chamados crimes de colarinho branco. Em "*White Collar Crime"* (1949), o autor criticou a tendência da criminologia tradicional de concentrar suas análises sobre indivíduos pertencentes às classes socialmente marginalizadas, ignorando práticas ilícitas desenvolvidas por pessoas economicamente privilegiadas.

Sutherland afirma:

> "(...) as concepções e explicações acerca do crime que acabaram de ser descritas são equivocadas e incorretas; que a criminalidade, na realidade, não está estreitamente correlacionada à pobreza nem às condições psicopáticas e sociopáticas associadas à pobreza; e que uma explicação adequada do comportamento criminoso deve seguir direções bastante distintas. As explicações convencionais são inválidas principalmente porque se baseiam em amostras enviesadas. Essas amostras são enviesadas porque não incluem amplas áreas da conduta criminosa praticada por indivíduos que não pertencem às classes inferiores." (SUTHERLAND, 1940, p. 02, tradução própria)

A ascensão da criminalidade digital reforça essa constatação. Ataques cibernéticos sofisticados, fraudes eletrônicas complexas e esquemas de manipulação digital frequentemente exigem elevado grau de conhecimento técnico e capacidade organizacional, distanciando-se das representações tradicionais do criminoso construídas pela criminologia clássica e positivista.

Paralelamente à evolução das teorias criminológicas, a própria sociedade passou por transformações estruturais profundas. A Revolução Industrial alterou as formas de produção econômica e organização social. Posteriormente, a revolução tecnológica promovida pela informática e pela internet inaugurou um novo paradigma civilizatório.

Nesse contexto, destaca-se a contribuição de Manuel Castells:

> "(...) o processo atual de transformação tecnológica expande-se exponencialmente em razão de sua capacidade de criar uma interface entre campos tecnológicos mediante uma linguagem digital comum na qual a informação é gerada, armazenada, recuperada, processada e transmitida. Vivemos em um mundo que, segundo Nicholas Negroponte, se tornou digital. " (CASTELLS, 1999, p. 68)

Segundo Castells, a principal característica da sociedade contemporânea não reside apenas na presença da tecnologia, mas na forma como ela reorganiza relações de poder, processos econômicos e mecanismos de comunicação.

A informação transforma-se em recurso estratégico, enquanto as redes digitais passam a desempenhar papel central na estruturação das relações sociais. Essa transformação possui profundas implicações criminológicas.

A criminalidade deixa de estar necessariamente vinculada a espaços físicos determinados e passa a desenvolver-se em ambientes digitais que transcendem fronteiras territoriais. A internet permite que indivíduos localizados em diferentes países interajam instantaneamente, compartilhem informações e desenvolvam atividades coordenadas.

Como consequência, surgem novas formas de criminalidade e novos desafios para os sistemas jurídicos tradicionais.

A própria noção de local do crime torna-se mais complexa. Em muitos casos, autor, vítima, servidor utilizado na prática da infração e resultado produzido encontram-se situados em diferentes países, dificultando a aplicação dos mecanismos tradicionais de investigação e persecução penal.

Além disso, o ambiente digital modifica significativamente as relações entre anonimato e responsabilidade.

Embora a internet não proporcione anonimato absoluto, ela frequentemente produz nos usuários uma sensação subjetiva de invisibilidade e impunidade. Essa percepção influencia comportamentos e reduz barreiras psicológicas associadas à prática de determinadas condutas ilícitas.

O fenômeno foi analisado por John Suler em seu artigo “The Online Disinhibition Effect*”* (2004):

> “Usuários comuns da Internet — assim como clínicos e pesquisadores — observaram que as pessoas dizem e fazem no ciberespaço coisas que normalmente não diriam nem fariam no mundo das interações presenciais. Elas se tornam mais desinibidas, sentem-se menos contidas e se expressam de maneira mais aberta. Tão difundido é esse fenômeno que surgiu uma expressão específica para designá-lo: o efeito de desinibição online. “ (SULER, 2004, p. 01, tradução própria)

A chamada “desinibição online” constitui um dos elementos centrais para a compreensão da criminalidade digital contemporânea.

A sociedade digital não transformou apenas os instrumentos utilizados para a prática de crimes. Ela alterou os próprios processos de socialização, interação e construção identitária que influenciam o comportamento humano.

Nesse cenário, torna-se evidente a necessidade de desenvolver novos referenciais teóricos capazes de compreender a criminalidade para além dos limites tradicionalmente estabelecidos pela criminologia clássica.

É justamente dessa necessidade que emerge a denominada Criminologia Digital, campo de estudos dedicado à análise das relações entre tecnologia, comportamento humano e fenômenos criminais na sociedade em rede.

A criminologia digital não rejeita as contribuições das teorias anteriores. Pelo contrário, busca reinterpretá-las à luz das transformações produzidas pela revolução tecnológica, incorporando elementos relacionados aos ambientes digitais, aos algoritmos, à circulação de informações e às novas formas de controle social.

A compreensão desses fenômenos constitui requisito indispensável para o enfrentamento dos desafios impostos pela criminalidade contemporânea e para a construção de políticas públicas compatíveis com as exigências do Estado Democrático de Direito na era digital.

1.2 O surgimento da criminologia digital

O desenvolvimento acelerado das tecnologias da informação e comunicação produziu transformações tão profundas nas dinâmicas sociais contemporâneas que diversos campos do conhecimento passaram a reformular seus referenciais teóricos para compreender os novos fenômenos decorrentes da digitalização da vida cotidiana. A criminologia não permaneceu imune a esse processo. O crescimento exponencial da internet, das redes sociais, dos dispositivos móveis e das plataformas digitais revelou a necessidade de construção de uma abordagem específica capaz de analisar os impactos da tecnologia sobre o crime, os criminosos, as vítimas e os mecanismos de controle social.

Foi nesse contexto que se consolidou aquilo que a literatura especializada passou a denominar Criminologia Digital (*Digital Criminology*). Embora não exista consenso absoluto sobre sua autonomia enquanto ramo específico da criminologia, há crescente reconhecimento de que a sociedade digital produziu desafios suficientemente distintos para justificar a construção de novos modelos analíticos.

Entre os principais estudiosos dessa temática destaca-se David S. Wall. Em sua obra "*Cybercrime: The Transformation of Crime in the Information Age"* (2024), Wall sustenta que o impacto da tecnologia sobre a criminalidade vai muito além do surgimento de novos instrumentos para a prática de delitos. Segundo o autor, a internet transformou a própria natureza do fenômeno criminal, alterando as formas de organização, execução e percepção social dos comportamentos ilícitos (WALL, 2024, p. 01, tradução própria).

A contribuição de Wall é importante, porque rompe com uma visão reducionista segundo a qual os crimes digitais representariam apenas uma versão tecnológica de infrações já existentes. Embora determinadas condutas realmente correspondam à adaptação de crimes tradicionais ao ambiente virtual, outras apresentam características inéditas que desafiam categorias jurídicas e criminológicas consolidadas.

A disseminação de *malwares*[1], os ataques de negação de serviço (DDoS)[2], a exploração de vulnerabilidades informáticas, a manipulação massiva de dados e a utilização de inteligência artificial para fins ilícitos constituem exemplos de práticas que dificilmente poderiam ser explicadas pelos modelos criminológicos desenvolvidos para uma realidade pré-digital.

Outra contribuição relevante para a construção da criminologia digital encontra-se nos trabalhos de Majid Yar. Em "*Cybercrime and Society"* (YAR, 2006, p. 13, tradução própria), o autor argumenta que os crimes praticados na internet exigem uma abordagem sociológica capaz de compreender simultaneamente as dimensões tecnológicas, culturais e institucionais envolvidas na produção do comportamento criminoso.

Para Yar, o ambiente digital não deve ser tratado apenas como um novo local onde crimes são praticados. Trata-se de um espaço social específico, dotado de características próprias, capaz de influenciar relações humanas, estruturas de poder e mecanismos de controle social (YAR, 2006, p. 21, tradução própria).

Essa percepção representa uma importante mudança de paradigma.

Tradicionalmente, a criminologia concentrava seus esforços na identificação das motivações individuais dos infratores. A criminologia digital, por sua vez, amplia o foco da análise para incluir as características dos próprios ambientes tecnológicos em que os comportamentos se desenvolvem.

Surge, assim, uma preocupação crescente com elementos como arquitetura das plataformas, algoritmos de recomendação, anonimato digital, cultura participativa e mecanismos de moderação de conteúdo.

A relevância dessa abordagem torna-se evidente quando se observa que muitos comportamentos ilícitos dependem diretamente das condições proporcionadas pelas tecnologias digitais.

A formação de comunidades extremistas, por exemplo, não pode ser explicada exclusivamente pelas características psicológicas dos indivíduos envolvidos. É necessário compreender como determinadas plataformas facilitam a comunicação entre grupos dispersos geograficamente, permitem a circulação de conteúdos radicais e favorecem processos de reforço ideológico mútuo.

Nesse aspecto, a criminologia digital aproxima-se das reflexões desenvolvidas por Manuel Castells acerca da sociedade em rede.

---

[1] Programa projetado para infectar dispositivos eletrônicos, roubar dados e causar danos.
[2] Tentativa cibernética maliciosa de tornar um site, servidor ou rede inacessível aos seus usuários legítimos.

Segundo Castells, a internet produziu uma profunda reorganização das estruturas sociais contemporâneas. Em vez de relações rigidamente hierarquizadas, observa-se a predominância de redes flexíveis e descentralizadas capazes de conectar indivíduos, instituições e organizações em escala global (CASTELLS, 1999, p. 566).

Essa nova configuração social possui implicações diretas para a criminalidade.

Grupos criminosos podem coordenar atividades transnacionais sem necessidade de estruturas organizacionais tradicionais. Comunidades virtuais permitem a troca instantânea de informações, técnicas e recursos. Redes digitais possibilitam a formação de vínculos sociais entre indivíduos que jamais se encontraram presencialmente.

Como consequência, o crime passa a assumir características compatíveis com a lógica da sociedade em rede.

A própria distinção entre espaço físico e espaço virtual torna-se progressivamente menos relevante.

Grande parte das atividades humanas contemporâneas ocorre simultaneamente em ambas as dimensões. Relações profissionais, afetivas, econômicas e políticas desenvolvem-se de forma híbrida, combinando interações presenciais e digitais.

Esse fenômeno também afeta a criminalidade.

Fraudes financeiras iniciadas em plataformas digitais podem produzir prejuízos patrimoniais concretos. Campanhas de desinformação disseminadas na internet podem influenciar processos eleitorais. Discursos de ódio publicados em redes sociais podem resultar em agressões físicas e violência real.

A fronteira entre o virtual e o real torna-se cada vez mais tênue.

Essa constatação levou diversos autores a questionarem a própria utilização da expressão “crime virtual”. Como observa Wall (WALL, 2024, p. 01, tradução própria), os efeitos produzidos pelos delitos praticados na internet são absolutamente reais, atingindo bens jurídicos concretos e produzindo consequências tangíveis para vítimas, instituições e sociedades inteiras.

Outro aspecto fundamental para a consolidação da criminologia digital refere-se à transformação dos mecanismos de controle social.

Plataformas digitais, empresas de tecnologia, desenvolvedores de algoritmos e provedores de serviços online passaram a exercer influência significativa sobre a produção e aplicação de normas comportamentais.

A remoção de conteúdos, a suspensão de perfis, a definição de políticas de uso e a moderação automatizada de informações passaram a desempenhar funções que

tradicionalmente eram associadas exclusivamente ao Estado.

Essa descentralização do controle social constitui uma das características mais marcantes da sociedade digital.

Ao mesmo tempo em que amplia possibilidades de participação e comunicação, ela também cria novos desafios relacionados à transparência, à responsabilidade e à proteção dos direitos fundamentais.

Por essa razão, a criminologia digital não se limita à análise dos delitos praticados na internet. Seu objeto de estudo abrange as transformações mais amplas produzidas pela tecnologia sobre os mecanismos de poder, vigilância, controle e regulação social.

Trata-se, portanto, de um campo de investigação que busca compreender não apenas quem pratica crimes no ambiente digital, mas também como as estruturas tecnológicas influenciam comportamentos, produzem oportunidades delitivas e redefinem os próprios limites entre legalidade, ilegalidade e controle social.

A consolidação dessa perspectiva representa um passo fundamental para a construção de respostas jurídicas e institucionais adequadas aos desafios impostos pela criminalidade contemporânea.

Contudo, para compreender plenamente os impactos da tecnologia sobre o fenômeno criminal, torna-se necessário examinar de forma mais aprofundada as características específicas do ciberespaço enquanto ambiente capaz de favorecer determinadas formas de comportamento desviante. É justamente essa análise que será desenvolvida no próximo tópico.

1.3 O ciberespaço como novo ambiente criminógeno

A compreensão da criminalidade digital exige a análise das características específicas do ambiente em que tais comportamentos se desenvolvem. Diferentemente dos espaços físicos tradicionalmente estudados pela criminologia, o ciberespaço apresenta atributos próprios que influenciam significativamente as oportunidades criminosas, os processos de tomada de decisão dos agentes e os mecanismos de controle social. Por essa razão, diversos pesquisadores passaram a sustentar que o ambiente digital não constitui apenas um novo local para a prática de delitos, mas um contexto social capaz de atuar como verdadeiro fator criminógeno.

A noção de fator criminógeno refere-se a elementos ou circunstâncias que favorecem a ocorrência de comportamentos criminosos. Tradicionalmente, a criminologia identificava tais fatores em aspectos econômicos, sociais, culturais ou psicológicos. Contudo, a ascensão da sociedade digital demonstrou que determinadas características tecnológicas também podem

influenciar a prática de infrações penais.

Uma das teorias criminológicas mais utilizadas para compreender esse fenômeno é a Teoria das Atividades Rotineiras (*Routine Activity Theory*), desenvolvida por Lawrence Cohen e Marcus Felson em artigo publicado em 1979. Segundo os autores, a ocorrência de um crime depende da convergência de três elementos fundamentais: um infrator motivado, uma vítima adequada e a ausência de mecanismos eficazes de vigilância ou controle (COHEN; FELSON, 1979, p. 589, tradução própria).

Embora originalmente formulada para explicar crimes patrimoniais em ambientes físicos, essa teoria revelou grande potencial explicativo para a criminalidade digital.

A internet ampliou significativamente o número de potenciais vítimas, disponibilizando enorme quantidade de informações pessoais e financeiras acessíveis por meios eletrônicos. Ao mesmo tempo, a velocidade das comunicações e a dimensão global das redes digitais dificultam a atuação dos mecanismos tradicionais de controle.

Consequentemente, a convergência entre infratores motivados, vítimas vulneráveis e ausência de vigilância efetiva torna-se mais frequente no ambiente digital.

Além disso, a própria arquitetura tecnológica das plataformas contribui para a ampliação das oportunidades criminosas.

Redes sociais, aplicativos de mensagens instantâneas e sistemas de compartilhamento de arquivos permitem que indivíduos estabeleçam contato com milhares de pessoas em poucos segundos, ampliando significativamente o alcance potencial de fraudes, golpes financeiros e campanhas de desinformação.

Outro aspecto particularmente relevante refere-se à percepção de anonimato proporcionada pela internet.

Embora especialistas em segurança digital frequentemente ressaltem que o anonimato absoluto praticamente não existe no ambiente virtual, diversos usuários experimentam uma sensação subjetiva de invisibilidade durante suas interações online.

Essa percepção influencia diretamente o comportamento humano. O chamado efeito de desinibição online possui enorme relevância criminológica. Muitas condutas relacionadas ao assédio virtual, aos discursos de ódio, ao *cyberbullying* e à disseminação de conteúdos ilícitos são facilitadas pela redução das barreiras psicológicas normalmente presentes nas interações presenciais. A ausência de contato direto com a vítima dificulta processos de empatia e aumenta a tendência à objetificação do outro.

Além disso, a velocidade das interações digitais frequentemente reduz o tempo disponível para reflexão crítica sobre as consequências das próprias ações.

Outro elemento que contribui para o caráter criminógeno do ciberespaço é a descentralização geográfica.

No ambiente físico, a prática de muitos delitos depende da proximidade espacial entre autor e vítima. Na internet, essa limitação praticamente desaparece.

Um indivíduo localizado em qualquer parte do mundo pode acessar sistemas informáticos, realizar fraudes financeiras, disseminar conteúdos ilícitos ou estabelecer contato com vítimas situadas em diferentes países.

Essa característica amplia significativamente o alcance potencial das atividades criminosas e dificulta os mecanismos tradicionais de investigação e persecução penal.

A transnacionalidade dos delitos virtuais constitui um dos principais desafios enfrentados pelos sistemas jurídicos contemporâneos.

A cooperação internacional frequentemente torna-se indispensável para identificação de autores, obtenção de provas e responsabilização criminal.

Entretanto, diferenças legislativas, limitações jurisdicionais e dificuldades operacionais frequentemente comprometem a efetividade dessas iniciativas.

Outro fenômeno relevante para a compreensão do ciberespaço como ambiente criminógeno é o desenvolvimento da chamada *Dark Web*[3].

A *Dark Web* corresponde a uma parcela da internet que não pode ser acessada por mecanismos convencionais de navegação e indexação. Seu funcionamento depende da utilização de tecnologias específicas destinadas a ampliar a privacidade e dificultar a identificação dos usuários.

Importa destacar que a *Dark Web* não possui natureza necessariamente ilícita. Diversos indivíduos utilizam essas ferramentas para proteger sua privacidade, evitar censura estatal ou exercer atividades legítimas em contextos politicamente repressivos.

Todavia, a mesma infraestrutura tecnológica também favorece o desenvolvimento de mercados ilícitos destinados à comercialização de drogas, documentos falsificados, dados pessoais roubados, softwares maliciosos e outros produtos ilegais.

A existência desses ambientes demonstra que a tecnologia pode ser utilizada simultaneamente para promoção de direitos fundamentais e para facilitação de práticas criminosas.

Essa dualidade representa uma das principais dificuldades enfrentadas pela criminologia digital.

---

[3] Camada oculta da internet que não é indexada por buscadores tradicionais, como o Google. Embora ofereça forte anonimato e privacidade, é amplamente associada a crimes virtuais, golpes e vazamentos de dados

Não é a tecnologia em si que produz a criminalidade, mas as formas pelas quais ela é incorporada às relações sociais e utilizada pelos indivíduos.

Por fim, merece destaque a crescente influência dos algoritmos na organização das interações digitais.

Embora o tema seja aprofundado nos capítulos posteriores, é importante reconhecer desde já que os sistemas algorítmicos deixaram de desempenhar funções meramente operacionais.

Atualmente, algoritmos selecionam conteúdos, recomendam conexões sociais, organizam fluxos informacionais e influenciam significativamente a exposição dos indivíduos a determinadas ideias e comportamentos.

Essa capacidade de mediação tecnológica introduz uma variável inédita na análise criminológica.

Pela primeira vez na história, parte significativa das interações humanas ocorre em ambientes estruturados por sistemas automatizados capazes de influenciar padrões de comportamento em larga escala.

A compreensão desse fenômeno será fundamental para os capítulos seguintes, especialmente quando forem analisados os processos de radicalização digital, disseminação de discursos de ódio e formação de comunidades extremistas.

Diante de todos esses elementos, torna-se possível afirmar que o ciberespaço não deve ser compreendido apenas como cenário passivo da criminalidade contemporânea. Trata-se de um ambiente social complexo cujas características específicas influenciam oportunidades criminosas, processos de socialização e mecanismos de controle social, desempenhando papel ativo na configuração dos fenômenos criminais da era digital.

1.3 Os desafios da criminologia contemporânea diante da sociedade em rede

As profundas transformações promovidas pela revolução digital impuseram à criminologia desafios teóricos e metodológicos sem precedentes. Durante grande parte de sua história, a disciplina desenvolveu seus modelos explicativos a partir de uma realidade social caracterizada por interações predominantemente presenciais, delimitação territorial relativamente clara e mecanismos de controle social exercidos principalmente por instituições estatais. A consolidação da sociedade em rede alterou significativamente esse cenário, exigindo uma revisão crítica dos paradigmas criminológicos tradicionais.

Nesse contexto, a criminalidade também passa a assumir características compatíveis com a lógica das redes.

Diferentemente dos modelos tradicionais de organização criminosa, frequentemente

estruturados de maneira hierárquica, diversos grupos envolvidos em atividades ilícitas passaram a adotar formas descentralizadas de coordenação. Organizações criminosas, comunidades extremistas, redes de compartilhamento de conteúdos ilícitos e grupos especializados em fraudes eletrônicas frequentemente operam por meio de estruturas flexíveis, horizontais e altamente adaptáveis.

Essa realidade desafia instrumentos analíticos desenvolvidos para compreender organizações relativamente estáveis e territorialmente delimitadas.

A criminalidade digital introduziu uma ruptura significativa entre espaço físico e espaço social. Segundo o autor, muitos comportamentos criminosos contemporâneos desenvolvem-se em ambientes cuja lógica de funcionamento não depende das limitações geográficas tradicionalmente associadas ao exercício da jurisdição estatal.

A consequência imediata é a ampliação da complexidade investigativa.

A identificação dos autores, a preservação das provas digitais, a cooperação internacional e a responsabilização criminal tornam-se tarefas consideravelmente mais difíceis quando os elementos envolvidos na prática delitiva encontram-se distribuídos em diferentes países e sistemas jurídicos.

Além disso, a velocidade das transformações tecnológicas frequentemente supera a capacidade de adaptação das instituições responsáveis pela produção normativa e pela aplicação do direito.

Esse fenômeno produz aquilo que parte da doutrina denomina defasagem regulatória. Enquanto novas tecnologias surgem e se difundem rapidamente, o processo legislativo e a construção jurisprudencial tendem a ocorrer em ritmo significativamente mais lento.

Como consequência, práticas potencialmente lesivas podem permanecer durante longos períodos sem regulamentação adequada, gerando incertezas jurídicas e dificuldades para a atuação dos órgãos responsáveis pela prevenção e repressão criminal.

Outro desafio relevante refere-se à crescente influência de atores privados sobre os mecanismos contemporâneos de controle social.

Tradicionalmente, a definição do que seria considerado crime e a aplicação de sanções constituíam atribuições predominantemente estatais. Na sociedade digital, entretanto, empresas de tecnologia passaram a desempenhar papel central na regulação dos comportamentos desenvolvidos em ambientes virtuais.

Plataformas digitais estabelecem regras de utilização, removem conteúdos, suspendem contas, restringem publicações e definem parâmetros para circulação de informações. Em muitos casos, tais decisões produzem impactos significativos sobre direitos fundamentais

relacionados à liberdade de expressão, privacidade e participação política.

Essa realidade gera importante deslocamento do poder regulatório.

Embora o Estado continue exercendo papel fundamental na produção e aplicação do direito, parte significativa do controle social passa a ser realizada por instituições privadas cujos critérios decisórios nem sempre estão submetidos aos mesmos níveis de transparência e controle democrático exigidos das autoridades públicas.

A criminologia contemporânea não pode ignorar esse fenômeno.

Compreender os mecanismos de controle social na era digital exige analisar simultaneamente a atuação do Estado e das plataformas tecnológicas, reconhecendo que ambas influenciam diretamente a construção dos limites entre comportamentos permitidos, tolerados e proibidos.

Outro aspecto particularmente relevante refere-se à crescente utilização de sistemas automatizados para monitoramento, classificação e previsão de comportamentos.

O desenvolvimento da inteligência artificial ampliou significativamente a capacidade de processamento de dados e identificação de padrões comportamentais. Em diferentes países, tecnologias de análise preditiva passaram a ser utilizadas para orientar decisões relacionadas à segurança pública, policiamento e investigação criminal.

Embora esses instrumentos apresentem potencial para aprimorar determinadas atividades estatais, também suscitam importantes preocupações éticas e jurídicas.

A criminologia crítica tem chamado atenção para os riscos associados à reprodução automatizada de desigualdades historicamente construídas. Sistemas alimentados por bases de dados enviesadas podem reforçar padrões discriminatórios preexistentes, ampliando processos de seletividade penal e aprofundando vulnerabilidades sociais.

Nesse sentido, as reflexões de Alessandro Baratta permanecem extremamente atuais.

Ao analisar os mecanismos de criminalização, Baratta, em sua obra “Criminologia Crítica e Crítica do Direito Penal: introdução à sociologia do direito penal”, demonstrou que o sistema penal não atua de forma neutra ou igualmente distribuída sobre todos os segmentos sociais. Pelo contrário, existe tendência histórica de concentração da intervenção punitiva sobre determinados grupos considerados mais vulneráveis ou menos capazes de resistir ao poder estatal.

A introdução de tecnologias digitais não elimina essa seletividade. Pelo contrário, existe o risco de que sistemas automatizados reproduzam e amplifiquem desigualdades já presentes nos processos de controle social.

A sociedade em rede também desafia concepções tradicionais sobre identidade,

pertencimento e interação social.

A aprendizagem criminal, a radicalização política, a disseminação de discursos de ódio e a formação de subculturas desviantes podem ocorrer em espaços digitais que transcendem fronteiras nacionais e culturais.

Consequentemente, teorias criminológicas centradas exclusivamente em fatores locais ou territoriais mostram-se insuficientes para explicar determinados fenômenos observados na contemporaneidade.

Diante desse cenário, torna-se evidente que a criminologia precisa ampliar seus referenciais analíticos para compreender adequadamente os desafios impostos pela sociedade digital.

Isso não significa abandonar as contribuições produzidas pelas teorias clássicas e contemporâneas. Pelo contrário. O desafio consiste em reinterpretá-las à luz das transformações tecnológicas que caracterizam a sociedade em rede.

A compreensão da criminalidade digital exige uma abordagem interdisciplinar capaz de articular conhecimentos provenientes da criminologia, sociologia, ciência política, psicologia social, ciência da computação e estudos sobre comunicação.

Somente a partir dessa perspectiva será possível compreender adequadamente os fatores que influenciam a prática de delitos virtuais, os processos de radicalização online, os mecanismos contemporâneos de controle social e os impactos da tecnologia sobre a proteção dos direitos fundamentais.

Encerradas essas considerações sobre a transformação do fenômeno criminal na sociedade digital, torna-se possível avançar para a análise dos fatores criminológicos específicos associados à prática de delitos virtuais. Para tanto, o capítulo seguinte examinará as principais teorias criminológicas capazes de explicar os processos de aprendizagem, motivação e construção dos comportamentos criminosos no ambiente digital.

CAPÍTULO II – Perfis criminológicos e fatores associados à criminalidade virtual

2.1 A teoria da associação diferencial e a aprendizagem criminal online

Nesse contexto, uma das teorias criminológicas mais relevantes para a compreensão da criminalidade virtual é a Teoria da Associação Diferencial, desenvolvida por Edwin H. Sutherland.

Originalmente formulada na obra *Principles of Criminology* (1939), a teoria surgiu como reação às explicações biológicas e psicológicas predominantes na criminologia do início do século XX. Sutherland rejeitou a ideia de que o comportamento criminoso resultaria de características inatas do indivíduo ou de patologias específicas. Em seu lugar, propôs uma interpretação sociológica baseada nos processos de interação social.

Segundo o autor:

“O comportamento criminoso é aprendido por meio da interação com outras pessoas em um processo de comunicação. ” (SUTHERLAND; CRESSEY, 1974, p. 75, tradução própria).

A afirmação representa uma ruptura importante com os modelos criminológicos anteriores. O crime deixa de ser compreendido como consequência de predisposições biológicas ou falhas morais individuais e passa a ser analisado como resultado de um processo de aprendizagem social.

Para Sutherland, os indivíduos aprendem comportamentos criminosos da mesma forma que aprendem qualquer outro comportamento social. A interação com grupos específicos permite a transmissão de técnicas, justificativas, motivações e racionalizações favoráveis à violação da lei.

O autor sustenta ainda que o comportamento criminoso surge quando o indivíduo é exposto a um número maior de definições favoráveis à infração da norma do que de definições desfavoráveis.

Embora formulada em contexto histórico anterior à internet, essa teoria apresenta extraordinária capacidade explicativa para os fenômenos observados na sociedade digital.

O ambiente virtual ampliou significativamente as possibilidades de interação social e transmissão de conhecimentos. Fóruns especializados, redes sociais, aplicativos de mensagens instantâneas, plataformas de compartilhamento de conteúdo e comunidades online passaram a funcionar como espaços de aprendizagem e socialização em escala global.

A principal diferença em relação aos modelos tradicionais de interação social reside na eliminação das barreiras geográficas.

Antes da internet, a aprendizagem criminal dependia predominantemente de contatos

presenciais. A transmissão de conhecimentos ilícitos ocorria em grupos familiares, comunidades locais, organizações criminosas ou círculos sociais específicos.

Na sociedade digital, esse processo assume dimensões completamente distintas.

Um indivíduo pode ter acesso a conteúdos relacionados à prática de crimes cibernéticos sem jamais estabelecer contato físico com outros participantes dessas atividades. Tutoriais, fóruns de discussão, vídeos explicativos e plataformas especializadas permitem a circulação instantânea de informações sobre invasão de sistemas, criação de softwares maliciosos, engenharia social, ocultação de identidade digital e exploração de vulnerabilidades tecnológicas.

Nesse sentido, a internet potencializa significativamente os mecanismos descritos por Sutherland.

A aprendizagem criminal deixa de depender de estruturas sociais locais e passa a ocorrer em comunidades digitais globalizadas.

David Wall observa que uma das características mais marcantes da criminalidade digital consiste justamente na facilidade de compartilhamento de conhecimento técnico entre indivíduos dispersos geograficamente. Em muitos casos, comunidades virtuais funcionam como verdadeiras redes de formação criminosa, promovendo intercâmbio permanente de informações e aperfeiçoamento coletivo de técnicas ilícitas.

A relevância desse fenômeno torna-se ainda mais evidente quando se analisam grupos especializados em fraudes eletrônicas, ataques cibernéticos e exploração de vulnerabilidades informáticas.

Sob essa perspectiva, a internet não apenas facilita a prática criminosa, mas também amplia os mecanismos de transmissão cultural do comportamento desviante.

Além da aprendizagem técnica, as comunidades digitais desempenham importante papel na construção de justificativas morais favoráveis à criminalidade.

Esse aspecto é particularmente relevante para a teoria de Sutherland. Segundo o autor, o indivíduo não aprende apenas como praticar o delito. Ele aprende também por que a prática criminosa seria aceitável ou legítima (SUTHERLAND; CRESSEY, 1974, p. 87, tradução própria).

Em diversos ambientes digitais observa-se a disseminação de narrativas destinadas a minimizar a gravidade de determinadas condutas.

Fraudes eletrônicas podem ser apresentadas como formas legítimas de obtenção de recursos financeiros. Ataques contra instituições podem ser justificados por razões ideológicas. Invasões de sistemas podem ser romantizadas como demonstrações de habilidade

técnica ou resistência política.

Esses discursos desempenham função semelhante àquela identificada por Sutherland ao analisar grupos criminosos tradicionais.

A exposição contínua a definições favoráveis à violação da norma contribui para reduzir barreiras morais e facilitar a adoção de comportamentos ilícitos.

O fenômeno torna-se particularmente preocupante quando associado aos mecanismos de recomendação algorítmica presentes nas plataformas digitais.

Ao identificar interesses específicos dos usuários, os algoritmos tendem a recomendar conteúdos semelhantes aos previamente consumidos. Como consequência, indivíduos podem ser progressivamente expostos a comunidades cada vez mais especializadas e ideologicamente homogêneas.

Esse processo cria condições favoráveis para a intensificação da aprendizagem criminal.

A exposição contínua a conteúdos que legitimam comportamentos ilícitos pode fortalecer percepções favoráveis à criminalidade e enfraquecer mecanismos tradicionais de controle social.

Outro aspecto relevante refere-se ao anonimato relativo proporcionado pelo ambiente digital.

A possibilidade de interação sob identidades fictícias reduz riscos de estigmatização social e amplia a disposição dos indivíduos para participar de comunidades voltadas à prática de atividades ilícitas.

Sob essa perspectiva, o ambiente virtual potencializa simultaneamente dois elementos centrais da teoria da associação diferencial: a frequência das interações e a intensidade das influências sociais.

A internet permite que indivíduos permaneçam permanentemente conectados a grupos capazes de transmitir valores, conhecimentos e justificativas favoráveis à prática criminosa.

Consequentemente, a criminalidade digital não pode ser compreendida apenas como resultado da existência de tecnologias sofisticadas ou de vulnerabilidades técnicas exploráveis. Ela também decorre de processos de aprendizagem social desenvolvidos em ambientes digitais específicos.

A principal contribuição da teoria de Sutherland para a criminologia digital consiste justamente em demonstrar que o comportamento criminoso continua sendo fundamentalmente um fenômeno social, mesmo quando praticado por meio de instrumentos tecnológicos

altamente complexos.

A tecnologia modifica os meios pelos quais a aprendizagem ocorre, mas não elimina a importância das interações humanas na construção dos comportamentos desviantes.

Por essa razão, a análise da criminalidade virtual exige compreender não apenas os recursos tecnológicos utilizados pelos infratores, mas também os processos de socialização que permitem a formação, manutenção e reprodução das comunidades responsáveis pela transmissão desses conhecimentos.

Contudo, a aprendizagem criminal representa apenas uma das dimensões necessárias para compreender a criminalidade digital. Também se faz necessário investigar os fatores estruturais que levam determinados indivíduos a buscar meios ilícitos para alcançar objetivos socialmente valorizados.

2.2 A teoria da anomia e os delitos virtuais

Além dos processos de aprendizagem social descritos por Edwin H. Sutherland, a compreensão da criminalidade digital exige a análise das pressões estruturais que influenciam o comportamento dos indivíduos na sociedade contemporânea. Nesse sentido, uma das contribuições mais relevantes para a criminologia continua sendo a Teoria da Anomia desenvolvida por Robert K. Merton.

Publicada originalmente no artigo "*Social Structure and Anomie"* (1938), a teoria de Merton procurou explicar a criminalidade não a partir de características individuais dos infratores, mas das tensões produzidas pela própria organização social (MERTON, 1938, p. 672, tradução própria). Inspirado parcialmente nas reflexões de Émile Durkheim sobre a anomia, Merton argumenta que sociedades modernas tendem a valorizar intensamente determinados objetivos culturais, especialmente o sucesso econômico, o reconhecimento social e a ascensão material. Entretanto, os meios legítimos disponíveis para alcançar esses objetivos não são distribuídos de forma igualitária entre todos os indivíduos.

Para Merton, a criminalidade surge quando existe um descompasso entre os fins socialmente valorizados e os meios institucionalmente aceitos para alcançá-los. Diante dessa tensão, os indivíduos desenvolvem diferentes formas de adaptação social.

Entre elas, destaca-se a denominada inovação, caracterizada pela aceitação dos objetivos culturais acompanhada da rejeição ou substituição dos meios legítimos para atingi-los.

Em outras palavras, o indivíduo continua desejando riqueza, prestígio e reconhecimento, mas passa a buscar esses resultados por meio de práticas ilícitas.

Embora formulada em contexto histórico muito anterior à internet, a teoria da anomia

apresenta extraordinária atualidade para a compreensão da criminalidade digital.

A sociedade contemporânea é marcada por intensa valorização do desempenho individual, da produtividade, da visibilidade social e do sucesso econômico. As plataformas digitais ampliaram significativamente a exposição dos indivíduos a padrões de vida frequentemente associados ao consumo, à riqueza e ao reconhecimento público.

As redes sociais desempenham papel central nesse processo.

Influenciadores digitais, celebridades, empreendedores e criadores de conteúdo exibem diariamente estilos de vida marcados por viagens, bens de consumo, conquistas profissionais e reconhecimento social. Embora muitas dessas narrativas representem apenas recortes cuidadosamente selecionados da realidade, elas contribuem para a construção de expectativas sociais relacionadas ao sucesso e à realização pessoal.

Nesse contexto, diversos autores contemporâneos passaram a observar que a internet intensificou mecanismos de comparação social anteriormente existentes.

Zygmunt Bauman, ao analisar as transformações da modernidade tardia, sustenta que as sociedades contemporâneas passaram a organizar-se em torno da lógica do consumo e da permanente necessidade de afirmação individual. Em “Vida para Consumo*”* (2008), o autor afirma que, na sociedade de consumidores, ninguém pode se tornar sujeito sem primeiro virar mercadoria. ” (BAUMAN, 2008, p. 20).

As redes sociais transformaram a própria identidade em objeto de exposição pública e avaliação constante. Curtidas, compartilhamentos, seguidores e métricas de engajamento passaram a funcionar como indicadores simbólicos de reconhecimento social.

Consequentemente, a busca por visibilidade assume papel cada vez mais relevante na construção das identidades contemporâneas.

Essa dinâmica produz impactos criminológicos significativos.

Assim como a busca por riqueza material pode estimular determinadas formas de criminalidade econômica, a busca por reconhecimento social pode favorecer comportamentos ilícitos destinados à obtenção de notoriedade, influência ou validação grupal.

Em muitos casos, a criminalidade digital não está relacionada exclusivamente à obtenção de vantagens financeiras. A prática de ataques cibernéticos, invasões de sistemas ou campanhas de assédio virtual pode estar associada à busca por status dentro de determinadas comunidades digitais.

Além disso, a internet ampliou significativamente as oportunidades para a prática de delitos econômicos.

Golpes financeiros, fraudes bancárias eletrônicas, esquemas de *phishing*[4], estelionatos digitais e pirâmides financeiras representam algumas das modalidades criminosas mais diretamente relacionadas à lógica descrita por Merton.

Os autores dessas infrações frequentemente compartilham os mesmos objetivos culturais valorizados pela sociedade — riqueza, sucesso e ascensão econômica — mas recorrem a meios ilícitos para alcançá-los.

A tecnologia reduz custos operacionais, amplia o alcance potencial das fraudes e dificulta a identificação dos responsáveis, tornando determinadas práticas criminosas particularmente atrativas para indivíduos motivados por ganhos econômicos.

Nesse ponto, a teoria da anomia oferece importante explicação estrutural para a criminalidade digital.

O problema não reside apenas nas características individuais dos infratores, mas também nas pressões produzidas por uma sociedade que valoriza intensamente o sucesso econômico e a visibilidade social.

A reflexão torna-se ainda mais relevante quando analisada à luz das contribuições de Byung-Chul Han.

Em *A Sociedade do Cansaço* (2010), Han argumenta que a sociedade contemporânea deixou de ser organizada predominantemente pela disciplina e passou a estruturar-se em torno da lógica do desempenho. Segundo o autor, o sujeito do desempenho explora a si mesmo até consumir-se completamente. ” (HAN, 2017, p. 30).

A crítica de Han permite compreender que a pressão por produtividade, sucesso e realização individual não opera apenas como expectativa externa. Ela é progressivamente internalizada pelos próprios indivíduos.

Na sociedade digital, essa dinâmica é amplificada pelas redes sociais e pelos mecanismos de exposição permanente da vida privada.

Os indivíduos são constantemente incentivados a demonstrar sucesso, produtividade e realização pessoal. O fracasso, por sua vez, tende a ser interpretado como responsabilidade exclusivamente individual.

Esse contexto produz importantes implicações criminológicas.

Quando objetivos socialmente valorizados se tornam cada vez mais ambiciosos e os meios legítimos para alcançá-los permanecem limitados, aumenta a probabilidade de adoção de estratégias alternativas, inclusive ilícitas.

---

[4] É um golpe cibernético em que criminosos se passam por instituições confiáveis para enganar alguém. Eles usam mensagens falsas para roubar senhas, dados de cartões ou instalar vírus no dispositivo da vítima.

A criminalidade digital surge, assim, não apenas como resultado de oportunidades tecnológicas, mas também como consequência de tensões estruturais produzidas pela organização social contemporânea.

A internet potencializa essas tensões ao ampliar simultaneamente a exposição aos modelos de sucesso e as oportunidades para a prática de delitos. Por essa razão, a teoria da anomia continua oferecendo valiosa contribuição para a criminologia digital.

Ela permite compreender que os delitos virtuais não decorrem exclusivamente de fatores tecnológicos ou psicológicos. São também expressão das contradições presentes em uma sociedade que exige desempenho permanente, valoriza intensamente o sucesso individual e oferece oportunidades desiguais para sua realização.

Entretanto, embora as teorias de Sutherland e Merton expliquem importantes aspectos relacionados à aprendizagem criminal e às tensões estruturais da sociedade digital, ainda permanece uma questão fundamental: quem são os autores dos delitos virtuais?

2.3 Perfis criminológicos dos autores de crimes digitais

Uma das principais contribuições da criminologia digital consiste na desconstrução de estereótipos historicamente associados à figura do criminoso. Durante grande parte do século XX, a criminologia e a própria opinião pública frequentemente relacionaram a criminalidade a fatores como marginalização econômica, baixa escolaridade, exclusão social e inserção em contextos urbanos degradados. Embora tais fatores continuem relevantes para a compreensão de determinadas modalidades criminosas, a criminalidade digital demonstra que o fenômeno criminal contemporâneo apresenta características significativamente mais complexas.

Os delitos praticados no ambiente virtual frequentemente são cometidos por indivíduos que não correspondem aos perfis tradicionalmente associados à delinquência convencional. Em muitos casos, os autores possuem elevado nível educacional, amplo domínio tecnológico e plena integração econômica e social.

Essa realidade foi observada por David Wall ao analisar as transformações produzidas pela internet sobre a criminalidade contemporânea. Segundo o autor, o cibercrime desafia diversas categorias tradicionais da criminologia porque envolve agentes cujas características sociais frequentemente diferem daquelas observadas nos delitos convencionais (WALL, 2024, p. 01, tradução própria).

A heterogeneidade dos autores de crimes digitais impede a construção de um perfil único ou universal. Entretanto, a literatura especializada permite identificar algumas categorias recorrentes que auxiliam na compreensão criminológica do fenômeno.

2.3.1 Hackers e crackers: distinções necessárias

Um dos equívocos mais comuns relacionados à criminalidade digital consiste na utilização indiscriminada do termo hacker para designar qualquer indivíduo envolvido em atividades ilícitas na internet.

Do ponto de vista técnico e acadêmico, essa associação é inadequada.

O termo hacker surgiu originalmente para designar indivíduos altamente qualificados em tecnologia da informação, caracterizados pela curiosidade intelectual, criatividade e interesse na compreensão profunda do funcionamento dos sistemas computacionais.

Para Steven Levy, em *Hackers: Heroes of the Computer Revolution* (1984):

> "Tratava-se de uma filosofia baseada no compartilhamento, na abertura, na descentralização e no acesso direto às máquinas a qualquer custo para aperfeiçoá-las e melhorar o mundo. Essa Ética Hacker é seu legado para todos nós." (LEVY, 1984, p. 11, tradução própria).

A literatura especializada costuma reservar a expressão cracker para designar indivíduos que utilizam conhecimentos técnicos para violar sistemas, obter acesso não autorizado a informações ou praticar atividades ilícitas.

Embora a distinção nem sempre seja observada pela mídia ou pela legislação, ela possui relevância criminológica porque evidencia que o domínio tecnológico, por si só, não constitui fator determinante para a criminalidade.

O mesmo conhecimento pode ser utilizado para finalidades legítimas ou ilícitas, dependendo dos contextos sociais, motivações e processos de socialização envolvidos.

2.3.2 Cibercriminosos econômicos

Entre os perfis mais recorrentes da criminalidade digital contemporânea encontram-se os chamados cibercriminosos econômicos.

Esses agentes atuam predominantemente com o objetivo de obter vantagens patrimoniais mediante utilização de recursos tecnológicos.

Fraudes bancárias eletrônicas, phishing, ransomware, invasões de contas digitais, clonagem de cartões e esquemas de engenharia social constituem exemplos típicos dessa modalidade de atuação criminosa.

Sob a perspectiva criminológica, esses indivíduos frequentemente apresentam características compatíveis com a adaptação inovadora descrita por Robert Merton.

Os objetivos culturais relacionados ao sucesso econômico permanecem presentes, mas os meios utilizados para alcançá-los situam-se à margem da legalidade.

A expansão das tecnologias digitais ampliou significativamente as oportunidades

para esse tipo de criminalidade.

Ao contrário dos delitos patrimoniais convencionais, as fraudes eletrônicas permitem alcançar grande número de vítimas simultaneamente, reduzindo custos operacionais e aumentando o potencial de lucro dos infratores.

Além disso, a natureza transnacional da internet dificulta a identificação dos autores e amplia a percepção de impunidade.

Esses fatores contribuem para tornar a criminalidade econômica digital uma das modalidades mais relevantes do cibercrime contemporâneo.

2.3.3 Hacktivistas e a criminalidade de motivação ideológica

Outro perfil relevante corresponde aos chamados hacktivistas.

O termo resulta da combinação das palavras *hacker* e *activism*, sendo utilizado para designar indivíduos ou grupos que empregam recursos tecnológicos como instrumento de protesto político, social ou ideológico.

Diferentemente dos cibercriminosos econômicos, os hacktivistas frequentemente não possuem motivação financeira predominante.

Suas ações costumam estar relacionadas à defesa de causas políticas, denúncias contra governos ou corporações e promoção de determinadas agendas ideológicas.

Entre as práticas mais comuns encontram-se ataques de negação de serviço (DDoS), divulgação não autorizada de informações sigilosas, invasão de sistemas governamentais e desfiguração de páginas institucionais.

A análise criminológica desses agentes revela importante desafio conceitual.

Em muitos casos, os próprios participantes não se percebem como criminosos, mas como ativistas engajados em formas alternativas de resistência política.

Essa percepção evidencia a importância das justificativas morais e ideológicas na construção dos comportamentos criminosos.

Conforme observado por Sutherland, o comportamento desviante frequentemente depende da internalização de definições favoráveis à violação da norma.

No caso dos hacktivistas, tais definições costumam estar associadas à ideia de que determinadas infrações seriam justificáveis diante de objetivos considerados moralmente superiores.

2.3.4 *Trolls*, assediadores digitais e ofensores online

Nem toda criminalidade digital está relacionada à obtenção de vantagens econômicas ou à defesa de causas políticas.

Uma parcela significativa dos comportamentos ilícitos observados na internet

envolve práticas de assédio, intimidação, perseguição e humilhação direcionadas a indivíduos específicos.

Nesse contexto, destaca-se a figura dos chamados *trolls.*

O termo é utilizado para designar indivíduos que provocam conflitos deliberadamente em ambientes digitais por meio da publicação de mensagens ofensivas, provocativas ou manipuladoras.

Embora nem toda atividade de *trolling* constitua crime, determinadas condutas podem ultrapassar os limites da liberdade de expressão e configurar delitos relacionados à honra, perseguição, ameaça ou discriminação.

No artigo "*Personality and Individual Differences*", publicado na revista *Personality and Individual Differences* (2014), pesquisas conduzidas por Erin Buckels, Paul Trapnell e Delroy Paulhus identificaram correlação entre comportamentos de *trolling* e traços de personalidade associados ao chamado "lado sombrio" da personalidade, especialmente sadismo cotidiano, pois tanto os *trolls* quanto os sádicos sentem prazer sádico diante do sofrimento dos outros. Os sádicos apenas querem se divertir... e a internet é o seu playground. (BUCKELS; TRAPNELL; PAULHUS, 2014, p. 05, tradução própria).

Embora tais resultados não permitam generalizações absolutas, eles evidenciam que determinadas modalidades de criminalidade digital podem estar relacionadas à busca por prazer, reconhecimento grupal ou sensação de poder sobre as vítimas.

2.3.5 Extremistas digitais e agentes da radicalização online

Entre os perfis mais preocupantes da contemporaneidade encontram-se os indivíduos envolvidos em processos de radicalização digital.

A expansão das redes sociais permitiu a formação de comunidades virtuais estruturadas em torno de ideologias extremistas, teorias conspiratórias e discursos de ódio.

Nesses ambientes, indivíduos progressivamente expostos a conteúdos homogêneos podem desenvolver visões cada vez mais polarizadas da realidade.

A radicalização raramente ocorre de forma abrupta.

Trata-se, em regra, de processo gradual caracterizado pela exposição contínua a narrativas que reforçam preconceitos, desumanizam grupos sociais e legitimam comportamentos hostis ou violentos.

A criminologia contemporânea reconhece que muitos crimes de ódio praticados no ambiente digital resultam justamente desses processos de socialização desenvolvidos em comunidades extremistas.

Nesse sentido, os extremistas digitais representam um dos exemplos mais evidentes

da interação entre tecnologia, aprendizagem social e comportamento criminoso.

2.3.6 Para além do estereótipo do criminoso digital

A análise dos diferentes perfis envolvidos na criminalidade virtual permite concluir que não existe um modelo único de infrator digital.

Hackers, crackers, fraudadores eletrônicos, hacktivistas, *trolls* e extremistas digitais apresentam motivações, trajetórias e formas de atuação profundamente distintas.

Essa diversidade reforça a necessidade de superar explicações simplistas centradas exclusivamente em características individuais dos agentes.

A criminalidade digital constitui fenômeno multifacetado que resulta da interação entre fatores tecnológicos, sociais, econômicos, psicológicos e culturais.

A principal contribuição da criminologia contemporânea consiste justamente em demonstrar que o comportamento criminoso não pode ser reduzido a uma única causa ou perfil.

No ambiente digital, essa constatação torna-se ainda mais evidente.

Compreender quem pratica delitos virtuais exige analisar simultaneamente os processos de aprendizagem social, as pressões estruturais da sociedade contemporânea e as oportunidades produzidas pelas tecnologias digitais.

Todavia, a compreensão dos perfis criminológicos não é suficiente para explicar integralmente a criminalidade na era digital. É necessário examinar também as estruturas econômicas e tecnológicas que influenciam comportamentos e moldam as interações sociais contemporâneas. Essa análise será desenvolvida no próximo tópico, por meio do estudo do denominado capitalismo de vigilância.

2.4 Capitalismo de vigilância e produção de comportamentos digitais

A análise dos perfis criminológicos associados à criminalidade digital demonstra que os delitos praticados no ambiente virtual não podem ser compreendidos apenas a partir das características individuais dos agentes. Embora fatores relacionados à aprendizagem social, às tensões estruturais e às motivações pessoais permaneçam relevantes, a sociedade digital introduziu uma nova variável criminologicamente significativa: a influência exercida pelas próprias plataformas tecnológicas sobre o comportamento humano.

Durante grande parte da história da criminologia, o ambiente social era concebido principalmente como contexto no qual os indivíduos desenvolviam suas ações. Na contemporaneidade, entretanto, as tecnologias digitais deixaram de desempenhar função meramente instrumental e passaram a participar ativamente da organização das interações humanas.

Tradicionalmente, as teorias criminológicas concentravam suas análises sobre fatores sociais, econômicos, culturais e psicológicos relacionados aos indivíduos. O capitalismo de vigilância introduz uma nova dimensão: a existência de estruturas tecnológicas capazes de influenciar permanentemente processos decisórios e comportamentais.

Se as plataformas digitais possuem capacidade de influenciar preferências, hábitos de consumo, padrões de interação e exposição a conteúdos específicos, torna-se necessário considerar também seus impactos sobre comportamentos socialmente desviantes e potencialmente criminosos.

Nesse contexto, a criminalidade passa a ser compreendida também como fenômeno relacionado às estruturas tecnológicas que organizam a circulação de informações e as relações sociais contemporâneas.

A relevância criminológica dessa perspectiva pode ser observada em diferentes situações.

Plataformas digitais são projetadas para maximizar o tempo de permanência dos usuários e aumentar seus níveis de engajamento. Para atingir esse objetivo, utilizam mecanismos sofisticados de personalização capazes de identificar interesses individuais e adaptar continuamente os conteúdos apresentados.

O problema surge quando conteúdos emocionalmente intensos demonstram maior capacidade de capturar atenção do que informações neutras ou equilibradas.

Estudos realizados no campo da psicologia social indicam que emoções como medo, indignação, raiva e ressentimento tendem a produzir elevados níveis de interação em ambientes digitais.

Consequentemente, sistemas orientados exclusivamente pela maximização do engajamento podem favorecer a circulação de conteúdos capazes de despertar essas emoções.

Embora o objetivo primário das plataformas seja econômico, os efeitos sociais produzidos por essa lógica são extremamente relevantes.

Discursos polarizadores, teorias conspiratórias, campanhas de desinformação e manifestações extremistas frequentemente apresentam elevado potencial de compartilhamento e interação.

A consequência é a formação de ambientes digitais nos quais determinados conteúdos recebem visibilidade desproporcional em razão de sua capacidade de capturar atenção.

Sob a perspectiva criminológica, isso significa que fatores estruturais relacionados ao funcionamento das plataformas podem influenciar processos de radicalização, disseminação

de discursos de ódio e fortalecimento de comunidades voltadas à prática de atividades ilícitas.

Assim como a legislação condiciona comportamentos por meio de normas jurídicas, a arquitetura digital influencia condutas por meio do design das plataformas e dos algoritmos que organizam a circulação de informações.

Essa constatação possui profundas implicações para a criminologia contemporânea.

Se os ambientes digitais são estruturados por mecanismos capazes de influenciar comportamentos, a análise da criminalidade não pode limitar-se aos indivíduos que praticam infrações.

Torna-se igualmente necessário examinar as características dos sistemas tecnológicos nos quais esses comportamentos se desenvolvem.

Outro aspecto relevante refere-se à concentração de poder informacional.

As grandes plataformas digitais acumulam quantidades sem precedentes de dados sobre hábitos, preferências e comportamentos de bilhões de usuários.

Essa capacidade de monitoramento produz novas formas de poder social que transcendem os mecanismos tradicionais de controle estudados pela criminologia.

Michel Foucault já havia observado, em *Vigiar e Punir* (1975), que o exercício do poder moderno depende cada vez mais da vigilância permanente e da produção de conhecimento sobre os indivíduos.

Embora suas reflexões tenham sido formuladas antes da internet, muitos autores identificam paralelos significativos entre o modelo panóptico descrito por Foucault e os sistemas contemporâneos de monitoramento digital.

A diferença fundamental reside na escala.

Enquanto os mecanismos clássicos de vigilância possuíam limitações materiais significativas, as tecnologias digitais permitem monitoramento contínuo de populações inteiras em tempo real.

A criminologia digital precisa, portanto, considerar não apenas a criminalidade produzida no ambiente virtual, mas também os impactos decorrentes das novas formas de vigilância e controle social possibilitadas pela tecnologia.

Diante dessas transformações, torna-se evidente que a compreensão da criminalidade contemporânea exige uma ampliação do objeto tradicional da criminologia.

O estudo dos delitos digitais não pode restringir-se à análise dos infratores. É necessário examinar também as estruturas econômicas, tecnológicas e institucionais que moldam comportamentos e influenciam a produção do desvio na sociedade em rede.

O capitalismo de vigilância representa uma das expressões mais sofisticadas dessa

nova realidade, revelando que os desafios da criminologia digital ultrapassam a simples adaptação de antigas teorias a novos instrumentos tecnológicos. Trata-se da necessidade de compreender como a própria organização econômica da internet influencia processos de socialização, controle social e construção da criminalidade contemporânea.

Contudo, a influência das plataformas digitais sobre o comportamento humano não se limita à coleta de dados e ao monitoramento das atividades dos usuários. Ela também se manifesta por meio dos algoritmos responsáveis por selecionar, priorizar e recomendar conteúdos. A análise desses mecanismos constitui o próximo passo para compreender a relação entre tecnologia e criminalidade na sociedade digital.

2.5 Economia da atenção, algoritmos e amplificação do comportamento desviante

A compreensão da criminalidade digital contemporânea exige a análise de um dos elementos mais influentes da sociedade conectada: os algoritmos de recomendação e os mecanismos associados à denominada economia da atenção. Embora frequentemente apresentados como ferramentas neutras destinadas a organizar informações em ambientes digitais, os algoritmos desempenham papel decisivo na forma como os indivíduos acessam conteúdos, constroem opiniões e estabelecem relações sociais.

A relevância criminológica desse fenômeno decorre do fato de que grande parte das interações humanas na internet não ocorre de maneira espontânea. O acesso às informações é mediado por sistemas automatizados capazes de selecionar, priorizar e recomendar conteúdos de acordo com critérios previamente definidos pelas plataformas.

Para compreender esse processo, é necessário inicialmente analisar o conceito de economia da atenção.

A expressão foi popularizada por Herbert Simon, prêmio Nobel de Economia, que já na década de 1970 observava que a abundância de informações produziria uma nova escassez social: a escassez de atenção. Segundo Simon, quanto maior a quantidade de informações disponíveis, mais valiosa se torna a capacidade de capturar a atenção dos indivíduos. (SIMON, 1971, p. 40, tradução própria).

Na sociedade digital, essa lógica tornou-se o fundamento econômico de grande parte das plataformas tecnológicas.

Redes sociais, mecanismos de busca, plataformas de vídeo e aplicativos diversos dependem da permanência contínua dos usuários em seus ambientes digitais. Quanto maior o tempo de permanência, maior a coleta de dados e maior o potencial de monetização por meio de publicidade direcionada.

Nesse contexto, os algoritmos assumem função central.

Seu objetivo principal não consiste apenas em organizar informações, mas em identificar quais conteúdos possuem maior probabilidade de manter o usuário engajado. Os usuários deixam de ser apenas consumidores de conteúdo e passam a constituir objeto permanente de observação, análise e influência comportamental.

A criminologia digital encontra nesse fenômeno um campo de investigação particularmente relevante.

Se as plataformas possuem interesse econômico em maximizar engajamento, torna-se necessário questionar quais tipos de conteúdo tendem a produzir maiores níveis de interação.

Diversos estudos indicam que emoções intensas geram maior compartilhamento e participação dos usuários.

Jonathan Haidt, professor da Universidade de Nova York, dedicou parte significativa de suas pesquisas à análise das relações entre emoções, polarização política e redes sociais.

Em *The Righteous Mind* (2012), Haidt argumenta que os seres humanos tendem a reagir mais intensamente a conteúdos que despertam emoções relacionadas à indignação moral, medo e hostilidade. (HAIDT, 2012, p. 55, tradução própria).

A observação possui importantes implicações para o funcionamento dos algoritmos.

Conteúdos capazes de provocar reações emocionais intensas tendem a gerar mais comentários, compartilhamentos e tempo de permanência nas plataformas.

Consequentemente, sistemas orientados pela lógica do engajamento frequentemente conferem maior visibilidade a informações polarizadoras ou controversas.

Não se trata necessariamente de uma decisão deliberada das plataformas de promover extremismo ou criminalidade.

O problema é estrutural.

Quando o principal critério de sucesso de um conteúdo passa a ser sua capacidade de capturar atenção, mensagens que despertam emoções intensas tendem a ser privilegiadas independentemente de sua qualidade informacional ou de seus impactos sociais.

Indivíduos expostos predominantemente a opiniões semelhantes às suas tendem a adotar posições progressivamente mais extremas ao longo do tempo.

No ambiente digital, os algoritmos podem intensificar esse processo.

Ao identificar preferências e padrões de consumo informacional, as plataformas frequentemente recomendam conteúdos semelhantes aos já acessados anteriormente.

Como consequência, o usuário passa a ser inserido em ambientes cada vez mais homogêneos do ponto de vista ideológico.

Essas estruturas passaram a ser popularmente conhecidas como câmaras de eco (*echo*

chambers).

Sob a perspectiva criminológica, o problema torna-se particularmente relevante quando tais ambientes favorecem a disseminação de discursos de ódio, teorias conspiratórias ou narrativas que legitimam comportamentos ilícitos.

A exposição contínua a conteúdos homogêneos reduz a presença de perspectivas divergentes e dificulta processos de contestação crítica das informações recebidas.

Esse mecanismo contribui para a construção de ambientes favoráveis à radicalização.

A radicalização online não decorre exclusivamente da existência de indivíduos predispostos ao extremismo.

Ela resulta também da interação entre vulnerabilidades individuais, processos de socialização digital e mecanismos tecnológicos de recomendação.

Nesse sentido, os algoritmos podem atuar como amplificadores de tendências já existentes.

A criminologia contemporânea não sustenta que os sistemas automatizados sejam responsáveis diretos pela criminalidade.

Entretanto, torna-se cada vez mais difícil ignorar seu papel na estruturação dos ambientes sociais em que determinados comportamentos se desenvolvem.

A análise criminológica passa, assim, a incorporar elementos tradicionalmente ausentes das teorias clássicas.

Além das características individuais dos agentes e das condições sociais que influenciam suas ações, torna-se necessário compreender os impactos produzidos pela arquitetura tecnológica das plataformas.

A criminalidade digital não é resultado apenas da interação entre indivíduos.

Ela ocorre em ambientes estruturados por sistemas automatizados capazes de influenciar padrões de exposição informacional, formação de opiniões e construção de identidades coletivas.

Essa constatação conduz a uma das principais hipóteses da criminologia digital contemporânea: determinados modelos tecnológicos podem atuar como fatores criminógenos indiretos ao favorecer processos de radicalização, disseminação de discursos de ódio e fortalecimento de comunidades voltadas à prática de atividades ilícitas.

Todavia, a compreensão desses fenômenos permanece incompleta sem a análise de outro aspecto fundamental da criminalidade contemporânea: a seletividade dos mecanismos de controle social e do sistema penal diante das transformações produzidas pela sociedade digital. É justamente essa questão que será examinada no próximo tópico.

2.6 Seletividade penal e criminalidade digital

A análise dos fatores criminológicos associados aos delitos virtuais não estaria completa sem a consideração crítica dos mecanismos de controle social responsáveis pela definição, investigação e punição das condutas consideradas ilícitas. Desde a segunda metade do século XX, a criminologia crítica passou a questionar a ideia de que o sistema penal atuaria de maneira neutra, objetiva e igualmente distribuída sobre todos os segmentos da sociedade. Ao contrário, diversos autores demonstraram que os processos de criminalização são influenciados por fatores políticos, econômicos e sociais que determinam quais comportamentos receberão maior atenção repressiva e quais permanecerão relativamente invisíveis à intervenção estatal.

Nesse contexto, destaca-se a contribuição de Alessandro Baratta. Em sua obra "Criminologia Crítica e Crítica do Direito Penal*"* (1982), o autor sustenta que a criminalidade não pode ser compreendida apenas como resultado da prática de determinadas condutas, mas também como consequência de processos seletivos desenvolvidos pelas instituições responsáveis pela produção e aplicação das normas penais.

Segundo Baratta, o sistema penal não protege todos os bens jurídicos de maneira igual, nem todos os indivíduos contra as ofensas a esses bens. " (BARATTA, 2011, p. 165).

A afirmação revela uma das principais teses da criminologia crítica: a atuação do sistema penal é seletiva.

Determinadas condutas são criminalizadas com maior intensidade do que outras, e determinados grupos sociais encontram-se mais expostos à intervenção punitiva do que outros.

Essa reflexão assume especial relevância quando aplicada à criminalidade digital.

O debate público frequentemente concentra sua atenção sobre figuras específicas, como hackers, fraudadores eletrônicos ou indivíduos envolvidos em ataques cibernéticos. Contudo, a sociedade digital produziu formas de lesão social muito mais amplas e complexas, nem sempre enfrentadas com a mesma intensidade pelos mecanismos tradicionais de controle.

A coleta massiva de dados pessoais sem transparência adequada, a manipulação algorítmica de informações, a disseminação sistemática de desinformação e determinadas práticas abusivas desenvolvidas por grandes corporações tecnológicas podem produzir impactos sociais extremamente significativos.

Entretanto, tais condutas frequentemente recebem tratamento jurídico distinto daquele reservado à criminalidade convencional.

A observação não implica negar a importância do combate aos delitos virtuais

praticados por indivíduos ou organizações criminosas. O objetivo consiste em evidenciar que a seleção dos comportamentos considerados prioritários para a intervenção penal não ocorre de forma neutra.

A criminologia crítica demonstra que a própria definição do que será tratado como problema criminal resulta de escolhas políticas e institucionais.

Essa percepção aproxima-se das reflexões desenvolvidas por Nils Christie. Em sua obra *A Indústria do Controle do Crime* (1993), Christie alerta para o risco de expansão contínua dos mecanismos punitivos como resposta automática aos conflitos sociais, pois o crime não existe, ele é criado. (CHRISTIE, 1995, p. 21, tradução própria).

A frase não significa que comportamentos lesivos sejam imaginários. O que Christie procura demonstrar é que a transformação de determinados conflitos em objetos de intervenção penal depende de processos sociais de definição e atribuição de significado.

Na sociedade digital, essa reflexão torna-se particularmente relevante.

A rápida evolução tecnológica frequentemente produz situações nas quais as fronteiras entre comportamento aceitável, comportamento abusivo e comportamento criminoso permanecem em disputa.

Questões relacionadas à privacidade, proteção de dados, moderação de conteúdo e utilização de inteligência artificial demonstram que a criminalidade digital não pode ser analisada exclusivamente a partir das categorias tradicionais do direito penal.

Além disso, a seletividade manifesta-se também na própria capacidade de investigação e responsabilização.

Delitos praticados por indivíduos isolados costumam ser mais facilmente identificáveis e processáveis do que práticas desenvolvidas por grandes organizações dotadas de significativo poder econômico e tecnológico.

A assimetria de recursos frequentemente influencia a forma como os mecanismos de controle social são aplicados.

Nesse aspecto, as reflexões de Eugenio Raúl Zaffaroni oferecem importante contribuição.

Ao analisar o funcionamento concreto dos sistemas penais latino-americanos, Zaffaroni observa que o poder punitivo tende a operar de forma seletiva e desigual, incidindo com maior intensidade sobre determinados grupos sociais.

Segundo o autor, o sistema penal exerce seu poder de forma seletiva porque não possui capacidade operacional para atingir todos aqueles que praticam condutas criminalizadas. ” (ZAFFARONI; BATISTA; ALAGIA; SLOKAR, 2003, p. 50).

A observação possui grande relevância para a criminalidade digital.

O volume de condutas potencialmente ilícitas praticadas diariamente na internet supera em muito a capacidade operacional dos órgãos responsáveis pela investigação e persecução penal.

Consequentemente, torna-se inevitável a realização de escolhas institucionais sobre quais comportamentos serão efetivamente priorizados.

Essas escolhas podem refletir critérios legítimos relacionados à gravidade das infrações e à proteção dos bens jurídicos mais relevantes. Contudo, também podem reproduzir desigualdades estruturais e padrões históricos de seletividade.

A questão torna-se ainda mais complexa diante do crescente uso de tecnologias de monitoramento e inteligência artificial para fins de segurança pública.

Frequentemente apresentadas como instrumentos capazes de reduzir subjetividades e aumentar a eficiência das investigações, essas tecnologias não estão imunes aos problemas tradicionalmente identificados pela criminologia crítica.

Sistemas automatizados são alimentados por bases de dados construídas socialmente. Se essas bases refletem padrões históricos de discriminação ou seletividade, existe o risco de reprodução automatizada dessas distorções.

Diversos estudos internacionais têm demonstrado que algoritmos utilizados em contextos relacionados à segurança pública podem apresentar vieses raciais, socioeconômicos e territoriais.

A tecnologia, portanto, não elimina a seletividade. Em determinadas circunstâncias, pode até mesmo ampliá-la.

Essa constatação reforça a necessidade de submeter os novos mecanismos de controle social aos mesmos parâmetros críticos tradicionalmente aplicados às instituições penais.

A criminologia digital não pode limitar-se ao estudo dos delitos praticados por meio da tecnologia. Ela deve investigar também os impactos produzidos pela própria utilização da tecnologia como instrumento de vigilância, monitoramento e controle social.

Sob essa perspectiva, a criminalidade digital revela uma importante contradição da sociedade contemporânea.

Ao mesmo tempo em que a internet amplia oportunidades para a prática de delitos, ela também amplia extraordinariamente a capacidade de vigilância exercida por empresas privadas e instituições públicas.

A expansão simultânea da criminalidade e da vigilância constitui uma das

características centrais da era digital.

Diante desse cenário, a principal contribuição da criminologia crítica consiste em recordar que o combate à criminalidade não pode justificar a expansão ilimitada do poder punitivo.

A busca por segurança deve permanecer compatível com a proteção dos direitos fundamentais e com os princípios que estruturam o Estado Democrático de Direito.

Conclui-se, portanto, que a criminalidade digital não desafia apenas as teorias tradicionais sobre o comportamento criminoso. Ela também exige reflexão crítica sobre os mecanismos contemporâneos de controle social, vigilância e produção da punição.

Encerradas as análises relativas aos perfis criminológicos e aos fatores associados à criminalidade virtual, torna-se possível avançar para uma das manifestações mais preocupantes da sociedade digital contemporânea: os crimes de ódio, os processos de radicalização online e os desafios impostos à proteção de dados pessoais. Esses temas serão objeto do capítulo seguinte, no qual serão examinadas as relações entre discurso de ódio, algoritmos, liberdade de expressão e os impactos da Lei Geral de Proteção de Dados Pessoais.

CAPÍTULO III – Crimes de ódio, radicalização digital e os impactos da LGPD

3.1 Crimes de ódio e violência simbólica no ambiente digital

A expansão das tecnologias digitais e das redes sociais transformou profundamente a forma como discursos discriminatórios são produzidos, disseminados e consumidos na sociedade contemporânea. Embora manifestações de intolerância, preconceito e hostilidade contra grupos vulneráveis não constituam fenômenos inéditos, a internet modificou significativamente seu alcance, velocidade de propagação e potencial de impacto social. Nesse contexto, os crimes de ódio passaram a ocupar posição central nos debates criminológicos relacionados à sociedade digital.

A literatura especializada não apresenta uma definição única e universalmente aceita para os crimes de ódio. Contudo, existe relativo consenso de que tais condutas se caracterizam pela escolha da vítima em razão de sua pertença — real ou presumida — a determinado grupo social, étnico, religioso, racial, nacional, político ou relacionado à orientação sexual e identidade de gênero.

Entre as principais referências internacionais sobre o tema destaca-se Barbara Perry. Em *In the Name of Hate: Understanding Hate Crimes* (2001), a autora define os crimes de ódio como atos de violência e intimidação, geralmente direcionados a grupos já estigmatizados e marginalizados. (PERRY, 2001, p. 10, tradução própria).

A definição proposta por Perry evidencia uma característica fundamental desses delitos: eles não atingem apenas a vítima individualmente considerada.

Quando uma pessoa é atacada em razão de sua identidade racial, religiosa ou sexual, a mensagem transmitida alcança toda a coletividade à qual ela pertence. O crime de ódio possui, portanto, uma dimensão simbólica que ultrapassa os efeitos produzidos sobre o indivíduo diretamente atingido.

Essa característica distingue os crimes de ódio de diversas outras modalidades criminosas.

Enquanto muitos delitos produzem danos predominantemente individuais, os crimes motivados por preconceito operam como instrumentos de intimidação coletiva. Seu objetivo não consiste apenas em lesionar uma pessoa específica, mas também reafirmar relações de poder, exclusão e subordinação dirigidas contra grupos inteiros.

A análise criminológica desse fenômeno exige compreender a relação entre criminalidade e estrutura social.

Barbara Perry sustenta que os crimes de ódio não devem ser interpretados como manifestações isoladas de intolerância individual. Pelo contrário, refletem relações históricas

de desigualdade e dominação presentes na própria organização social.

Segundo a autora, o crime de ódio constitui um mecanismo de poder e opressão, destinado a reafirmar as hierarquias precárias que caracterizam uma determinada ordem social. (PERRY, 2001, p. 29, tradução própria).

A observação possui grande relevância para a sociedade digital.

A internet frequentemente é apresentada como ambiente democrático, horizontal e acessível a todos os indivíduos. Entretanto, pesquisas contemporâneas demonstram que preconceitos e desigualdades historicamente existentes também se reproduzem nos espaços virtuais.

Racismo, misoginia, antissemitismo, xenofobia, homofobia e outras formas de discriminação encontraram nas plataformas digitais novos meios de circulação e reprodução.

Em muitos casos, a internet não cria o preconceito, mas amplia significativamente sua capacidade de difusão.

Jack Levin e Jack McDevitt, em *Hate Crimes Revisited* (2009), observam que os crimes de ódio apresentam forte dimensão comunicativa. Segundo os autores, a agressão dirigida à vítima constitui simultaneamente uma mensagem destinada a toda a coletividade representada por ela.

A lógica do crime de ódio envolve, portanto, a produção de medo social.

Ao atingir um indivíduo específico, o agressor procura transmitir uma mensagem de exclusão, inferiorização ou ameaça a todos aqueles que compartilham determinada característica identitária.

No ambiente digital, essa dimensão comunicativa assume proporções inéditas.

Uma manifestação discriminatória publicada em rede social pode alcançar milhares ou milhões de pessoas em questão de horas. A velocidade de circulação das informações potencializa significativamente os efeitos simbólicos dos discursos de ódio.

Além disso, as plataformas digitais permitem que mensagens discriminatórias permaneçam acessíveis por longos períodos, ampliando continuamente seu alcance potencial.

Outro aspecto particularmente relevante refere-se à redução dos custos associados à disseminação de conteúdo.

Antes da internet, a divulgação de mensagens extremistas dependia frequentemente da existência de estruturas organizacionais relativamente complexas, capazes de produzir e distribuir materiais impressos ou promover eventos presenciais.

Na sociedade digital, qualquer indivíduo com acesso à internet pode produzir conteúdo potencialmente acessível a audiências massivas.

Essa democratização dos meios de comunicação representa importante conquista para a liberdade de expressão. Entretanto, também amplia as possibilidades de circulação de mensagens discriminatórias e conteúdos extremistas.

A criminologia contemporânea passou a reconhecer que o ambiente digital modifica não apenas a quantidade, mas também a qualidade dos discursos de ódio.

O anonimato relativo proporcionado pela internet reduz barreiras psicológicas relacionadas à exposição pública e à responsabilização social. Como consequência, indivíduos que dificilmente manifestariam determinadas opiniões em contextos presenciais podem sentir-se encorajados a fazê-lo em ambientes virtuais.

Esse fenômeno conecta-se diretamente ao chamado efeito de desinibição online descrito por John Suler.

Conforme analisado no capítulo anterior, a ausência de contato físico direto, a percepção de anonimato e a distância emocional proporcionada pelas interações digitais tendem a reduzir mecanismos de autocontrole presentes nas relações presenciais.

Sob a perspectiva dos crimes de ódio, isso significa que discursos discriminatórios podem ser produzidos com menor percepção das consequências emocionais causadas às vítimas.

A desumanização do outro torna-se mais fácil quando a interação ocorre mediada por telas e sistemas tecnológicos.

Contudo, os impactos produzidos por essas condutas permanecem profundamente reais.

Diversos estudos demonstram que vítimas de assédio, perseguição e discriminação online frequentemente desenvolvem consequências psicológicas significativas, incluindo ansiedade, depressão, isolamento social e comprometimento de sua participação em espaços públicos digitais.

Nesse sentido, torna-se cada vez mais difícil sustentar a distinção simplista entre violência virtual e violência real.

Os efeitos produzidos pelos crimes de ódio praticados na internet ultrapassam o ambiente digital e afetam concretamente a vida das vítimas.

A gravidade do fenômeno aumenta quando se observa que os discursos de ódio frequentemente funcionam como etapa preliminar de processos mais amplos de radicalização.

A exposição contínua a mensagens discriminatórias pode contribuir para a normalização do preconceito e para a legitimação de comportamentos progressivamente mais agressivos.

Por essa razão, a criminologia contemporânea passou a dedicar atenção crescente aos mecanismos de formação e fortalecimento de comunidades extremistas no ambiente digital.

A análise desses processos demonstra que os crimes de ódio não constituem fenômenos isolados, mas frequentemente integram dinâmicas mais amplas de radicalização social e política.

Compreender essas dinâmicas exige examinar o funcionamento das chamadas câmaras de eco e dos mecanismos de polarização que caracterizam parte significativa das interações desenvolvidas nas plataformas digitais. É justamente esse o objeto do próximo tópico.

3.2 Radicalização online e câmaras de eco

A crescente preocupação com os crimes de ódio praticados no ambiente digital levou pesquisadores de diferentes áreas do conhecimento a investigar os mecanismos que favorecem a formação de visões extremistas e a intensificação da polarização social nas plataformas digitais. Embora a intolerância e o radicalismo não tenham surgido com a internet, a sociedade em rede modificou profundamente as formas de disseminação, reforço e legitimação dessas ideias.

Nesse contexto, um dos conceitos mais relevantes para a compreensão da radicalização contemporânea é o de câmara de eco (*echo chamber*).

A expressão refere-se a ambientes informacionais nos quais indivíduos são predominantemente expostos a conteúdos, opiniões e interpretações compatíveis com suas crenças previamente estabelecidas. Como consequência, ocorre redução progressiva do contato com perspectivas divergentes e fortalecimento de percepções homogêneas da realidade.

Entre os principais estudiosos desse fenômeno destaca-se Cass Sunstein. Segundo o autor, as pessoas devem ser expostas a temas e pontos de vista que não tenham escolhido previamente, e a internet permite que os indivíduos selecionem de maneira cada vez mais restrita os conteúdos aos quais desejam se expor. (SUNSTEIN, 2007, p. 5, tradução própria).

A afirmação parte da premissa de que a democracia depende da existência de espaços de encontro entre diferentes perspectivas e visões de mundo.

Quando os indivíduos passam a consumir apenas informações compatíveis com suas crenças, reduz-se a possibilidade de confronto crítico de ideias e amplia-se a tendência à polarização.

Posteriormente, Sunstein desenvolveu de forma mais aprofundada o conceito de polarização grupal.

Segundo o autor, grupos compostos por indivíduos com opiniões semelhantes tendem a adotar posições progressivamente mais extremas após interações reiteradas entre seus membros.

A radicalização raramente ocorre de maneira abrupta. Em regra, trata-se de processo gradual caracterizado pela exposição contínua a narrativas que reforçam preconceitos, legitimam hostilidades e reduzem a complexidade dos problemas sociais.

As plataformas digitais oferecem condições particularmente favoráveis para esse processo.

Por meio de grupos fechados, fóruns especializados, canais de comunicação privada e redes sociais segmentadas, indivíduos podem encontrar comunidades inteiras dedicadas à confirmação de suas crenças e percepções.

A ausência de contraditório e a repetição constante das mesmas narrativas contribuem para a consolidação de interpretações cada vez mais rígidas da realidade.

A relevância criminológica desse fenômeno torna-se evidente quando se observa a formação de comunidades dedicadas à disseminação de discursos racistas, misóginos, antissemitas, xenófobos ou violentamente extremistas.

Em muitos casos, a radicalização não decorre inicialmente de uma predisposição criminosa intensa, mas de um processo progressivo de socialização digital.

O indivíduo passa a frequentar ambientes virtuais nos quais determinadas ideias são constantemente reforçadas, enquanto posições divergentes são deslegitimadas ou excluídas.

Gradualmente, comportamentos que anteriormente seriam percebidos como inaceitáveis passam a ser considerados normais ou justificáveis.

A análise desse fenômeno aproxima-se das contribuições de Manuel Castells sobre a sociedade em rede.

Embora Castells não tenha desenvolvido especificamente uma teoria da radicalização digital, suas reflexões ajudam a compreender como a internet reorganizou os processos de construção identitária contemporâneos.

Segundo o autor:

> “A sociedade em rede possibilita a formação de comunidades estruturadas em torno de identidades compartilhadas, independentemente da localização geográfica dos indivíduos. As pessoas organizam cada vez mais o sentido de suas vidas não em torno daquilo que fazem, mas com base naquilo que são, ou acreditam ser.” (CASTELLS, 2010, p. 7, tradução própria).

A observação possui especial relevância para os processos de radicalização.

Comunidades digitais frequentemente se estruturam em torno de identidades

percebidas como ameaçadas ou marginalizadas. Narrativas de vitimização coletiva, teorias conspiratórias e discursos de antagonismo social tornam-se instrumentos de fortalecimento desses vínculos grupais.

A construção de uma identidade coletiva baseada na oposição a determinados grupos sociais pode favorecer a legitimação de comportamentos discriminatórios e violentos.

Outro aspecto relevante refere-se ao papel desempenhado pelas emoções nos processos de radicalização.

Jonathan Haidt sustenta que as convicções humanas são frequentemente influenciadas por reações emocionais anteriores à reflexão racional. Em *The Righteous Mind* (2012), o autor afirma que "a cauda emocional abana o cão racional", (HAIDT, 2012, p. 44, tradução própria).

A metáfora utilizada por Haidt indica que emoções frequentemente precedem e condicionam os processos de racionalização.

Na sociedade digital, conteúdos capazes de despertar medo, indignação, ressentimento ou hostilidade tendem a receber maior atenção dos usuários.

Consequentemente, tornam-se particularmente eficazes para fortalecer narrativas polarizadoras e processos de radicalização.

Essa dinâmica é potencializada pelos mecanismos de recomendação algorítmica analisados no capítulo anterior.

Ao identificar preferências individuais, os algoritmos frequentemente sugerem conteúdos semelhantes aos previamente consumidos, contribuindo para a formação de ambientes informacionais homogêneos.

Importa destacar que a radicalização online não deve ser compreendida como fenômeno exclusivamente político.

Embora frequentemente associada ao extremismo ideológico, ela pode ocorrer em diferentes contextos sociais.

Comunidades voltadas à misoginia, supremacismo racial, perseguição coordenada de indivíduos, teorias conspiratórias e até mesmo determinadas formas de criminalidade econômica podem apresentar mecanismos semelhantes de reforço grupal e construção identitária.

A criminologia digital passou a reconhecer que muitos comportamentos ilícitos praticados na internet não resultam apenas de decisões individuais isoladas, mas de processos coletivos de socialização desenvolvidos em comunidades digitais específicas.

A aprendizagem criminal descrita por Sutherland e a polarização grupal analisada por

Sunstein frequentemente atuam de forma complementar.

Os indivíduos não apenas aprendem técnicas e justificativas para determinadas condutas. Eles também passam a integrar grupos capazes de reforçar continuamente percepções favoráveis à prática desses comportamentos.

O resultado é a formação de ambientes digitais nos quais discursos discriminatórios, comportamentos agressivos e narrativas extremistas podem adquirir aparência de normalidade.

Essa constatação possui implicações importantes para a prevenção dos crimes de ódio.

Estratégias centradas exclusivamente na punição individual dos autores mostram-se insuficientes para enfrentar fenômenos cuja origem está associada a processos coletivos de socialização e radicalização.

A compreensão da radicalização digital exige atenção não apenas aos indivíduos, mas também às estruturas tecnológicas e comunitárias que favorecem a produção e circulação dessas narrativas.

Nesse cenário, torna-se indispensável examinar o papel específico desempenhado pelos algoritmos na amplificação dos conteúdos extremistas e na intensificação dos processos de polarização. Essa análise será desenvolvida no próximo tópico.

3.3 Algoritmos e disseminação do extremismo

A análise dos processos de radicalização digital conduz inevitavelmente à investigação do papel desempenhado pelos algoritmos na organização contemporânea dos fluxos informacionais. Embora frequentemente apresentados como mecanismos técnicos destinados apenas a selecionar conteúdos relevantes para os usuários, os sistemas algorítmicos exercem influência significativa sobre a forma como informações circulam, opiniões são formadas e comunidades se estruturam no ambiente digital.

A importância desse debate decorre do fato de que a maior parte das experiências digitais contemporâneas não ocorre em ambientes neutros. Redes sociais, plataformas de vídeo, mecanismos de busca e aplicativos diversos utilizam sistemas automatizados para determinar quais conteúdos serão exibidos, em que ordem serão apresentados e qual alcance potencial poderão alcançar.

Esses sistemas operam a partir de critérios que, em regra, não são integralmente transparentes aos usuários.

A relevância criminológica dessa dinâmica está relacionada à capacidade dos algoritmos de influenciar processos de exposição informacional.

Ao selecionar determinados conteúdos em detrimento de outros, os sistemas automatizados participam ativamente da construção dos ambientes sociais nos quais os indivíduos desenvolvem suas interações.

Quanto maior a capacidade de capturar atenção, maior tende a ser o valor econômico dos conteúdos para as plataformas. Consequentemente, sistemas de recomendação são frequentemente desenvolvidos para identificar quais informações possuem maior potencial de manter os usuários conectados por períodos prolongados.

O problema surge porque conteúdos emocionalmente intensos costumam apresentar desempenho superior nesse aspecto.

Pesquisas desenvolvidas no campo da psicologia social indicam que emoções relacionadas ao medo, à indignação, à hostilidade e ao ressentimento frequentemente geram elevados níveis de interação digital.

Conteúdos capazes de despertar essas emoções tendem a ser mais compartilhados, comentados e consumidos.

Como consequência, existe o risco de que sistemas orientados predominantemente por métricas de engajamento favoreçam a circulação de mensagens polarizadoras ou extremistas.

Importa destacar que a maioria dos pesquisadores não sustenta que os algoritmos possuam intenção própria ou promovam deliberadamente discursos de ódio.

A questão central reside na lógica estrutural que orienta seu funcionamento.

Quando o principal objetivo de um sistema consiste em maximizar atenção e permanência dos usuários, conteúdos emocionalmente intensos frequentemente recebem vantagens competitivas em relação a informações moderadas ou equilibradas.

Se os algoritmos contribuem para ampliar a visibilidade de conteúdos polarizadores, torna-se necessário investigar seus impactos sobre os processos de radicalização e disseminação do extremismo.

Diversos estudos recentes sugerem que sistemas de recomendação podem favorecer trajetórias progressivas de exposição a conteúdos cada vez mais extremos.

O mecanismo é relativamente simples.

Ao identificar interesse do usuário por determinado tema, o algoritmo tende a recomendar conteúdos relacionados. Em busca de maximizar engajamento, as recomendações podem tornar-se gradualmente mais intensas, controversas ou emocionalmente estimulantes.

Embora nem todos os usuários sigam esse percurso, a lógica do sistema cria condições potencialmente favoráveis para a ampliação da polarização.

Cass Sunstein observa que a exposição contínua a conteúdos ideologicamente homogêneos reduz oportunidades de contato com perspectivas divergentes e fortalece processos de polarização grupal.

Quando essa dinâmica se combina com sistemas automatizados de recomendação, os riscos tornam-se ainda maiores.

O usuário não apenas escolhe consumir determinados conteúdos. Ele passa a receber estímulos constantes direcionados à manutenção e aprofundamento de suas preferências previamente identificadas.

A consequência pode ser a formação de ciclos de retroalimentação ideológica.

Comunidades extremistas tornam-se progressivamente mais fechadas e resistentes a perspectivas externas. Narrativas discriminatórias passam a circular sem contestação significativa. Teorias conspiratórias são reforçadas por conteúdos sucessivos que aparentam confirmar percepções já existentes.

Sob determinadas circunstâncias, esse ambiente pode favorecer processos de radicalização capazes de culminar na prática de crimes de ódio ou outras formas de violência.

A preocupação não é meramente teórica.

Nos últimos anos, diversos episódios envolvendo ataques motivados por extremismo ideológico revelaram a existência de vínculos entre processos de radicalização e comunidades digitais estruturadas em torno de discursos de ódio.

Embora a relação causal entre consumo de conteúdo online e prática de violência seja extremamente complexa, existe crescente consenso de que os ambientes digitais desempenham papel relevante na socialização de indivíduos envolvidos nesses processos.

A criminologia digital não pode ignorar essa realidade.

A análise da criminalidade contemporânea exige considerar não apenas os agentes diretamente responsáveis pelos delitos, mas também os fatores estruturais que influenciam a formação de comportamentos e crenças.

Os algoritmos não substituem a responsabilidade individual dos infratores. Entretanto, participam da construção dos ambientes sociais em que determinadas formas de radicalização se desenvolvem.

Essa constatação conduz a um dos debates mais relevantes da atualidade: a definição dos limites entre liberdade de expressão, moderação de conteúdo e combate aos discursos de ódio.

Se as plataformas digitais exercem influência significativa sobre a circulação das informações, surge a questão sobre quais responsabilidades devem assumir diante da

disseminação de conteúdos discriminatórios ou potencialmente violentos.

A resposta exige análise cuidadosa dos direitos fundamentais envolvidos, especialmente da liberdade de expressão e da proteção da dignidade humana. É justamente essa discussão que será desenvolvida no próximo tópico.

3.4 Liberdade de expressão e discurso de ódio

A análise dos crimes de ódio praticados no ambiente digital conduz inevitavelmente a uma das discussões mais complexas do constitucionalismo contemporâneo: a definição dos limites da liberdade de expressão diante da disseminação de discursos discriminatórios. Trata-se de um debate que envolve valores fundamentais para as sociedades democráticas e que se tornou ainda mais relevante com a expansão das redes sociais e das plataformas digitais.

A liberdade de expressão ocupa posição central nos Estados Democráticos de Direito. Sua importância decorre do papel que desempenha na formação da opinião pública, na circulação de informações e no controle social exercido sobre os poderes públicos.

No ordenamento jurídico brasileiro, a proteção da liberdade de expressão encontra fundamento em diversos dispositivos constitucionais.

O artigo 5º, inciso IV, assegura a livre manifestação do pensamento. O inciso IX protege a livre expressão da atividade intelectual, artística, científica e de comunicação. O artigo 220 da Constituição Federal estabelece que a manifestação do pensamento, a criação, a expressão e a informação não sofrerão qualquer restrição, observado o próprio texto constitucional.

Essas garantias refletem o reconhecimento de que sociedades democráticas dependem da existência de espaços abertos ao debate público e à pluralidade de ideias.

Contudo, a liberdade de expressão não possui caráter absoluto.

A própria Constituição Federal estabelece mecanismos de proteção à honra, à intimidade, à imagem, à igualdade e à dignidade da pessoa humana.

A tensão entre esses valores torna-se particularmente intensa quando se analisam manifestações discriminatórias dirigidas a grupos historicamente vulnerabilizados.

Nesse contexto, surge a discussão sobre o chamado discurso de ódio (*hate speech*).

Embora não exista definição única e universalmente aceita, a expressão costuma ser utilizada para designar manifestações destinadas a promover hostilidade, discriminação, inferiorização ou violência contra indivíduos ou grupos em razão de características identitárias específicas.

Jeremy Waldron, em *The Harm in Hate Speech* (2012), sustenta que o discurso de ódio não representa apenas a comunicação de opiniões ofensivas.

Segundo o autor, o propósito do discurso de ódio é minar a confiança fundamental de uma pessoa de que ela pode viver em sociedade como um membro plenamente respeitado e reconhecido. (WALDRON, 2012, p. 87, tradução própria).

A reflexão evidencia que o problema não se limita ao desconforto emocional eventualmente causado por manifestações ofensivas.

O discurso de ódio pode produzir efeitos concretos sobre a participação social, a segurança e a dignidade dos indivíduos pertencentes aos grupos atingidos.

A criminologia contemporânea reconhece que manifestações discriminatórias frequentemente desempenham papel relevante na legitimação de práticas mais amplas de exclusão e violência.

A normalização de discursos racistas, antissemitas, homofóbicos ou misóginos contribui para a construção de ambientes sociais nos quais comportamentos agressivos tornam-se progressivamente mais aceitáveis.

Sob essa perspectiva, o discurso de ódio não constitui apenas um problema comunicacional. Trata-se também de fenômeno relacionado à produção e reprodução de desigualdades estruturais.

No Brasil, o principal precedente judicial relacionado ao tema é o julgamento do Habeas Corpus nº 82.424/RS, conhecido como Caso Ellwanger.

O caso envolveu a condenação do escritor Siegfried Ellwanger pela publicação de obras de conteúdo antissemita.

Ao analisar a controvérsia, o Supremo Tribunal Federal enfrentou diretamente a questão relativa aos limites da liberdade de expressão diante de manifestações discriminatórias.

No julgamento, prevaleceu o entendimento de que a proteção constitucional da liberdade de expressão não abrange discursos destinados à propagação do racismo e da intolerância.

Em voto amplamente citado pela doutrina constitucional brasileira, o Ministro Celso de Mello destacou que os direitos fundamentais devem ser interpretados em harmonia com os princípios da dignidade da pessoa humana e da igualdade material.

O STF concluiu que manifestações voltadas à negação da dignidade de determinados grupos não podem ser legitimadas sob o argumento da liberdade de expressão.

A decisão representa marco importante na jurisprudência constitucional brasileira porque reafirma a inexistência de direitos fundamentais absolutos.

A liberdade de expressão possui posição preferencial nas democracias

contemporâneas, mas essa proteção não autoriza a promoção de práticas incompatíveis com os valores fundamentais da ordem constitucional.

Entretanto, a aplicação desses princípios ao ambiente digital apresenta desafios específicos.

As plataformas digitais ampliaram significativamente a capacidade de circulação de conteúdos potencialmente discriminatórios.

Ao mesmo tempo, a remoção de conteúdos e a restrição de manifestações em redes sociais suscitam preocupações relacionadas à censura, ao pluralismo e à liberdade de debate público.

Essa tensão tornou-se objeto de intenso debate doutrinário.

De um lado, autores enfatizam a necessidade de combater discursos capazes de promover discriminação e violência contra grupos vulneráveis.

De outro, destaca-se o risco de atribuir a plataformas privadas poderes excessivos para definir unilateralmente quais conteúdos podem ou não circular na esfera pública digital.

O problema torna-se ainda mais complexo quando se observa que grande parte do debate público contemporâneo ocorre justamente nessas plataformas.

A decisão de remover uma publicação, suspender uma conta ou restringir determinado conteúdo pode produzir impactos significativos sobre o exercício da liberdade de expressão.

Nesse contexto, ganha relevância a discussão sobre a responsabilidade das plataformas digitais.

A Lei nº 12.965/2014 (Marco Civil da Internet) buscou enfrentar essa questão por meio da adoção de modelo que, em regra, condiciona a responsabilização dos provedores ao descumprimento de ordem judicial específica.

O artigo 19 do Marco Civil estabelece que os provedores de aplicações de internet somente poderão ser responsabilizados civilmente por danos decorrentes de conteúdo gerado por terceiros, caso, após ordem judicial específica, deixem de promover sua remoção.

A opção legislativa buscou evitar práticas de censura privada e preservar a liberdade de expressão no ambiente digital.

Contudo, a evolução das plataformas digitais e o crescimento dos discursos de ódio intensificaram críticas a esse modelo.

Diversos autores sustentam que a velocidade de propagação dos conteúdos ilícitos exige mecanismos mais ágeis de resposta, especialmente em situações envolvendo discriminação, perseguição virtual e incitação à violência.

Outros argumentam que a ampliação das responsabilidades das plataformas pode gerar incentivos para remoções excessivas de conteúdo, comprometendo a pluralidade do debate público.

A controvérsia permanece aberta tanto na doutrina quanto na jurisprudência.

Sob a perspectiva criminológica, entretanto, uma conclusão parece relativamente consolidada: os crimes de ódio praticados no ambiente digital não podem ser analisados exclusivamente a partir da lógica da liberdade de expressão.

Embora a proteção ao debate público seja essencial para a democracia, discursos destinados à desumanização de grupos sociais produzem efeitos concretos sobre a segurança, a dignidade e a igualdade dos indivíduos atingidos.

A sociedade digital exige, portanto, mecanismos capazes de compatibilizar a proteção da liberdade de expressão com a tutela dos direitos fundamentais das vítimas de discriminação.

Esse desafio torna-se ainda mais complexo quando se considera que as plataformas digitais operam por meio da coleta massiva de dados pessoais e da utilização de sistemas algorítmicos altamente sofisticados.

A análise dessas questões conduz diretamente ao próximo tema da pesquisa: a proteção de dados pessoais como direito fundamental e os impactos da Lei Geral de Proteção de Dados na sociedade digital contemporânea.

3.5 A proteção de dados pessoais como direito fundamental

A consolidação da sociedade digital produziu uma transformação profunda na forma como informações pessoais são coletadas, armazenadas, processadas e compartilhadas. Se durante grande parte do século XX a privacidade estava associada principalmente à proteção da vida íntima contra interferências indevidas, o avanço das tecnologias informacionais revelou a necessidade de uma abordagem mais ampla e sofisticada, capaz de enfrentar os desafios decorrentes da circulação massiva de dados em ambientes digitais.

Nesse contexto, a proteção de dados pessoais passou gradualmente a ser reconhecida como direito autônomo, dotado de relevância própria e distinto da concepção clássica de privacidade.

A evolução desse entendimento pode ser observada especialmente na doutrina europeia, que desempenhou papel fundamental na construção dos fundamentos teóricos da proteção de dados contemporânea.

Entre os principais autores responsáveis por esse desenvolvimento destaca-se Stefano Rodotà.

Em suas reflexões sobre a sociedade informacional, Rodotà sustenta que o crescente poder exercido por governos e corporações sobre informações pessoais exige a construção de novos mecanismos jurídicos de proteção da liberdade individual. Segundo o autor, a proteção dos dados pessoais tornou-se uma condição necessária para o exercício das liberdades fundamentais. ” (RODOTÀ, 2008, p. 92). A afirmação revela uma mudança significativa de perspectiva.

Os dados pessoais deixam de ser compreendidos apenas como informações privadas pertencentes ao indivíduo. Passam a ser reconhecidos como elementos essenciais para a construção da autonomia, da identidade e da participação democrática.

A preocupação torna-se ainda mais relevante quando se observa a crescente capacidade tecnológica de coleta e processamento de informações.

Empresas privadas, plataformas digitais, instituições financeiras e órgãos governamentais passaram a acumular quantidades sem precedentes de dados sobre hábitos, preferências, deslocamentos, relações sociais e comportamentos dos indivíduos.

Na sociedade digital, praticamente todas as atividades humanas produzem rastros informacionais passíveis de registro e análise.

Pesquisas realizadas na internet, interações em redes sociais, compras online, utilização de aplicativos de mobilidade e simples navegação em páginas eletrônicas geram informações que podem ser armazenadas e utilizadas para múltiplas finalidades.

A consequência é o surgimento de novas formas de poder informacional.

Conforme observa Rodotà, a capacidade de conhecer detalhadamente os comportamentos dos indivíduos cria condições para influenciar decisões, direcionar escolhas e limitar espaços de autonomia pessoal.

Essa preocupação também foi amplamente desenvolvida na doutrina brasileira.

Danilo Doneda, um dos principais estudiosos da proteção de dados no Brasil, sustenta que o direito à proteção de dados deve ser compreendido como instrumento destinado a assegurar a autodeterminação informativa dos indivíduos.

Segundo o autor, a proteção de dados pessoais visa assegurar ao indivíduo o controle sobre as informações que lhe dizem respeito. ” (DONEDA, 2021, p. 27).

A noção de autodeterminação informativa possui origem na jurisprudência constitucional alemã, especialmente na decisão proferida pelo Tribunal Constitucional Federal da Alemanha no denominado Caso do Censo (*Volkszählungsurteil*), em 1983.

Na ocasião, a Corte reconheceu que a liberdade individual pressupõe a possibilidade de controlar a circulação e utilização das próprias informações pessoais.

Esse entendimento exerceu profunda influência sobre os sistemas contemporâneos de proteção de dados.

No Brasil, a consolidação desse movimento ocorreu por meio da promulgação da Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD).

Inspirada em grande medida pelo Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a LGPD estabeleceu princípios, direitos e deveres relacionados ao tratamento de dados pessoais por agentes públicos e privados.

O artigo 6º da lei consagra princípios fundamentais como finalidade, adequação, necessidade, transparência, segurança, prevenção e responsabilização.

A adoção desses princípios demonstra que a proteção de dados não se limita à proibição da coleta de informações. O objetivo consiste em assegurar que o tratamento de dados ocorra de maneira legítima, proporcional e compatível com os direitos fundamentais dos titulares.

Laura Schertel Mendes observa que a proteção de dados deve ser compreendida como instrumento de equilíbrio entre inovação tecnológica e proteção da dignidade humana.

Segundo a autora, “a disciplina da proteção de dados busca compatibilizar desenvolvimento tecnológico, livre iniciativa e tutela dos direitos fundamentais. ” (MENDES, 2014, p. 87).

A observação é particularmente relevante porque afasta interpretações que apresentam a proteção de dados como obstáculo ao desenvolvimento econômico ou à inovação tecnológica.

A LGPD não pretende impedir a utilização de dados pessoais. Seu objetivo consiste em estabelecer limites jurídicos para essa utilização, garantindo que ela ocorra em conformidade com os princípios constitucionais.

A importância da proteção de dados foi ainda mais reforçada pela Emenda Constitucional nº 115, de 2022.

A referida emenda introduziu o inciso LXXIX ao artigo 5º da Constituição Federal, estabelecendo expressamente que:

“é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.”

A constitucionalização da proteção de dados representa marco de enorme relevância jurídica.

Ao elevar esse direito ao patamar constitucional, o constituinte reconheceu que a sociedade digital exige novos mecanismos de proteção das liberdades fundamentais.

Sob a perspectiva criminológica, essa evolução possui implicações significativas.

A proteção dos dados pessoais não se relaciona apenas às atividades desenvolvidas por empresas privadas. Ela também influencia diretamente as formas pelas quais o Estado exerce funções de vigilância, investigação e persecução penal.

A crescente digitalização das relações sociais ampliou significativamente a quantidade de informações potencialmente disponíveis para utilização em investigações criminais.

Registros de acesso, históricos de navegação, dados de localização, comunicações eletrônicas e informações armazenadas em plataformas digitais passaram a desempenhar papel cada vez mais relevante na produção da prova penal.

Essa realidade produz uma tensão permanente entre dois valores igualmente relevantes: a proteção da privacidade e a eficiência da investigação criminal.

A solução desse conflito exige abordagem cuidadosa, capaz de evitar tanto a inviabilização das atividades investigativas quanto a legitimação de práticas incompatíveis com os direitos fundamentais.

A proteção de dados não pode ser compreendida como obstáculo absoluto à persecução penal. Tampouco pode ser reduzida a simples formalidade passível de afastamento diante de interesses investigativos.

O verdadeiro desafio consiste em construir mecanismos institucionais capazes de compatibilizar segurança pública, eficiência investigativa e proteção das liberdades fundamentais.

É justamente essa tensão entre proteção de dados e investigação criminal que será analisada no próximo tópico, dedicado aos impactos da LGPD sobre a atividade estatal de persecução penal e sobre os limites jurídicos da vigilância digital.

3.6 LGPD, investigação criminal e vigilância estatal

A crescente digitalização das relações sociais transformou profundamente as formas de produção da prova penal e de desenvolvimento das atividades investigativas. Se durante grande parte do século XX a investigação criminal dependia predominantemente de testemunhos, documentos físicos e diligências presenciais, a sociedade digital passou a produzir quantidades massivas de informações potencialmente relevantes para a persecução penal.

Registros de acesso à internet, históricos de navegação, dados de geolocalização, comunicações eletrônicas, metadados de aplicativos, movimentações financeiras digitais e interações em redes sociais passaram a constituir importantes fontes probatórias para a

investigação de infrações penais.

Essa transformação ampliou significativamente a capacidade estatal de reconstrução de comportamentos individuais.

Entretanto, também produziu novos desafios relacionados à proteção dos direitos fundamentais.

A possibilidade tecnológica de acesso a informações pessoais em larga escala exige a definição de limites jurídicos claros para a atuação estatal.

Nesse contexto, surge uma tensão permanente entre dois objetivos igualmente legítimos: de um lado, a necessidade de promover investigações eficazes e proteger a sociedade contra práticas criminosas; de outro, a obrigação constitucional de preservar direitos fundamentais relacionados à privacidade, à liberdade e à proteção de dados pessoais.

A discussão torna-se especialmente relevante quando se observa que a coleta de dados digitais permite formas de monitoramento significativamente mais invasivas do que aquelas tradicionalmente disponíveis ao Estado.

A obtenção de registros telemáticos pode revelar hábitos cotidianos, relações pessoais, preferências políticas, deslocamentos físicos e aspectos extremamente sensíveis da vida privada dos indivíduos.

Por essa razão, a utilização dessas informações não pode ocorrer sem observância rigorosa dos parâmetros constitucionais.

Nesse ponto, as contribuições de Luigi Ferrajoli mostram-se particularmente relevantes.

Em sua teoria do garantismo penal, desenvolvida especialmente na obra *Direito e Razão* (1989), Ferrajoli sustenta que o exercício do poder punitivo deve estar permanentemente submetido a limites jurídicos destinados à proteção da liberdade individual.

Segundo o autor, “os direitos fundamentais configuram-se como vínculos substanciais impostos ao exercício de todos os poderes. ” (FERRAJOLI, 2014, p. 37).

O avanço tecnológico ampliou significativamente as capacidades investigativas do Estado. Contudo, a mera possibilidade técnica de obtenção de determinadas informações não implica sua legitimidade jurídica.

A atuação estatal continua condicionada pelos princípios da legalidade, proporcionalidade, necessidade e controle jurisdicional.

A proteção de dados pessoais, reconhecida constitucionalmente pela Emenda Constitucional nº 115/2022, reforça ainda mais essa exigência.

Embora a própria LGPD exclua de sua incidência direta determinadas atividades

relacionadas à segurança pública e à investigação criminal, isso não significa ausência de limites jurídicos para a atuação estatal.

Pelo contrário.

As atividades investigativas continuam submetidas ao regime constitucional de proteção dos direitos fundamentais.

A obtenção de dados pessoais para fins de persecução penal deve observar requisitos rigorosos relacionados à necessidade, adequação e proporcionalidade das medidas adotadas.

Esse entendimento encontra respaldo na jurisprudência dos tribunais constitucionais contemporâneos e na própria evolução do direito internacional dos direitos humanos.

A preocupação torna-se ainda mais relevante diante do crescimento dos mecanismos de vigilância digital.

A utilização de tecnologias de monitoramento em massa, reconhecimento facial, análise preditiva de comportamento e inteligência artificial para fins de segurança pública passou a integrar o debate jurídico em diferentes países.

Embora essas ferramentas sejam frequentemente apresentadas como instrumentos de modernização das investigações criminais, sua utilização suscita importantes questionamentos éticos e constitucionais.

Nesse contexto, as reflexões de Michel Foucault permanecem extremamente atuais.

Em *Vigiar e Punir* (1975), o autor analisa a evolução histórica das formas de exercício do poder disciplinar e destaca a centralidade da vigilância na organização das sociedades modernas.

Ao examinar o modelo do Panóptico concebido por Jeremy Bentham, Foucault demonstra como a possibilidade permanente de observação influencia comportamentos e produz mecanismos de autocontrole social. Segundo o autor, “o princípio é conhecido: na periferia, uma construção em anel; no centro, uma torre; esta possui largas janelas que se abrem sobre a face interna do anel. ” (FOUCAULT, 2014, p. 190).

Mais importante do que a descrição arquitetônica é a lógica de funcionamento identificada por Foucault.

O indivíduo submetido à possibilidade constante de vigilância tende a modificar espontaneamente seu comportamento, internalizando mecanismos de disciplina e controle.

Embora o modelo analisado por Foucault tenha sido concebido em contexto anterior à internet, diversos autores identificam paralelos significativos entre o panoptismo clássico e os sistemas contemporâneos de monitoramento digital.

A principal diferença reside na escala.

As tecnologias digitais permitem formas de vigilância muito mais abrangentes, contínuas e sofisticadas do que aquelas disponíveis nos modelos históricos analisados pelo filósofo francês.

A coleta automatizada de dados possibilita monitoramento permanente de grandes populações sem necessidade de observação física direta.

Essa realidade produz preocupações legítimas relacionadas à preservação das liberdades individuais.

A criminologia crítica alerta que o combate à criminalidade não pode servir como justificativa para a expansão ilimitada dos mecanismos de vigilância estatal.

A história demonstra que poderes extraordinários conferidos ao Estado em contextos de insegurança frequentemente permanecem ativos mesmo após o desaparecimento das circunstâncias que inicialmente justificaram sua criação.

Sob essa perspectiva, a proteção de dados pessoais desempenha papel fundamental como instrumento de contenção do poder estatal.

A exigência de autorização judicial, fundamentação adequada e observância dos princípios da proporcionalidade e necessidade constitui mecanismo essencial para evitar abusos incompatíveis com o Estado Democrático de Direito.

Importa destacar que a defesa das garantias fundamentais não implica desconsideração da importância da investigação criminal.

A criminalidade digital frequentemente envolve condutas complexas, transnacionais e altamente sofisticadas, exigindo instrumentos investigativos compatíveis com essa realidade.

O verdadeiro desafio consiste em construir modelos institucionais capazes de conciliar eficiência investigativa e proteção das liberdades individuais.

A falsa oposição entre privacidade e segurança pública frequentemente obscurece essa discussão.

Não se trata de escolher entre direitos fundamentais e combate à criminalidade.

O objetivo consiste em desenvolver mecanismos que permitam a realização simultânea de ambos os valores.

A proteção dos dados pessoais fortalece a legitimidade das instituições públicas e contribui para a construção de sistemas investigativos mais transparentes e compatíveis com os princípios constitucionais.

Diante dessas considerações, torna-se evidente que a sociedade digital exige novas formas de equilíbrio entre vigilância, investigação e proteção dos direitos fundamentais.

A análise dessa relação conduz diretamente ao último tópico deste capítulo, dedicado

à discussão sobre privacidade, segurança pública e os desafios da democracia na era digital.

3.7 Privacidade, segurança pública e democracia digital

A consolidação da sociedade digital produziu um dos debates mais relevantes do constitucionalismo contemporâneo: a relação entre privacidade, segurança pública e democracia. O crescimento dos delitos virtuais, a ampliação das capacidades tecnológicas de monitoramento e a crescente dependência social das plataformas digitais criaram um cenário no qual a proteção dos direitos fundamentais passou a conviver com demandas cada vez mais intensas por mecanismos de vigilância e controle.

Frequentemente, o debate público apresenta essas questões sob a forma de uma suposta oposição entre privacidade e segurança. Segundo essa perspectiva, o fortalecimento das garantias relacionadas à proteção de dados e à privacidade dificultaria a atuação dos órgãos de investigação criminal, comprometendo a eficiência das políticas de segurança pública.

Essa formulação, contudo, revela-se excessivamente simplificadora.

A proteção da privacidade não constitui obstáculo ao funcionamento legítimo das instituições responsáveis pela persecução penal. Pelo contrário, representa elemento indispensável para a preservação das liberdades que caracterizam o Estado Democrático de Direito.

Nesse sentido, Stefano Rodotà sustenta que a privacidade contemporânea não deve ser compreendida apenas como direito ao isolamento ou à reserva da vida pessoal. Em uma sociedade marcada pela circulação permanente de informações, a proteção dos dados pessoais torna-se condição para o exercício efetivo da cidadania e da autonomia individual. Segundo o autor, “a privacidade deixou de ser o direito de ser deixado em paz para tornar-se o direito de manter o controle sobre as informações que dizem respeito à própria pessoa. ” (RODOTÀ, 2008, p. 93).

A preservação de espaços de autonomia informacional constitui requisito para o funcionamento saudável das instituições democráticas.

Sociedades nas quais indivíduos são permanentemente monitorados tendem a produzir restrições indiretas ao exercício da liberdade de expressão, da participação política e da liberdade de associação.

O problema torna-se ainda mais relevante quando se observa a crescente capacidade tecnológica de monitoramento.

A evolução dos sistemas de inteligência artificial, análise comportamental, reconhecimento facial e processamento massivo de dados criou possibilidades de vigilância

sem precedentes históricos.

A simples existência dessas tecnologias não implica necessariamente sua incompatibilidade com a democracia. Entretanto, exige a construção de mecanismos jurídicos rigorosos capazes de limitar sua utilização e impedir abusos.

A busca por eficiência investigativa não pode justificar a relativização indiscriminada de garantias constitucionais. A legitimidade da atuação estatal depende justamente de sua capacidade de respeitar os limites impostos pelo ordenamento jurídico.

A proteção da privacidade, portanto, não constitui obstáculo à democracia. Trata-se de um de seus pressupostos fundamentais.

Sob a perspectiva criminológica, essa discussão conecta-se diretamente às críticas formuladas por Eugenio Raúl Zaffaroni em relação à expansão do poder punitivo.

Ao analisar a evolução dos sistemas penais contemporâneos, Zaffaroni alerta para a tendência de utilização do direito penal como instrumento simbólico de resposta a problemas sociais complexos.

Embora a observação tenha sido formulada em contexto anterior à consolidação das redes sociais, sua atualidade é evidente.

A criminalidade digital frequentemente desperta forte sensação de vulnerabilidade social. Ataques cibernéticos, fraudes eletrônicas, vazamentos de dados e campanhas de desinformação produzem legítima preocupação coletiva.

Entretanto, a resposta a esses fenômenos não pode consistir simplesmente na ampliação contínua dos mecanismos de vigilância.

A história demonstra que poderes excepcionais conferidos ao Estado em contextos de crise frequentemente permanecem ativos mesmo após o desaparecimento das circunstâncias que inicialmente justificaram sua adoção.

A proteção dos direitos fundamentais funciona precisamente como mecanismo destinado a evitar essa expansão descontrolada.

Outro aspecto relevante refere-se ao papel desempenhado pelas empresas privadas na organização dos fluxos informacionais contemporâneos.

A sociedade digital produziu concentração sem precedentes de poder econômico e informacional nas mãos de grandes plataformas tecnológicas.

Essas empresas não apenas armazenam quantidades massivas de dados pessoais, mas também exercem significativa influência sobre a circulação de informações, a formação da opinião pública e a estruturação das interações sociais.

Consequentemente, a proteção da democracia digital exige atenção não apenas à

atuação do Estado, mas também ao poder exercido por agentes privados.

A preocupação com a vigilância não pode ser direcionada exclusivamente às instituições públicas.

O monitoramento permanente realizado por plataformas digitais também produz impactos significativos sobre a autonomia individual e sobre o exercício das liberdades fundamentais.

Nesse sentido, a LGPD representa importante instrumento de equilíbrio institucional.

Ao estabelecer limites para a coleta e utilização de dados pessoais, a legislação busca reduzir assimetrias de poder informacional e fortalecer a posição jurídica dos cidadãos diante de organizações públicas e privadas.

A proteção dos dados pessoais passa a funcionar, assim, como mecanismo de preservação democrática.

Essa perspectiva afasta interpretações que reduzem a LGPD a mero conjunto de regras administrativas voltadas à proteção da privacidade.

A proteção de dados deve ser compreendida como elemento integrante da própria estrutura constitucional destinada à tutela da dignidade humana, da liberdade e da cidadania.

A sociedade digital exige novas formas de proteção dos direitos fundamentais.

Se a revolução industrial impôs a construção de direitos sociais destinados a limitar desigualdades econômicas, a revolução informacional exige a consolidação de garantias capazes de proteger os indivíduos diante das novas formas de poder produzidas pela circulação massiva de informações.

Diante dessas considerações, torna-se possível concluir que a privacidade e a segurança pública não constituem valores necessariamente antagônicos.

Ambas representam dimensões essenciais de uma ordem democrática comprometida simultaneamente com a proteção dos direitos fundamentais e com a preservação da segurança coletiva.

O verdadeiro desafio da sociedade digital não consiste em escolher entre liberdade e segurança, mas em construir mecanismos institucionais capazes de compatibilizar esses valores sem comprometer os fundamentos do Estado Democrático de Direito.

A partir das reflexões desenvolvidas ao longo deste capítulo, verifica-se que os crimes de ódio, os processos de radicalização digital e os impactos da proteção de dados pessoais não podem ser compreendidos de forma isolada. Todos esses fenômenos encontram-se profundamente conectados às transformações produzidas pela sociedade em rede, pela economia da atenção e pelo crescente poder das plataformas digitais.

CONCLUSÃO

A presente pesquisa teve como objetivo analisar criticamente os fatores criminológicos relacionados aos delitos virtuais, aos crimes de ódio praticados nas redes sociais e aos impactos da proteção de dados pessoais na sociedade digital contemporânea. Partiu-se da hipótese de que os fenômenos criminais observados no ambiente digital não podem ser adequadamente compreendidos a partir dos modelos criminológicos tradicionais centrados exclusivamente nas características individuais dos infratores. Ao longo do trabalho, buscou-se demonstrar que a revolução tecnológica produziu transformações estruturais capazes de alterar profundamente as formas de socialização, interação humana, controle social e produção da criminalidade.

A análise desenvolvida permitiu concluir que a internet não representa apenas um novo espaço para a prática de crimes previamente existentes. O ambiente digital criou condições específicas que influenciam oportunidades criminosas, processos de aprendizagem social e mecanismos de radicalização. O surgimento da criminologia digital decorre justamente da necessidade de compreender essas novas dinâmicas e de reinterpretar as teorias criminológicas clássicas à luz das transformações produzidas pela sociedade em rede.

Verificou-se que importantes contribuições da criminologia tradicional permanecem plenamente relevantes para a compreensão da criminalidade contemporânea. A Teoria da Associação Diferencial de Edwin H. Sutherland continua oferecendo importante explicação para os processos de aprendizagem criminal observados nas comunidades digitais. Da mesma forma, a Teoria da Anomia de Robert K. Merton demonstra grande capacidade explicativa ao evidenciar como pressões relacionadas ao sucesso econômico e ao reconhecimento social podem influenciar a prática de delitos virtuais.

Entretanto, a pesquisa também demonstrou que essas teorias, isoladamente consideradas, não são suficientes para explicar a complexidade dos fenômenos observados na sociedade digital.

Os delitos virtuais desenvolvem-se em ambientes profundamente distintos daqueles analisados pelos criminólogos clássicos. Redes sociais, plataformas digitais, algoritmos de recomendação, sistemas de inteligência artificial e mecanismos de vigilância em massa passaram a exercer influência significativa sobre comportamentos individuais e coletivos.

A principal conclusão alcançada pelo trabalho consiste justamente no reconhecimento de que as estruturas tecnológicas contemporâneas não podem ser tratadas como elementos neutros na análise criminológica.

Ao longo da pesquisa demonstrou-se que plataformas digitais operam segundo

modelos econômicos baseados na captura da atenção e na coleta permanente de dados comportamentais. O capitalismo de vigilância produz incentivos específicos que influenciam a circulação de informações e a organização das interações sociais.

Os algoritmos responsáveis pela seleção e recomendação de conteúdos desempenham papel ativo na construção dos ambientes digitais. Embora não sejam diretamente responsáveis pela criminalidade, influenciam significativamente a forma como os indivíduos são expostos a informações, comunidades e narrativas específicas.

Essa constatação conduz a uma importante revisão dos paradigmas criminológicos tradicionais.

Durante grande parte de sua história, a criminologia concentrou seus esforços na identificação de fatores individuais ou sociais associados ao comportamento criminoso. A sociedade digital exige ampliação desse campo de análise para incluir também os impactos produzidos pela arquitetura tecnológica dos ambientes virtuais.

Em outras palavras, a compreensão da criminalidade contemporânea exige investigar não apenas quem pratica os delitos, mas também em quais ambientes sociais e tecnológicos esses comportamentos se desenvolvem.

Essa conclusão mostrou-se particularmente relevante na análise dos crimes de ódio e dos processos de radicalização digital.

A pesquisa demonstrou que o ambiente virtual ampliou significativamente a capacidade de circulação de discursos discriminatórios e narrativas extremistas. A formação de comunidades digitais estruturadas em torno de identidades compartilhadas, associada aos mecanismos de recomendação algorítmica e à lógica da economia da atenção, cria condições favoráveis ao fortalecimento de câmaras de eco e processos de polarização grupal.

Nesse contexto, verificou-se que os crimes de ódio não podem ser compreendidos apenas como manifestações isoladas de intolerância individual. Conforme sustentado por Barbara Perry, tais condutas constituem mecanismos de reafirmação de relações históricas de poder e exclusão social.

A internet não cria essas desigualdades, mas amplia significativamente sua capacidade de reprodução e disseminação.

A pesquisa também permitiu concluir que os processos de radicalização observados nas plataformas digitais resultam da interação entre fatores individuais, dinâmicas grupais e estruturas tecnológicas.

Os algoritmos não produzem automaticamente o extremismo, mas podem atuar como amplificadores de tendências já existentes ao favorecer a exposição contínua a conteúdos

homogêneos e emocionalmente intensos.

Essa realidade impõe desafios significativos às instituições democráticas contemporâneas.

O enfrentamento dos crimes de ódio e da radicalização digital não pode ser reduzido à simples ampliação das respostas penais. Estratégias exclusivamente repressivas mostram-se insuficientes diante de fenômenos cuja origem está associada a processos complexos de socialização e construção identitária.

A prevenção exige políticas públicas voltadas à educação digital, ao fortalecimento da alfabetização midiática e à promoção de ambientes digitais compatíveis com os valores democráticos.

Outro aspecto fundamental analisado pela pesquisa refere-se à proteção dos dados pessoais e aos impactos da Lei Geral de Proteção de Dados.

A investigação demonstrou que a proteção de dados deve ser compreendida como direito fundamental indispensável para a preservação da autonomia individual e para o funcionamento saudável das instituições democráticas.

A constitucionalização desse direito por meio da Emenda Constitucional nº 115/2022 representa reconhecimento formal de que a sociedade digital exige novas formas de proteção das liberdades fundamentais.

A pesquisa permitiu concluir que a proteção de dados não constitui obstáculo à investigação criminal ou à segurança pública.

A verdadeira questão consiste em estabelecer mecanismos institucionais capazes de compatibilizar eficiência investigativa e proteção dos direitos fundamentais.

Nesse sentido, as contribuições garantistas de Luigi Ferrajoli revelam-se especialmente relevantes. O avanço tecnológico ampliou significativamente as capacidades de vigilância do Estado, mas não eliminou a necessidade de observância dos princípios da legalidade, proporcionalidade e controle jurisdicional.

Ao contrário, quanto maiores os poderes tecnológicos disponíveis, maior deve ser a preocupação com os mecanismos destinados a limitar seu exercício.

A análise desenvolvida também evidenciou a atualidade das reflexões de Michel Foucault sobre vigilância e controle social.

A sociedade digital produziu formas de monitoramento muito mais sofisticadas do que aquelas existentes nos modelos disciplinares clássicos. Contudo, os riscos relacionados à concentração de poder informacional e à expansão dos mecanismos de vigilância permanecem essencialmente os mesmos.

A proteção da privacidade e dos dados pessoais surge, assim, como instrumento indispensável para evitar a transformação da segurança em justificativa permanente para a ampliação descontrolada do monitoramento estatal e corporativo.

Sob uma perspectiva mais ampla, a pesquisa permite concluir que a criminalidade digital representa fenômeno inseparável das transformações estruturais produzidas pela sociedade em rede.

Os delitos virtuais, os crimes de ódio, os processos de radicalização e os conflitos relacionados à proteção de dados constituem diferentes manifestações de uma mesma realidade social marcada pela centralidade da informação, pela expansão das tecnologias digitais e pela crescente influência das plataformas sobre a vida cotidiana.

Diante desse cenário, a principal contribuição da criminologia digital consiste em ampliar o horizonte tradicional de análise do fenômeno criminal.

A criminalidade contemporânea não pode ser explicada exclusivamente pela vontade individual dos infratores, nem apenas por fatores econômicos ou sociais tradicionais. Ela deve ser compreendida como resultado da interação entre indivíduos, estruturas sociais e ambientes tecnológicos cada vez mais complexos.

Conclui-se, portanto, que os desafios impostos pela sociedade digital exigem uma criminologia igualmente capaz de dialogar com a complexidade de seu tempo. Uma criminologia que não se limite à análise do crime consumado, mas que investigue criticamente as estruturas de poder, informação e tecnologia que condicionam a produção dos comportamentos desviantes na contemporaneidade.

Somente a partir dessa perspectiva será possível construir respostas jurídicas, políticas e institucionais compatíveis com os valores do Estado Democrático de Direito, assegurando simultaneamente a proteção da liberdade, da dignidade humana, da segurança coletiva e dos direitos fundamentais em uma sociedade cada vez mais conectada e orientada por dados.

REFERÊNCIAS

BARATTA, Alessandro. *Criminologia crítica e crítica do direito penal: introdução à sociologia jurídico-penal*. 6. ed. Rio de Janeiro: Revan, 2011.

BAUMAN, Zygmunt. *Vida para consumo: a transformação das pessoas em mercadoria*. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2008.

BECCARIA, Cesare. *Dos delitos e das penas*. Tradução de Paulo M. Oliveira. São Paulo: Edipro, 2015.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 1988.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Diário Oficial da União, Brasília, DF, 11 fev. 2022.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BUCKELS, Erin E.; TRAPNELL, Paul D.; PAULHUS, Delroy L. *Trolls just want to have fun. Personality and Individual Differences*, Amsterdam, v. 67, p. 97-102, 2014.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 1999. (A Era da Informação: economia, sociedade e cultura, v. 1). ISBN 85-219-0329-4.

CASTELLS, Manuel. *O poder da identidade*. 8. ed. São Paulo: Paz e Terra, 2018. (A era da informação: economia, sociedade e cultura, v. 2).

CHRISTIE, Nils. *A indústria do controle do crime: a caminho dos GULAGs em estilo ocidental*. Rio de Janeiro: Forense, 1998.

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

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados*. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

FERRAJOLI, Luigi. *Direito e razão: teoria do garantismo penal*. 4. ed. São Paulo: Revista dos Tribunais, 2014.

FERRI, Enrico. *Sociologia criminale*. 3. ed. Torino: Fratelli Bocca, 1892.

FOUCAULT, Michel. *Vigiar e punir: nascimento da prisão*. 42. ed. Petrópolis: Vozes, 2014.

HAIDT, Jonathan. *The righteous mind: why good people are divided by politics and religion*. New York: Pantheon Books, 2012.

HAN, Byung-Chul. *Sociedade do cansaço*. 2. ed. Petrópolis: Vozes, 2017.

LESSIG, Lawrence. *Code and other laws of cyberspace*. New York: Basic Books, 1999.

LEVIN, Jack; MCDEVITT, Jack. *Hate crimes revisited: America's war on those who are different*. Boulder: Westview Press, 2009.

LEVY, Pierre. Cibercultura. Tradução de Carlos lrineu da Costa. São Paulo: Editora 34, 1999. (Coleção TRANS).

LEVY, Steven. *Hackers: heroes of the computer revolution*. 25th anniversary edition. Sebastopol: O'Reilly Media, 2010. LOMBROSO, Cesare. L'Uomo Delinquente. Torino: Fratelli Bocca, 1876.

MENDES, Laura Schertel Ferreira. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014.

MERTON, Robert K. Social structure and anomie. *American Sociological Review*, Washington, v. 3, n. 5, p. 672-682, 1938.

PERRY, Barbara. *In the name of hate: understanding hate crimes*. New York: Routledge, 2001.

RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008.

SIMON, Herbert A. Designing organizations for an information-rich world. In: GREENBERGER, Martin (org.). *Computers, communication and the public interest*. Baltimore: Johns Hopkins Press, 1971. p. 37-72.

SULER, John. The online disinhibition effect. *CyberPsychology & Behavior*, New Rochelle, v. 7, n. 3, p. 321-326, 2004. Disponível em: https://johnsuler.com/article_pdfs/online_dis_effect.pdf. Acesso em: jun. 2026.

SUNSTEIN, Cass R. *Republic.com 2.0*. Princeton: Princeton University Press, 2007.

SUNSTEIN, Cass R. *Going to extremes: how like minds unite and divide*. New York: Oxford University Press, 2009.

SUTHERLAND, Edwin H.; CRESSEY, Donald R. *Principles of criminology*. 9. ed. Philadelphia: J. B. Lippincott, 1974.

SUTHERLAND, Edwin H. White-collar criminality. *American Sociological Review*, Washington, v. 5, n. 1, p. 1-12, fev. 1940.

WALDRON, Jeremy. *The harm in hate speech*. Cambridge: Harvard University Press, 2012.

WALL, D.S. (2024) Cybercrime: *The Transformation of Crime in the Information Age*, 2nd edition, Cambridge, Cambridge: Polity. ISBN-10: 0745653529 / ISBN-13: 978-0745653525.

YAR, Majid. *Cybercrime and society*. London: Sage Publications, 2006.

ZAFFARONI, Eugenio Raúl. *Em busca das penas perdidas: a perda da legitimidade do sistema penal*. 5. ed. Rio de Janeiro: Revan, 2001.

ZAFFARONI, Eugenio Raúl; BATISTA, Nilo; ALAGIA, Alejandro; SLOKAR, Alejandro. *Direito penal brasileiro: teoria geral do direito penal*. Rio de Janeiro: Revan, 2003.