

**PERSPECTIVAS PARA UM NOVO DIREITO PENAL NA ERA DIGITAL:
EQUILÍBRIO ENTRE INVESTIGAÇÃO AOS CRIMES VIRTUAIS E PROTEÇÃO DE
DADOS PESSOAIS**

**PERSPECTIVES FOR A NEW CRIMINAL LAW IN THE DIGITAL AGE:
BALANCING INVESTIGATION OF VIRTUAL CRIMES AND PERSONAL DATA
PROTECTION**

**PERSPECTIVAS PARA UN NUEVO DERECHO PENAL EN LA ERA DIGITAL:
EQUILIBRIO ENTRE LA INVESTIGACIÓN DE LOS CRÍMENES VIRTUALES Y LA
PROTECCIÓN DE DATOS PERSONALES**

Melk Gonçalves Mereles ¹
Eudes Aragão da Frota ²

1. INTRODUÇÃO

A consolidação da era digital introduziu transformações profundas no modo como indivíduos se reconhecem, se relacionam e interagem com as instituições públicas e privadas. A interconexão entre tecnologia, comunicação e vida cotidiana fez surgir um novo ambiente sociocultural, no qual a circulação de informações ocorre de forma contínua, veloz e intensa. Nesse contexto, as fronteiras que antes separavam o espaço físico e o espaço virtual se tornam porosas e interdependentes. Como observa Eugênio Trivinho, a sociedade digital é um espaço de hipervisibilidade, no qual o sujeito encontra-se simultaneamente exposto e vulnerável a novas formas de violência simbólica e informacional. Essa transformação não representa apenas um avanço técnico, mas inaugura uma nova condição existencial mediada pelo fluxo incessante de dados.

¹Acadêmico do curso de Direito da UNIR, 2025.2. E-mail: melk189206@gmail.com

²Acadêmico do curso de Direito da UNIR, 2025.2. E-mail: frotaeudes@gmail.com

Esse ambiente digital, marcado pela expansão da cibercultura, também propicia o surgimento de novas modalidades de crimes e práticas lesivas. Golpes digitais, fraudes eletrônicas, clonagem de perfis, uso indevido de dados pessoais e a difusão de conteúdos manipulados através de técnicas de inteligência artificial, como os *deepfakes*, são manifestações típicas desse cenário. A sofisticação tecnológica, aliada ao anonimato proporcionado pela internet, cria um ambiente no qual condutas ilícitas podem ser praticadas de modo rápido, discreto e com maior dificuldade de rastreamento pelas autoridades estatais. Essa realidade desafia o Direito Penal, que passa a lidar com ações que se desenvolvem em um ambiente informacional muito mais dinâmico e volátil do que o previsto em sua tradição jurídica.

Nesse contexto de hiperconectividade e risco, surge a necessidade de pensar um novo equilíbrio entre repressão penal e proteção dos direitos fundamentais, especialmente no que diz respeito à privacidade e à proteção de dados pessoais. A promulgação da Lei Geral de Proteção de Dados (LGPD) introduziu no ordenamento brasileiro diretrizes essenciais para salvaguardar informações pessoais, mas sua interface com a investigação criminal apresenta tensões particulares. O desafio que se coloca, portanto, é compreender como o Direito Penal pode responder de forma eficaz às condutas ilícitas praticadas no ambiente digital, sem comprometer as bases constitucionais da dignidade humana, da privacidade e do devido processo legal.

2. SOCIEDADE VIRTUAL E PREVENÇÃO DE CRIMES DIGITAIS

Para entender os desafios da criminalidade digital, é indispensável compreender o conceito de cibercultura. Segundo Trivinho, a cibercultura representa o conjunto de práticas sociais, comunicacionais e cognitivas mediadas pela tecnologia digital, produzindo uma nova ambiência existencial marcada pela velocidade e pela desmaterialização. Não se trata apenas de uma cultura na internet, mas de uma cultura atravessada pela tecnologia, capaz de reconfigurar comportamentos individuais e coletivos, além de impor novas formas de sociabilidade. Aparecida Zuin complementa essa visão ao propor a ideia do “cidadão-pixel”, sujeito cuja identidade se desfaz parcialmente na rede, sendo reconfigurada em imagens, dados, rastros digitais e fluxos informacionais que circulam em escala global. Esse cidadão, simultaneamente local e global (glocal) passa a existir não apenas como corpo físico, mas também como representação digital, marcando a fusão entre o real e o virtual.

Essa nova configuração identitária amplifica vulnerabilidades e facilita a ocorrência de crimes cibernéticos. Devido à confiança excessiva em ambientes digitais, muitos usuários tornam-se alvos fáceis de golpes como phishing, clonagem de contas, engenharia social e invasão de dispositivos. Esses golpes utilizam-se tanto da ingenuidade humana quanto da ausência de práticas sistemáticas de proteção digital. A ilusão de segurança e a sensação de familiaridade com o ambiente virtual contribuem para que indivíduos compartilhem dados sensíveis ou acessem links maliciosos sem perceberem o perigo. A facilidade de circulação de informações, a fragmentação das identidades e a rapidez das interações tornam o ambiente digital terreno fértil para práticas criminosas que, muitas vezes, ultrapassam fronteiras físicas e jurisdicionais.

Dessa forma, a prevenção de crimes digitais assume um papel essencial na proteção da cidadania. Isso envolve não apenas políticas públicas, mas também a educação digital da população, que deve compreender os riscos inerentes ao ambiente virtual. A alfabetização midiática e o incentivo a boas práticas de segurança, como o uso de senhas fortes, autenticação de dois fatores e a verificação de fontes informacionais, são medidas essenciais para a conscientização das pessoas e para a prevenção à golpes e divulgação de dados pessoais de forma desgovernada. Por outro lado, do ponto de vista jurídico, a prevenção demanda cooperação internacional, atualização normativa e investimentos em tecnologia e principalmente a capacitação de profissionais. Tendo em vista que, apenas por meio de uma atuação integrada entre sociedade, Estado e plataformas digitais será possível reduzir a incidência de crimes virtuais e fortalecer a proteção dos usuários.

3. DEEPFAKES E O USO INDEVIDO DE IMAGEM

Os *deepfakes*, termo derivado da combinação de *deep learning* e *fake*, consistem em vídeos, áudios ou imagens produzidos ou manipulados por algoritmos de inteligência artificial capazes de imitar a aparência, a voz ou os movimentos de uma pessoa de forma quase perfeita. Essa tecnologia representa um avanço impressionante no campo da simulação digital, mas também uma ameaça significativa à segurança informacional e à integridade das pessoas. Como observa Paul Virillio, toda nova tecnologia traz consigo a sua própria forma de acidente, isto é, um risco inerente ao seu funcionamento. Com base na teoria de Virillio, os

deepfakes constituem o “acidente” próprio da era algorítmica, na qual a perfeição técnica da imagem digital pode ser usada para fins destrutivos, enganando cidadãos, instituições e sistemas jurídicos.

A produção de *deepfakes* agrava um fenômeno identificado por Aparecida Zuin como “corpografia pixelada”, no qual o corpo físico se converte em representação digital manipulável. Essa transformação elimina limites entre verdade e simulação, tornando o indivíduo vulnerável à difamação, extorsão, exposição indevida e outras formas de violência simbólica. Zuin aponta que a identidade digital do sujeito, quando fragmentada em pixels, se torna suscetível a manipulações que escapam ao controle individual, o que agrava os riscos e dificulta a responsabilização dos autores dessas práticas. Essa lógica de “corpos manipuláveis” torna-se ainda mais grave no caso de crianças e adolescentes, que podem ter imagens ou fotografias reutilizadas em *deepfakes* para fins ilícitos, violando o Estatuto da Criança e do Adolescente (Zuin, Gois Júnior, Alves. 2018).

As dificuldades investigativas relacionadas aos *deepfakes* são enormes. O avanço tecnológico permite que criminosos ocultem sua identidade, utilizem redes privadas virtuais e disseminem o conteúdo rapidamente em diversas plataformas. Além disso, a distinção entre o real e o fabricado exige perícias altamente especializadas, tornando o trabalho policial mais complexo. A volatilidade das provas digitais e a rápida circulação de conteúdos exigem protocolos rigorosos de cadeia de custódia e ferramentas de validação forense, sob pena de inutilização da prova. O *deepfake*, portanto, representa não apenas um novo tipo de crime, mas um desafio ontológico para o Direito Penal, que precisa lidar com a instabilidade da verdade na era digital.

4. MARCO JURÍDICO BRASILEIRO E OS DESAFIOS DO DIREITO PENAL

O ordenamento jurídico brasileiro dispõe de legislação relevante para enfrentar crimes virtuais, como o Código Penal, a Lei Carolina Dieckmann, a Lei de Crimes Cibernéticos e o Marco Civil da Internet. Contudo, a velocidade com que novas tecnologias surgem e se popularizam cria um hiato entre a realidade digital e a capacidade normativa do Estado. O Direito Penal, estruturado para tipificar condutas relativamente estáveis, enfrenta dificuldade para abarcar práticas tecnológicas em

constante transformação. A ausência de tipificações específicas para condutas relacionadas à inteligência artificial, como *deepfakes* maliciosos ou manipulação de dados biométricos, deixa lacunas que favorecem a impunidade e dificultam a atuação policial.

Essa defasagem está diretamente relacionada ao fenômeno descrito por Paul Virillio como “dromologia”, a lógica da velocidade que rege o mundo contemporâneo. Para Virillio, as instituições políticas, jurídicas e sociais operam em ritmos muito mais lentos do que as tecnologias que transformam o cotidiano. Esse descompasso cria inevitáveis atrasos na capacidade do Direito de reagir aos novos acidentes tecnológicos. No caso do Direito Penal, isso resulta em investigações mais complexas, provas mais frágeis e limitações na responsabilização de agentes que utilizam ferramentas digitais para cometer ilícitos.

Nesse cenário de acelerada transformação tecnológica, torna-se ainda mais necessário observar os limites teóricos do próprio Direito Penal. Conforme destaca Claus Roxin, o Direito Penal deve atuar de forma fragmentária e subsidiária, intervindo somente quando outros ramos do Direito se mostram insuficientes para a proteção de bens jurídicos relevantes. Essa concepção reforça que a expansão do Direito Penal em resposta aos crimes digitais não pode ocorrer de maneira ilimitada, sob risco de violar garantias fundamentais e comprometer a legitimidade do sistema punitivo. Assim, a atualização legislativa na era digital deve respeitar a função mínima do Direito Penal, evitando a adoção de respostas punitivas desproporcionais.

Para além da necessidade de respeito aos limites teóricos do Direito Penal, há também desafios operacionais e estruturais que demandam atenção, tendo em vista que a investigação de crimes digitais exige conhecimentos técnicos especializados, mecanismos de cooperação internacional e infraestrutura adequada para rastrear atividades em ambientes virtuais descentralizados, tornando-se uma missão complexa e robusta. Destaca-se ainda que a volatilidade dos dados, a possibilidade de anonimato e o uso de ferramentas de criptografia dificultam a preservação de provas durante a persecução penal. Por isso, o Ministério Público, a Polícia Judiciária e o Poder Judiciário precisam investir em capacitação e atualização constante para lidar com esse ambiente. Dessa forma, o Direito Penal enfrenta o desafio de se modernizar sem romper as bases garantistas que sustentam o Estado de Direito.

5. A TENSÃO ENTRE INVESTIGAÇÃO PENAL E LGPD

A Lei Geral de Proteção de Dados (LGPD) estabelece princípios como finalidade, necessidade e proporcionalidade, buscando assegurar que o tratamento de dados pessoais, sobretudo sensíveis, seja realizado de forma legítima e segura. No entanto, quando aplicada ao contexto penal, a LGPD produz tensões importantes. De um lado, investigações criminais muitas vezes dependem da coleta de informações privadas, como registros de navegação, conteúdo de mensagens, dados biométricos e localização. De outro, a proteção de dados pessoais é uma garantia fundamental destinada a preservar a privacidade, a liberdade e a dignidade humana.

Eugênio Trivinho alerta que a era digital intensifica práticas de vigilância e controle social, criando novas formas de monitoramento que escapam à percepção dos cidadãos. Essa dinâmica, se aplicada de forma indiscriminada pelo Estado, pode gerar abusos investigativos e comprometer direitos fundamentais. A coleta excessiva de dados sob o pretexto de combate à criminalidade pode transformar a investigação penal em instrumento de violação de liberdades, distorcendo sua função constitucional. É nesse ponto que a LGPD funciona como limite ético e jurídico, estabelecendo parâmetros de proteção contra práticas estatais arbitrárias.

A harmonização entre investigação penal e proteção de dados exige o estabelecimento de critérios rigorosos, como a autorização judicial fundamentada, estrita necessidade da medida, análise de proporcionalidade e garantia de que os dados coletados serão utilizados exclusivamente para a finalidade específica da investigação. O desafio atual e futuro consiste em assegurar uma persecução penal eficiente sem abrir mão das garantias que protegem o indivíduo contra o abuso de poder, deixando como reflexão que tipo de Estado se deseja construir na era digital.

6. CONSIDERAÇÕES FINAIS

A era digital exige uma reconfiguração profunda do Direito Penal e dos mecanismos de investigação criminal. A expansão da cibercultura, a intensificação dos riscos tecnológicos identificados por Virillio e a hipere Exposição do sujeito destacada por Trivinho mostram que as práticas ilícitas se tornaram mais complexas, rápidas e difíceis de identificar. *Deepfakes*, manipulação de dados pessoais, golpes

digitais e fraudes informacionais representam não apenas novos tipos de crimes, mas novas formas de ameaça à dignidade humana.

A construção de um Direito Penal digital equilibrado depende da capacidade de integrar prevenção, repressão eficiente e respeito aos direitos fundamentais. Isso envolve atualização legislativa, capacitação técnica, cooperação institucional e políticas públicas de educação digital, além da reafirmação constante dos princípios constitucionais. O Estado deve ser capaz de investigar crimes digitais sem se transformar em agente de vigilância abusiva, respeitando os limites impostos pela LGPD e pela Constituição.

Portanto, é possível concluir que o desafio atual não é apenas tecnológico ou jurídico, mas sobretudo ético, consiste em construir uma sociedade digital que valorize a liberdade, a dignidade e a segurança, sem permitir que a tecnologia, na busca por controle e eficiência, reduza o indivíduo a mero dado, imagem ou pixel.

Palavras-Chave: Cibercultura. *Deepfakes*. Direito Penal Digital. Proteção de Dados. Investigação Criminal.

REFERÊNCIAS

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Diário Oficial da União, Rio de Janeiro, RJ, 31 dez. 1940.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente (ECA). Diário Oficial da União, Brasília, DF, 16 jul. 1990.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos e altera o Código Penal. Diário Oficial da União, Brasília, DF, 3 dez. 2012. (**Conhecida como Lei Carolina Dieckmann**).

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Marco Civil da Internet. 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.

ROXIN, Claus. **Direito Penal: parte geral.** 2. ed. Rio de Janeiro: Renovar, 2006. v. 1

TRIVINHO, Eugênio. **A dromocracia cibercultural: lógica da vida humana na civilização mediática avançada.** São Paulo: Paulus, 2007.

VIRILLIO, Paul. **O acidente original.** Lisboa: Teorema, 2002.

VIRILLIO, Paul. **Velocidade e política: um novo regime de dominação**. São Paulo: Estação Liberdade, 1996.

ZUIN, Aparecida Luzia Alzira; GOIS Júnior, José Caldas; ALVES, Gustavo Farias. **Cidadão-pixel: direito e democracia na sociedade digital**. Curitiba: Appris, 2018.

ZUIN, Aparecida; **Direitos humanos, sociedade e democracia na era cibercultural**. Arquivo didático. 2025. Disponível mediante envio pelo autor.