III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO PENAL E CIBERCRIMES II

D598
Direito penal e cibercrimes II [Recurso eletrônico on-line] organização III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores: Renan Posella Mandarino, Fábio Cantizani Gomes e Ana Carolina de Sá Juzo – Franca: Faculdade de Direito de Franca, 2025.

Inclui bibliografia
ISBN: 978-65-5274-364-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Governança, regulação e o futuro da inteligência artificial.
1. Direito. 2. Políticas Públicas. 3. Tecnologia. 4. Internet. I. III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2025 : Franca, SP).

CDU: 34

III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO PENAL E CIBERCRIMES II

Apresentação

Entre os dias 30 de setembro e 3 de outubro de 2025, a Faculdade de Direito de Franca recebeu o III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. O evento reuniu acadêmicos, profissionais, pesquisadores e estudantes, promovendo o debate interdisciplinar sobre o impacto das inovações tecnológicas no campo jurídico e nas políticas públicas. A programação envolveu Grupos de Trabalho (GTs) organizados para aprofundar temas específicos, abordando desde o acesso à justiça até as complexidades da regulação tecnológica, com ênfase na adaptação do sistema jurídico aos avanços da inteligência artificial e da automação.

O GT 9 foca nos crimes digitais e na responsabilização penal de condutas praticadas em ambiente virtual. As pesquisas discutem pornografia não consentida, cyberbullying, discursos de ódio e a eficácia das investigações digitais. O grupo ressalta a necessidade de adequação legislativa e de políticas públicas voltadas à prevenção e repressão dos cibercrimes.

DIREITO PENAL NA ERA DIGITAL: A EVOLUÇÃO DA LEGISLAÇÃO E OS NOVOS DESAFIOS NA TIPIFICAÇÃO E NO COMBATE AOS CRIMES PRATICADOS PELA INTERNET

CRIMINAL LAW IN THE DIGITAL AGE: THE EVOLUTION OF LEGISLATION AND NEW CHALLENGES IN CLASSIFYING AND COMBATING CRIMES COMMITTED OVER THE INTERNET

Paulo Henrique Miotto Donadeli

Resumo

O fenômeno da era digital traz um grande desafio ao Direito Penal na regulamentação jurídica dos cibercrimes, de forma a dar uma resposta rápida as violações de direitos cometidas por meio dos recursos tecnológicos. Essa situação tem exigido dos estudiosos uma profunda discussão de alternativas para transformar o ambiente virtual num espaço seguro, justo e ético. Por meio de uma metodologia descritiva bibliográfica e dogmática jurídica, o estudo busca refletir sobre a evolução da legislação penal brasileira, levantando as principais questões a serem enfrentadas pelo Direito Penal no campo digital.

Palavras-chave: Direito penal, Era digital, Cibercrimes

Abstract/Resumen/Résumé

The phenomenon of the digital age poses a major challenge to Criminal Law in the legal regulation of cybercrimes, in order to provide a rapid response to rights violations committed through technological resources. This situation has required scholars to deeply discuss alternatives to transform the virtual environment into a safe, fair and ethical space. Through a descriptive bibliographic and legal dogmatic methodology, the study seeks to reflect on the evolution of Brazilian criminal legislation, raising the main issues to be faced by Criminal Law in the digital field.

Keywords/Palabras-claves/Mots-clés: Criminal law, Digital age, Cybercrimes

Introdução

A era digital, que é a expressão do mundo contemporâneo, caminha aceleradamente com o surgimento de novas tecnologias de informação e comunicação a cada dia, causando transformações significativas na sociedade, sem que o Direito Penal consiga acompanhar com uma regulamentação jurídica as situações que geram lesões a bens jurídicos fundamentais e preocupações sociais.

É inegável a contribuição social que as tecnologias digitais trouxeram, ampliando o acesso à informação e ao conhecimento, promovendo a integração entre pessoas e o intercâmbio de ideias, favorecendo a comunicação em tempo real, possibilitando o desenvolvimento de novas formas de trabalho, impulsionando a economia por meio das atividades de comércio eletrônico, entre outros inúmeros benefícios. Mas, também, passou a ser terra fértil para a prática de ilícitos, quebrando a privacidade de muitas pessoas, permitindo o acesso indevido a dados pessoais, favorecendo a disseminação de notícias e conteúdos falsos e enganosos, abrindo espaço para fraudes patrimoniais, além de provocar o aumento de transtornos mentais ligados a ansiedade e depressão, entro muitos outros problemas éticos e jurídicos que desafiam a comunidade acadêmica em refletir sobre como controlar esse espaço sem ferir direitos assegurados constitucionalmente.

O presente estudo objetiva analisar a relação do Direito Penal com essa nova era digital, buscando verificar como tem evoluído a legislação penal e a aplicabilidade dos tipos penais, conhecido como cibercrimes ou crimes de informática, que tem se colocado como um desafio para a persecução criminal do Estado, em razão da sofisticação e da diversidade dessas ações criminosas. O Estado precisa atuar na regulamentação jurídica, por meio de uma legislação específica e atualizada, de forma a ampliar os benefícios do mundo digital e reduzir seus danos.

Desenvolvimento

O legislador e os operadores do Direito começaram a perceber que as leis penais tradicionais, voltadas para os crimes presenciais e de natureza individual, não conseguiam dar uma resposta efetiva aos crimes praticados no ambiente virtual. Para lidar com este novo cenário da realidade criminal, foi necessário a criação de uma legislação própria e específica voltada as condutas que feriam bens jurídicos fundamentais realizadas no ambiente virtual.

> Organizada, modernizada e transnacional, a criminalidade emergente pode lesar tanto os indivíduos quanto os Estados e suas instituições, o que nos leva a discutir se o Direito Penal tradicional ou nuclear (“clássico”) – concebido e desenvolvido especialmente para a solução de casos interindividuais, com bens jurídicos tradicionais ou específicos – poderia, sem dissociar-se de seus princípios e, fundamentalmente, de suas garantias clássicas, responder a

> conceitos sociais complexos, numa sociedade de risco, globalizada. (MASI; MORAES, 2013)

O rápido avanço da tecnologia e a constante evolução das formas de criminalidade digital, tem gerado um desafio complexo para o Direito Penal. Há uma necessidade de atualização constante do arcabouço jurídico, para acompanhar de forma efetiva as inovações tecnológicas e, muitas vezes, o Estado não dá conta, o que causa uma situação de injustiça na opinião pública.

> O Direito, que mira os fatos, identifica os valores e cria as normas necessárias à sua regulação, aos poucos se amolda a essa nova realidade. Isso vale para diversos ramos jurídicos: há o contrato eletrônico, no Direito Civil, o e-commerce, no Direito Comercial e do Consumidor, o processo eletrônico, no Direito Processual (Civil e Penal), a tributação pelo computador, a emissão de nota fiscal on-line, o pregão eletrônico no Direito Administrativo e os delitos informáticos no Direito Penal. Em matéria criminal, boa parte das infrações cometidas por computadores e por sua rede mundial já se amoldava, sem maiores dificuldades, aos tipos penais existentes desde outrora. Isto porque, deve-se ressaltar, os crimes informáticos, em sua imensa maioria, não vulneram um novo bem jurídico, mas constituem meios de se ofender aqueles já reconhecidos pelo ordenamento: como a privacidade, a propriedade imaterial, o patrimônio, a fé pública, a Administração Pública etc. Assim, por exemplo, quem obtém a senha bancária da vítima e com ela efetua transferências eletrônicas, subtraindo valores de sua conta corrente, comete furto eletrônico (CP, art. 155, § 4º-B). Havia, porém, uma considerável gama de comportamentos ilícitos praticados no ambiente informatizado que se mostravam atípicos e, em virtude da proibição de analogia in malam partem, não poderiam ser açambarcados pelo manto protetivo do Direito Penal, senão por meio de uma reforma legislativa. (Estefam, 2022, p. 500)

A primeira legislação penal foi a Lei 12.737/2012, conhecida como a Lei Carolina Dieckmann, que alterou o Código Penal, inserindo no artigo 154-A o crime de invasão de dispositivo informático alheio, conectado ou não a internet, "mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita" (Brasil, 1940) Esse tipo penal trouxe "um novo bem jurídico alçado à categoria de valor penalmente relevante: a segurança informática" (Estefam, 2022, p. 500), ou seja, a liberdade de navegar no mundo digital, garantindo ao usuário "a integridade, disponibilidade e confidencialidade das informações e dados em ambiente telemático" (Estefam, 2022, p. 500), somando-se, também, a tutela da intimidade das informações pessoais presente nos meios informáticos.

> Até a aprovação da Lei n. 12.737/2012, a punição por crimes cibernéticos somente era possível na forma da legislação comum, na medida em que não havia crimes específicos em relação ao tema. Para que referida punição fosse possível, entretanto, mostrava-se necessário algum resultado posterior (a subtração de valores, o dano, a ofensa à honra etc.). (...) De acordo com a redação

> do dispositivo, basta que o agente invada o computador alheio com o fim de obter, adulterar ou destruir dados ou informações, ou, ainda, para instalar vulnerabilidades no sistema a fim de obter vantagem ilícita. Realizada uma dessas condutas, o delito estará consumado, ainda que o agente não atinja seu objetivo (obter, adulterar ou destruir informações ou obter vantagem ilícita). (Goncalves, 2002, p. 347)

Posteriormente, a Lei 13.964, de 2019, buscando o aperfeiçoamento da lei penal, deu nova redação ao artigo 141, parágrafo 2, do Código Penal, aplicando a pena em triplo se algum dos crimes contra a honra fossem cometidos ou divulgado em quaisquer modalidades das redes sociais na internet, por entender que no ambiente virtual potencializa a ação criminosa, possibilitando que um número grande de pessoas tome conhecimento da calúnia, difamação e injúria praticados contra a vítima, devendo ser punido mais gravemente o autor da ofensa e qualquer pessoa que a ela der divulgação pela internet (Goncalves, 2002). No mesmo sentido, a Lei 13968, de 2019, ao modificar a tipificação do crime de incitação e auxílio ao suicídio e as autolesões, prescreveu no parágrafo 4 do artigo 122 do Código Penal, o aumento da pena até o dobro se a conduta é realizada por meio da internet, também por entender o alcance amplificado que tal conduta pode ter no meio social.

Em 2021, foi promulgada a Lei 14.132 que introduziu no Código Penal o artigo147-A, tipificando o crime de perseguição, também conhecido como *stalking,* tratando-se de um crime de ação livre, que pode se dar tanto presencialmente quanto virtualmente. (Goncalves, 2022). Portanto, inclui o *cyberstalking,* que consiste na perseguição sistemática e reiterada de uma pessoa através de meios eletrônicos, como a internet, redes sociais, e-mails, entre outros, por meio de mensagens indesejadas, insistentes e ameaçadoras, ou com a publicação de informações falsas difamatórias da vítima, perturbando sua rotina e causando-lhe ansiedade, medo e insegurança. No mesmo ano, entrou em a Lei 14155 que novamente alterou o Código Penal, para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, entre outras providências, como forma de aumentar o rigor punitivo visando intimidar as práticas ilícitas em meio digital.

Mais recentemente, a Lei 14.811, de 2024, ao instituir medidas de proteção à criança e ao adolescente, alterou a legislação penal e incluiu dentro do Código Penal o crime de Intimidação sistemática, conhecido como *bullying*, no artigo 146-A, e estabeleceu como sua forma qualificada no caso da prática da conduta ser realizada por meio da internet, de rede social, de aplicativos, de jogos on-line ou por qualquer outro meio ou ambiente digital, ou transmitida em tempo real, que se intitula de *cyberbullying*, passando a pena de uma simples multa para reclusão, de dois anos a quatro anos, e multa, se a conduta não constituir crime mais grave. Mirabete (2024) ressalta que "a razão da majoração da pena nesses casos reside na facilidade de acesso imediato que a internet

propicia a um número maior e indeterminado de pessoas". Essa mesma lei, também, alterou o artigo 240, do Estatuto da Criança e do Adolescente, Lei 8.069, de 1990, que tipifica a conduta de produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente, passando o parágrafo 1, a prescrever:

> Incorre nas mesmas penas quem:
> II - exibe, transmite, auxilia ou facilita a exibição ou transmissão, em tempo real, pela internet, por aplicativos, por meio de dispositivo informático ou qualquer meio ou ambiente digital, de cena de sexo explícito ou pornográfica com a participação de criança ou adolescente. (Brasil, 1989)

Portanto, a legislação penal brasileira evolui bastante e hoje são diversos exemplos de ações criminosas no ambiente digital. É perceptível, que o Estado tem buscado dar uma resposta legislativa no enfrentamento aos crimes cibernéticos, com uma gradual e constante alteração e inserção de normas no arcabouço jurídico penal brasileiro.

Uma importante questão envolvendo esses crimes, que se põe como um grande desafio, é que estes crimes não se restringem ao território físico de um Estado, mas assumem, muitas vezes, o caráter transnacional, confrontando diferentes legislações e jurisdições, o que dificulta a ação dos Estados, o trabalho da polícia e da justiça na repressão criminal, requerendo novas formas de enfrentar este grave e complexo problema. Essa natureza transnacional desses crimes requer uma ação conjunta dos Estados na sociedade internacional, por meio de tratados e acordos que envolva a troca de informações de inteligência policial e de rastreamento internacional, visando uma efetiva cooperação no combate as atividades criminosas no âmbito virtual.

Outro desafio, é que muitos desses crimes se valem de anonimato, criptografia e redes descentralizadas, o que tem dificultado ainda mais a identificação e a responsabilização dos infratores. As tecnologias de anonimato permitem que os usuários naveguem pela internet de forma a ocultar sua identidade real, em nome da proteção da privacidade e da garantia à liberdade de expressão. Também, possibilitam resguardar dados pessoas contra ação de *hacking* e de espionagem. Vários são os recursos que permitem esse anonimato, como as tecnologias de redes virtuais privadas, as redes de roteamento anônimo, a criptografia ponta a ponta avançada, entre outros mecanismos que bloqueiam ou impedem a rastreabilidade do usuário.

Não são todos os usuários que valem desses instrumentos para a prática de ilícitos, para muitas pessoas essas tecnologias são necessárias para a realização de um trabalho seguro e isento, como são os casos de jornalista, ativistas, denunciantes de agressões aos direitos humanos em

regimes autoritários e minorias vulneráveis perseguidas. Desta forma, as tecnologias de anonimato têm um papel relevante na era digital, não podendo ser simplesmente proibidas pela legislação.

No entanto, tem pessoas que se aproveitam para cometer crimes, na ideia de que ficarão impunes. Perante essa realidade, o Estado não pode simplesmente criminalizar o seu uso, mas precisa buscar um equilíbrio, que ao mesmo tempo preserve a intimidade e a privacidade de quem há utiliza licitamente, com a necessidade de impor limites para coibir e punir o seu uso indevido, permitindo a quebra do anonimato em situações específicas e fundamentadas pela autoridade judicial competente, quando da existência de procedimentos de investigação abertos.

E não poderia deixar de lembrar nessa reflexão acadêmica o problema que representa os crimes de ódio e de discurso de ódio praticados na internet, que tem avançado de forma exponencial, tornando-se um desafio que vai além da tipificação criminal, mas que revela um fenômeno complexo e cruel de intolerância na sociedade contemporânea, causando enormes e preocupantes danos a convivência harmônica e pacífica, e que muitas vezes se reverbera em ações de violência e de agressões físicas e psicológicas a pessoas, marginalizando grupos vulneráveis e alimentando preconceitos e discriminações, o que tanto afeta a dignidade humana e os direitos fundamentais.

Conclusões

O combate à criminalidade digital implica uma série de medidas que estão além da simples tipificação penal, e requer uma abordagem multidisciplinar e inovadora por parte dos órgãos de persecução criminal do Estado, com aperfeiçoamento constante das infraestruturas de segurança cibernética, a necessidade de qualificação de profissionais para atuarem nessas áreas, a fomentação de políticas públicas de conscientização do uso correto e ético das redes, entre outras ações, que demandam investimentos públicos.

A legislação penal brasileira tem buscado dar uma resposta efetiva ao uso indevido do meio digital, tipificando crimes e cominando penas, de forma a responsabilizar agentes que utilizam das tecnologias para ofender bens jurídicos fundamentais e causar danos sociais. Mas, ainda é preciso enfrentar vários pontos relativos aos marcos regulatórios, tipificando novos crimes e promovendo a adaptação das normas existentes há nova era digital, visando que o Direito Penal consiga dar uma resposta segura, efetiva e rápida à sociedade, reprimindo e punindo os crimes cibernéticos, de forma a garantir a credibilidade do sistema de justiça penal.

Como se viu ao longo do texto, os desafios são muitos, e há muito o que se fazer para buscar uma real efetividade no combate aos crimes cibernéticos. Um grande dificultador para a

eficácia do combate aos crimes cibernéticos repousa nas tecnologias de anonimato, que impõe barreiras na rastreabilidade das condutas criminosas e na identificação de seus autores.

O estudo abordou que o uso de tecnologias de anonimato enfrenta um debate em torno da garantia dos direitos à privacidade e a liberdade de expressão perante a segurança no ambiente digital. Portanto, qualquer forma de criminalização do uso das tecnologias de anonimado na era digital deve pautar-se pela preocupação na busca de soluções que leve em consideração os direitos fundamentais das pessoas envolvidas, buscando combater as práticas criminosas, mas sem o cerceamento da intimidade e da liberdade de expressão.

É claro que das formas de anonimato devem ser aceitáveis dentro de padrões éticos, jurídicos e de segurança pública, cabendo ao Estado uma atuação por meio de uma regulamentação séria e adequada compatíveis com os fundamentos do Estado Democrático de Direito, fazendo um controle de forma transparente e responsável evitando abusos e desrespeitos aos direitos humanos, de forma a criar um ambiente digital livre de violações.

Outras questões estão a cada dia surgindo e que precisa de um olhar específico e atento do Direito Penal, para que temas tão importantes não fiquem sem uma disciplina jurídica capaz de evitar ações danosas a sociedade, como o uso da inteligência artificial, o combate notícias falsas, a regulamentação das criptomoedas, a utilização das tecnologias de reconhecimento facial na persecução criminal, entre muitos temas, que podem ter uma repercussão direta no Direito Penal.

Referências

Brasil. **Código Penal**: Decreto-lei n. 2.848, de 7 de dezembro de 1940. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm> Acesso em: 11 jun. 2025.

Brasil. **Estatuto da Criança e do Adolescente**: lei n. 8.069, de 13 de julho de 1990. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l8069.htm> Acesso em: 11 jun. 2025.

Estefam, André. **Direito penal**: parte especial. 9. ed. São Paulo: Saraiva, 2022.

Goncalves, Victor Eduardo Rios. **Direito penal**: parte especial. 12. ed. São Paulo: Saraiva, 2022.

Masi, Carlo Velho; Moraes, Voltaire de Lima. O "moderno" direito penal e a política criminal expansionista. **Revista Eletrônica da Faculdade de Direito Programa de Pós-Graduação em Ciências Criminais Pontifícia Universidade Católica do Rio Grande do Sul**. Porto Alegre, Volume 5, Número 1, p. 93-102, janeiro/junho 2013. Disponível em: <http://revistaseletronicas.pucrs.br/ojs/index.php/sistemapenaleviolencia/article/view/13004/9533> Acesso em: 11 maio 2025.

Mirabete, Julio Fabbrini; Mirabete, Renato. **Manual de direito penal**: parte especial. São Paulo: Foco, 2024.