

Resenha do artigo intitulado “Crimes cibernéticos e a falsa sensação de impunidade”¹

Review of the article entitled “Cybercrimes and the false sense of impunity”

 ARK: 44123/multi.v7i13.1691

Pedro Lucas Duarte França¹

<https://orcid.org/0009-0003-2446-8476>

<https://lattes.cnpq.br/4973155546326635>

UniProcessus – Centro Universitário Processus, DF, Brasil

E-mail: pedrofranca.df@gmail.com

Michael Douglas Mendes de Oliveira³

<https://orcid.org/0009-0008-0616-8791>

<https://lattes.cnpq.br/3793659690832183>

UniProcessus – Centro Universitário Processus, DF, Brasil

E-mail: michaelmendesdireito@gmail.com

Dayane Ferreira Soares⁴

<https://orcid.org/0009-0006-3395-0610>

<http://lattes.cnpq.br/1748222029118355>

UniProcessus – Centro Universitário Processus, DF, Brasil

E-mail: daayanesoares@gmail.com

Resumo

A presente resenha analisa o artigo “*Crimes Cibernéticos e a Falsa Sensação de Impunidade*”, de autoria de Juliana Fernandes Alvares Rodrigues e Diego Henrique da Cruz, publicado na *Revista Científica Eletrônica do Curso de Direito*, 13^a edição, em janeiro de 2018. O estudo examina a classificação dos crimes virtuais, as dificuldades investigativas e jurídicas associadas a essas infrações e a consequente percepção social de impunidade diante do acelerado avanço tecnológico. A principal contribuição do artigo consiste em demonstrar que o problema não decorre da inexistência de leis, mas sim das barreiras técnicas, estruturais e operacionais que dificultam a efetiva responsabilização dos infratores no ambiente digital.

Palavras-chave: Crimes Cibernéticos. Impunidade. Legislação. Investigação. Tecnologia.

¹Resenha de aproveitamento da disciplina TC (Trabalho de Curso), do curso *Bacharelado em Direito*, do Centro Universitário Processus – UniProcessus, sob a orientação dos professores Jonas Rodrigo Gonçalves e Danilo da Costa. A revisão linguística foi realizada por Tatianne Pereira da Silva.

²Graduando em Direito pelo Centro Universitário Processus – UniProcessus.

³Graduando em Direito pelo Centro Universitário Processus – UniProcessus.

⁴Graduanda em Direito pelo Centro Universitário Processus – UniProcessus.

Abstract

This review analyzes the article “Cybercrimes and the False Sense of Impunity”, authored by Juliana Fernandes Rodrigues and Diego Henrique da Cruz, published in the Revista Científica Eletrônica do Curso de Direito, 13th edition, January 2018. The study examines the classification of cybercrimes, the investigative and legal challenges associated with these offenses, and the resulting social perception of impunity in the face of rapid technological advancement. The article’s main contribution is to demonstrate that the problem does not stem from the absence of laws, but from technical, structural, and operational barriers that hinder the effective accountability of offenders in the digital environment.

Keywords: Cybercrimes. Impunity. Legislation. Investigation. Technology.

Resenha

Esta é uma resenha do artigo intitulado “Crimes Cibernéticos e a falsa sensação de impunidade”, de autoria de Diego Cruz e Juliana Rodrigues. O trabalho analisado foi publicado na Revista Científica Eletrônica do Curso de Direito (ISSN: 2358-8551), 13ª edição, em janeiro de 2018.

Em primeiro lugar, no que se refere aos autores do artigo, é pertinente conhecer brevemente seus percursos acadêmicos e profissionais, uma vez que a formação e a experiência de cada autor influenciam diretamente a abordagem do tema discutido. Conheçamos, então, um pouco sobre cada um deles.

A primeira autora é Juliana Fernandes Alvares Rodrigues, cuja trajetória acadêmica e profissional na área jurídica merece destaque. Ela possui graduação em Direito pelo Centro Universitário de Bauru – ITE (2013) e pós-graduação em Docência no Ensino Superior Jurídico pela Universidade Anhanguera-Uniderp (2014). Concluiu o mestrado em Direito Constitucional, com ênfase no Sistema de Garantias de Direitos do Centro Universitário de Bauru – ITE (2016), e possui, ainda, pós graduação em Psicologia Jurídica pela Universidade do Sagrado Coração de Bauru – UNISAGRADO (2021) e em Direito de Família e das Sucessões pela FMB (2022). Exerce funções docentes no Grupo – FAEF, atua como conciliadora e mediadora no Tribunal de Justiça de SP, e é advogada regularmente inscrita na OAB n 505.558/SP. Seu currículo Lattes está disponível em <http://lattes.cnpq.br/2315388898581072> e seu Orcid em <https://orcid.org/0000-0003-1087-6455>.

O segundo autor do artigo é Diego Henrique da Cruz, graduado em Direito pela FAEF – Faculdade de Ensino Superior e Formação Integral de Garça, em São Paulo.

O artigo está estruturado nos seguintes capítulos: Resumo, *Abstract*, *Keywords*, Introdução; 2. Crimes Cibernéticos, com as subseções: 2.1 Classificações dos Sujeitos que Praticam o Crime e dos Crimes Cibernéticos; 2.2 Tipicidade penal dos crimes cibernéticos frente à legislação brasileira; 2.3 Leis específicas a respeito dos crimes cibernéticos; 3. A problemática enfrentada pelo judiciário diante aos crimes virtuais; 3.1 composição do poder judiciário, tratando-se de crimes; 3.2 Problemática da investigação nos crimes cibernéticos;

4. Conclusão.

A obra apresenta o seguinte resumo:

Roubo de dados e de identidade, calúnia, difamação, bullying, crimes financeiros, pornografia e pedofilia infantil, verbos estes que constituem os crime cibernético praticado no Brasil, de modo que o presente artigo aborda classificação e características das práticas criminosas realizadas através da internet, inclusive

traz garantias fundamentais garantidos pela constituição federal, e destaca a sensação de impunidade que os cidadãos de bem sentem com o crescente aumento dos crimes virtuais em todo o Brasil, de modo que tenta esclarecer o fato causador da sensação de impunidade e uma possível solução para a não ocorrência dos cybercrimes ou a diminuição deste.
Palavras – Chave: Crimes, Crimes Cibernéticos, Crimes Virtuais, evolução, globalização.
 (CRUZ; RODRIGUES, 2018, p. 1).

O tema deste artigo é “*Crimes Cibernéticos e a Falsa Sensação de Impunidade*”. A problemática abordada consiste na “classificação e características das práticas criminosas realizadas por meio da internet”, considerando também as garantias fundamentais asseguradas pela Constituição Federal. O artigo destaca, ademais, a sensação de impunidade percebida pelos cidadãos diante do crescente aumento dos crimes virtuais em todo o Brasil, buscando identificar os fatores que geram essa percepção e apontando possíveis soluções para prevenir a ocorrência de cybercrimes.

A hipótese central do estudo é: a sensação de impunidade em relação aos crimes cibernéticos não decorre da ausência de leis específicas, mas das dificuldades técnicas e operacionais enfrentadas pelo sistema judiciário e pelas forças policiais na investigação e na punição desses delitos.

O objetivo principal do artigo é classificar e caracterizar as práticas criminosas realizadas por meio da internet, conhecidas como crimes cibernéticos. Além disso, busca apresentar as garantias fundamentais resguardadas pela Constituição Federal no uso da rede. Um foco central do estudo é evidenciar a sensação de impunidade percebida pelos cidadãos diante do crescente aumento desses crimes virtuais, procurando identificar os fatores que geram essa percepção e propondo possíveis soluções para prevenir ou reduzir a ocorrência desses crimes.

A justificativa do artigo está na relevância do tema, considerando que o avanço tecnológico criou a internet, uma ferramenta benéfica, mas que também oferece oportunidades para a atuação de indivíduos mal-intencionados. Diante do aumento dos crimes virtuais, o estudo se mostra necessário para analisar a falsa sensação de impunidade. A justificativa centra-se em demonstrar que a impunidade não é resultado da inexistência de leis, mas das dificuldades de investigação e da limitação de recursos técnicos e humanos para identificar e punir os infratores.

A metodologia do artigo fundamentou-se na análise de referencial teórico, por meio de pesquisa bibliográfica e documental. O estudo se desenvolveu em etapas: inicialmente, realizou-se a contextualização dos crimes cibernéticos, abordando a origem e os aspectos da internet, bem como apresentando um breve histórico de crimes e penas. Em seguida, analisou-se a proteção assegurada pela Constituição Federal no uso da rede de computadores, como a inviolabilidade da dados. Por fim, o trabalho detalhou a problemática enfrentada pelo Poder Judiciário, pelas forças policiais e pelo Ministério Público para identificar e punir os infratores, explicando, assim, os fatores que contribuem para a falsa sensação de impunidade.

Cruz e Rodrigues afirmam, de forma contundente, que a evolução está intrinsecamente relacionada ao ser humano, o qual está sempre em busca de inovação. No primeiro capítulo, os autores, de modo relevante, abordam conceitos importantes sobre a temática, como o da internet e sua origem, ressaltando que muitos desconhecem seu início e desenvolvimento. Entretanto, eles destacam que, agregados aos avanços tecnológicos, também podem surgir retrocessos: alguns indivíduos se aproveitam do desconhecimento sobre essas novidades tecnológicas para obter benefícios indevidos.

No segundo capítulo, os autores apontam a Constituição Federal, destacando a

proteção que ela oferece no uso das redes de computadores, incluindo a inviolabilidade de dados e o direito à privacidade. Já no quarto capítulo, tratam das dificuldades enfrentadas pelo Judiciário na repressão aos crimes cibernéticos, detalhando a estrutura do Poder Judiciário e apresentando uma síntese do procedimento penal, com o objetivo de esclarecer os fatores que contribuem para a falsa percepção de impunidade.

Cruz e Rodrigues afirmam que as pessoas estão constantemente conectadas a dispositivos que utilizam a internet, de modo que, a vida cotidiana está completamente integrada à rede virtual, seja para acessar plataformas como Facebook, enviar mensagens eletrônicas (e-mails), realizar chamadas telefônicas, participar de videoconferências ou mesmo efetuar operações bancárias.

Os autores destacam que esses mecanismos oferecem diversas vantagens. Contudo, ponderam que a principal ferramenta utilizada para a prática de delitos é o chamado “malware”, um aplicativo que invade sistemas com o objetivo de transmitir informações a terceiros ou causar danos a dispositivos eletrônicos.

Os estudiosos enfatizam que, nesse contexto, surgiram sistemas que facilitam a prática de crimes virtuais. O artigo cita, com base nas assertivas de Túlio Lima Vianna, que os desenvolvedores de *malwares* podem ser classificados de forma objetiva, conforme a maneira como atuam. Ressaltam que esses indivíduos possuem habilidades técnicas avançadas e, por vezes, criam ou utilizam tecnologias com o objetivo de causar danos, chegando até a produzir conteúdos que ensinam essas práticas a terceiros.

Cruz e Rodrigues aduzem uma classificação adicional, de caráter subjetivo, referente a pedófilos e intimidadores, embora Vianna não tenha abordado essa classificação. Os autores ressaltam que os crimes cibernéticos podem ser classificados em três categorias: puros, mistos e comuns. Segundo eles, essas classificações são relevantes, pois refletem a complexidade das ações dos infratores quando praticadas em ambiente virtual, desde a sua execução até a consumação do delito.

Os autores salientam que o crime consiste na violação de normas estabelecidas em lei. Sublinham que, na ausência de previsão legal, não se pode falar em crime, conforme dispõe o artigo 1º do Código Penal Brasileiro. Contrariando a crença comum, asseveram que os delitos cometidos pela internet possuem tipificação legal e, quando identificados, sujeitam os infratores a sanções penais. O artigo também lista, de forma pertinente, os crimes mais praticados na rede mundial de computadores, indicando suas respectivas medidas legais. Nessa seara, convém apontar:

1- Assédio Sexual: previsto no artigo 216-A do Código Penal (Decreto-Lei 2.848, de 1940), ocorre quando alguém, em posição de superioridade hierárquica, constrange outra pessoa para obter vantagem sexual.

2- Discriminação: regulada pela Lei nº 7.716/1989, em conjunto com o artigo 140 do Código Penal (Decreto-Lei nº 2.848, de 1940), refere-se a crimes relacionados a raça ou cor. Mesmo quando praticada online, a conduta produz os mesmos efeitos jurídicos e danos.

3- Mercado Negro: não há uma lei em específica que estipule penas para o mercado negro.

4- Calúnia/ Difamação/ Injúria: tipificadas nos artigos 138, 139 e 140 do Código Penal (Decreto-Lei nº 2.848, de 1940), esses crimes contra a honra mantêm os requisitos, independentemente de ocorrerem presencialmente ou pela internet.

5- Apologia ao crime: prevista no artigo 287 do Código Penal (Decreto-Lei 2.848, de 1940), abrange a divulgação ou compartilhamento de conteúdo que apoie a violência.

6- Pornografia Infantil: o Estatuto da Criança e do Adolescente (Lei 8.069, de 1990), criminaliza a produção, venda, distribuição, aquisição e posse de material pornográfico.

7 – Espionagem: ganhou destaque no Brasil em 2013, quando informações sigilosas de vários países, incluindo o Brasil, foram divulgadas na internet por um ex-funcionário americano.

8 – Estelionato: tornou-se frequente na internet, especialmente com a criação de sites falsos que fazem as pessoas efetuarem pagamentos por produtos inexistentes.

9 – Roubo de identidade: ocorre por meio de *malwares* que capturam informações de sistemas.

Os autores reiteram que o Brasil não carece de leis para reprimir crimes praticados na internet. Declaram, ainda, que não é necessário incluir expressamente o termo “internet” nas normas, uma vez que as condutas já são tipificadas, contrariando a crença popular.

Cruz e Rodrigues frisam que a internet começou a ser usada no Brasil em 1988, inicialmente em São Paulo e no Rio de Janeiro, expandindo-se gradualmente para os demais estados. A pesquisa sublinha que as leis sobre crimes cibernéticos, promulgadas a partir de 2012, sofreram influência da pressão exercida pela mídia sobre o Poder Legislativo.

Os especialistas argumentam que muitas discussões surgiram em torno das Leis 12.735/2012 e 12.737/2012, sendo esta última conhecida como Lei Carolina Dieckmann, sancionada após o vazamento de fotos íntimas da atriz. Observam, no entanto, que o legislador não se preocupou em tipificar os cibercrimes de forma específica. Concluem, com precisão, que a verdadeira problemática não reside na falta de leis, mas em questões técnicas relacionadas à identificação do infrator e à definição de competência para julgamento.

Prudentemente, os autores ressaltam que, no âmbito da justiça, o Ministério Público, a polícia e o Judiciário enfrentam dificuldades em relação ao processamento de crimes virtuais. Salientam que este capítulo se propõe a relatar essas dificuldades, uma vez que cabe ao Estado a investigação, o processamento e a aplicação das sanções nos casos concretos.

O artigo esclarece que, de acordo com a Constituição Federal de 1988, o Poder Judiciário é composto por órgãos responsáveis por garantir direitos fundamentais individuais, coletivos e sociais, além de resolver conflitos entre cidadãos, entidades e Estado. Os juristas demonstram que a estrutura do Judiciário é organizada em forma de pirâmide, e entre os órgãos aptos a julgar casos criminais destacam-se: o Supremo Tribunal Federal (STF), o Superior Tribunal de Justiça (STJ), a Justiça Federal, o Tribunal de Justiça Militar e a Justiça Comum.

Os teóricos acentuam que a verdadeira problemática em punir efetivamente os criminosos virtuais não reside na falta de leis, mas na falta de mão de obra especializada e na escassez de tecnologia adequada para combatê-los, diante da elevada capacidade técnica desses infratores. Denotam que o número de crimes cometidos no Brasil supera sua capacidade investigativa, considerando que é necessário comprovar tanto a materialidade quanto a autoria para que se possa responsabilizar alguém.

Outro obstáculo mencionado é a recusa de empresas de informação, como o *WhatsApp*, em cooperar com as investigações. Revelam que leis fundamentais voltadas à proteção dos direitos individuais podem tornar os processos mais morosos e, com a globalização, aumenta-se o número de crimes praticados por estrangeiros em território brasileiro.

A pesquisa buscou reunir informações confiáveis sobre crimes cibernéticos, tema de grande relevância atualmente. Os autores abordaram a origem da internet e o contexto histórico que levou ao surgimento dos primeiros crimes online. Além disso, trouxeram a

atuação do Estado na salvaguarda de direitos fundamentais, o que, por um lado, protege liberdades, mas, por outro, pode tornar as investigações policiais mais demoradas, uma vez que dependem de autorização judicial.

Cruz e Rodrigues concluem que o ordenamento jurídico brasileiro, conquanto não mencione explicitamente a palavra “internet” em todos os tipos penais, prevê punição para as condutas delituosas independentemente do meio utilizado. Finalizam o estudo deduzindo que a sensação de impunidade em relação aos crimes cibernéticos não se deve à falta de leis específicas. Os autores, de maneira relevante, inferem que a internet, como a maior tecnologia já desenvolvida, não possui fronteiras e permite o aprofundamento do conhecimento em todas as áreas. Contudo, essa liberdade tem um custo: a perda da privacidade.

Referências

- BORRI, Luiz. Competência nos crimes contra a honra cometidos pela internet. Disponível em: <http://www.conjur.com.br/2012-out-09/luiz-borri-competencia-crimes-honra-cometidos-internet>. Acesso em: 18 set. 2016.
- BRASIL. Constituição da República Federativa do Brasil de 1988. Promulgada em 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 4 nov. 2025.
- BRASIL. Lei nº 7.716, de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 4 nov. 2025.
- BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 4 nov. 2025.
- BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Dispõe sobre condutas do uso do sistema eletrônico. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: 4 nov. 2025.
- BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos (Lei Carolina Dieckmann). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em: 4 nov. 2025.
- BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 4 nov. 2025.
- BURROWES, Frederick B. A proteção constitucional das comunicações de dados: internet, celulares e outras tecnologias. Disponível em: <https://revistajuridica.presidencia.gov.br/index.php/saj/article/viewFile/278/267>. Acesso em: 5 set. 2016.

CÂMARA DOS DEPUTADOS. CPI constata dificuldade em rastrear e punir crimes de internet.

Disponível em:

<http://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/494363-CPI-CONSTATA-DIFICULDADE-EM-RASTREAR-E-PUNIR-CRIMES-DE-INTERNET.html>.

Acesso em: 16 set. 2016.

CARVALHO, Marcelo Sávio Revoredo Menezes de. A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança.

Disponível em: <http://www.nethistory.info/Resources/Internet-BR-Dissertacao-MestradoMSavio-v1.2.pdf>. Acesso em: 10 set. 2016.

CASTRO, Luiz Augusto Sartori de. “Lei Carolina Dieckmann” seria a salvação da internet?

Disponível em: <http://www.migalhas.com.br/dePeso/16,MI167980,81042-Lei+Carolina+Dieckmann+seria+a+salvacao+da+internet>.

Acesso em: 15 set. 2016.

ELEUTÉRIO, Fernando. Análise do conceito de crime. Disponível em:

<http://www.uepg.br/rj/a1v1at09.htm>. Acesso em: 18 set. 2016.

G1.GLOBO.COM. WhatsApp: Justiça do RJ manda bloquear aplicativo em todo o Brasil.

Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-deve-ser-bloqueado-decide-justica-do-rio.html>. Acesso em: 18 set. 2016.

GONÇALVES, Jonas Rodrigo. Como elaborar uma resenha de um artigo acadêmico ou científico. Revista JRG de Estudos Acadêmicos, v. 3, n. 7, p. 95–107, 2020. DOI:

10.5281/zenodo.3969652. Disponível em:

<http://revistajrg.com/index.php/jrg/article/view/41>. Acesso em: 3 ago. 2021.

GONÇALVES, Jonas Rodrigo. Como escrever um artigo de revisão de literatura. Revista JRG de Estudos Acadêmicos, v. 2, n. 5, p. 29–55, 2019. DOI: 10.5281/zenodo.4319105.

Disponível em: <http://revistajrg.com/index.php/jrg/article/view/122>. Acesso em: 13 ago. 2021.

GONÇALVES, Jonas Rodrigo. Como fazer um projeto de pesquisa de um artigo de revisão de literatura. Revista JRG de Estudos Acadêmicos, v. 2, n. 5, p. 01–28, 2019. DOI:

10.5281/zenodo.4319102. Disponível em:

<http://revistajrg.com/index.php/jrg/article/view/121>. Acesso em: 13 ago. 2021.

GONÇALVES, Jonas Rodrigo. Escolha do tema de trabalho de curso na graduação em Direito. Revista Coleta Científica, v. 5, n. 9, p. 88–118, 2021. DOI: 10.5281/zenodo.5150811.

Disponível em: <http://portalcoleta.com.br/index.php/rcc/article/view/58>. Acesso em: 13 ago. 2021.

JUSBRASIL. Direito à privacidade: intimidade, vida privada e imagem. Disponível em:

<http://quentasol.jusbrasil.com.br/artigos/214374415/direito-a-privacidade-intimidade-vidaprivada-e-imagem>. Acesso em: 8 set. 2016.

KUROSE, Ross. Redes de computadores e a internet: uma abordagem top-down. 5. ed. 2012.

OFICINA DA NET. Diferença entre: vírus, spam, spyware, worm, phishing, botnet, rootkit.

Disponível em: <https://www.oficinadanet.com.br/post/12991-diferenca-entre-virusspam-spyware-worm-phishing-botnet-rootkit>. Acesso em: 13 set. 2016.

ONU. Declaração Universal dos Direitos Humanos (DUDH). Disponível em: <http://www.dudh.org.br/declaracao/>. Acesso em: 11 set. 2016.

RODRIGUES, Juliana Fernandes Alvares; CRUZ, Diego Henrique da. Crimes cibernéticos e a falsa sensação de impunidade. Revista Científica Eletrônica do Curso de Direito, v. 13, jan.-jun. 2018. Disponível em: <http://revista.fae.br/pub/1786>. Acesso em: 27 out. 2025.