Revista Escola de Governo de Alagoas
2ª Edição – Vol. 1 – 2024

DOI 10.5281/zenodo.13942044

CRIMES CIBERNÉTICOS E LEGISLAÇÃO PENAL: UMA ANÁLISE HISTÓRICA SOB O CÓDIGO DE HAMURABI

CYBERCRIMES AND PENAL LEGISLATION: A HISTORICAL ANALYSIS UNDER THE CODE OF HAMMURABI

Amanda Ribeiro Santos [1]
Francisco de Assis Nascimento Júnior [2]

RESUMO

Este artigo explora as leis do Código de Hamurabi em relação ao homicídio, fornecendo uma análise comparativa entre este antigo código e as leis atuais, destacando aspectos preservados, modificações e diferenças. Além disso, o estudo examina a evolução da legislação penal brasileira em resposta aos crimes cibernéticos, discutindo os desafios enfrentados pela legislação na era digital e a necessidade de superar esses obstáculos. O artigo analisa a capacidade da legislação penal brasileira de evoluir e se adaptar, com foco nas leis 12.735 e 12.737 e no Marco Civil da Internet. A metodologia utilizada compreende investigação literária, análise *ex-post facto*, estudo de corte, análise de caso, pesquisa qualitativa e quantitativa, estudo descritivo e pesquisa de precedentes legais. As expectativas de resultados abrangem a formulação de uma teoria lógica e sólida sobre os padrões de avaliação das leis, a contribuição para discussão acadêmica e legal sobre o tema, e a análise da necessidade de conscientizar e educar a população a fim de evitar a prática de crimes ilícitos por meio da rede.

Palavras-chave: Legislação Penal Brasileira. Código de Hamurabi. Justiça Equitativa. Crimes Cibernéticos. Desafios da Era Digital.

ABSTRACT

This article explores the laws of the Code of Hammurabi regarding homicide, providing a comparative analysis between this ancient code and current laws, highlighting preserved aspects, modifications and differences. In addition, the study examines the evolution of Brazilian criminal legislation in response to cybercrimes, discussing the challenges faced by legislation in the digital age and the need to overcome these obstacles. The article analyzes the capacity of Brazilian criminal legislation to evolve and adapt, focusing on laws 12.735 and 12.737 and the Internet Civil Rights Framework. The methodology used includes literary research, ex-post facto analysis, court study, case analysis, qualitative and quantitative research, descriptive study and research of legal precedents. The expected results include the formulation of a logical and solid theory on the standards of evaluation of laws, the contribution to academic and legal discussion on the subject, and the analysis of the need to raise awareness and educate the population in order to prevent the practice of illicit crimes through the Internet.

***Keywords*:** Brazilian Criminal Legislation. Code of Hammurabi. Equitable Justice. Cybercrimes. Challenges of the Digital Age.

[1] Acadêmica da UFSB), atualmente matriculada no Bacharelado Interdisciplinar em Humanidades, no Campus Sosígenes Costa, em Porto Seguro.Atua como pesquisadora nas áreas de ciências humanas aplicadas, história do direito, direitos humanos, direitos constitucionais, direito administrativo, direito penal e direito processual. Atualmente, está vinculada ao Banco de Projetos de Bolsa de Apoio à Permanência (BAP) na UFSB. **Email:** amanda.ribeiro@gfe.ufsb.edu.br

[2] Graduado em Física, mestre em Ensino de Ciências (Física) pelo Instituto de Física e doutor em Educação pela Faculdade da USP. Francisco é professor adjunto do Programa de Pós-Graduação em Ensino e Relações Étnico-Raciais (PPGER) da UFSB. Diretor do Instituto de Humanidades, Artes e Ciências do Campus Sosígenes Costa da Universidade Federal do Sul da Bahia (UFSB - IHAC). E-mail: francisco.nascimento@ufsb.edu.br

INTRODUÇÃO

O Código de Hamurabi, amplamente conhecido como o primeiro compêndio de leis escritas existente, proporciona uma visão para o entendimento dos fundamentos de justiça e implementação da lei nas civilizações antigas.

As leis eram estabelecidas de tal maneira que não permitiam desculpas ou justificativas para erros ou falhas: o código era publicamente visível para todos, de forma que ninguém pudesse alegar desconhecimento da lei como defesa. No entanto, vale lembrar que poucos sabiam ler naquela época. Na era digital atual, os crimes cibernéticos tornaram-se uma preocupação crescente. Para entender como a legislação penal evoluiu para lidar com esses crimes, é útil olhar para trás, para o primeiro alfarrábio de leis escritas existente, o Código de Hamurabi. (Pedros, 2002, p. 463).

Segundo Pedrosa (2002), é importante destacar que o Código de Hamurabi não se resume a penalidades e disposições de morte, como muitos sugerem. Ele apresenta alguns princípios que, sem dúvida, foram adotados por legislações subsequentes e incorporados ao universo jurídico. Assim, este artigo explora o Código de Hamurabi, instituído por volta de 1700 a.C. pelo rei Khammurabi, com o propósito de estabelecer leis baseadas em costumes para organizar e governar a região da Mesopotâmia. (Pedrosa, 2002, p. 73).

De acordo com os textos históricos, as leis abordaram as primeiras preocupações com os direitos humanos, buscando “proteger” os mais fracos dos mais fortes, estabelecer a justiça para assegurar a segurança, os direitos e as responsabilidades, além de promover o bem-estar do povo. Nesse contexto, Hamurabi foi escolhido pelos próprios deuses, Anu e Bel, o que conferia ao rei total respeito e incontestabilidade.

Hamurabi, o monarca, concebeu 282 leis que englobavam uma variedade de temas, tais como adoção, furtos, agricultura, incesto, divórcios, pagamentos, salários e homicídios, com o intuito de garantir a observância das obrigações e o respeito recíproco entre os indivíduos. De acordo com a legislação, se um crime fosse cometido ou se uma moradia construída desmoronasse e resultasse na morte de um filho da família, o arquiteto responsável pelo erro teria que compensar com a vida de seu próprio filho. Percebe-se que as leis de Hamurabi eram regidas pela doutrina do “olho por olho, dente por dente”, uma frase famosa que tem como base a lei de talião. (Pedrosa, 2002, p. 71).

Como mencionado anteriormente, as leis de Hamurabi eram extremamente severas em relação

às sanções aplicadas aos infratores. A pena de morte era uma punição aceita nesta legislação, além de mutilações, de acordo com os crimes cometidos. O código funcionava da seguinte forma: para cada ato fora da lei haveria uma punição, que acreditavam ser proporcional ao crime cometido. Sabe-se que até então, a justiça era feita única e exclusivamente para o lado mais forte, não havia a oportunidade do contraditório, e tudo era resolvido da maneira comissória e acreditava ser a maneira mais correta possível. (Pedrosa, 2002, p. 71).

Para realizar este projeto, será adotada uma metodologia descritiva, quantitativa e qualitativa baseada em estudo descritivo e pesquisa de precedentes legais, conjuntamente à pesquisa nos sites dos tribunais de Justiça Estaduais, Tribunais superiores, em especial as decisões das Turmas do Superior Tribunal de Justiça (STJ) e do Supremo Tribunal Federal (STF), e principalmente o Código Penal Brasileiro, para verificar, assim, os entendimentos doutrinários e os recentes julgados. Além de uma pesquisa realizada nas bases de dados do Scielo e Capes, seguida de uma metassíntese qualitativa dos achados, ou seja, uma interpretação condensada dos dados. Por exemplo, na pesquisa qualitativa, por sua vez, foca em aprofundar o entendimento, convertendo a quantidade em qualidade, evoluindo de um conhecimento amplo superficial para um conhecimento restrito e profundo. Isso contribui para a competência e eficiência na obtenção da qualidade. Fernandes (2001, p. 48) em seu trabalho pondera: A qualidade só será atingida quando se alcançar o nível supremo de excelência, que abrange competência e eficiência. Durante a jornada, parte-se da ineficácia e começa-se a ser competente; porém, a eficiência só é alcançada quando se atinge o objetivo. (Fernandes, 2001, p. 48).

Ainda nos dizeres de Pedrosa (2002), o Código de Hamurabi procurou estabelecer a justiça em sua época, a legislação penal brasileira também evoluiu ao longo dos anos para lidar com novos tipos de crimes, como os crimes cibernéticos. Ou seja, com o avanço das leis e a consolidação de estudos sobre as punições, o Direito compreendeu que a justiça não era aplicada pela Lei do Talião. Fazer um indivíduo pagar pelo erro de outro não promovia a segurança social e não favorecia o bom cidadão. A trajetória histórica brasileira mostra que os direitos e os princípios que protegem a dignidade humana foram alcançados progressivamente. Desde a época monárquica até a era republicana, as garantias fundamentais foram ganhando espaço em nossa legislação, tornando-a cada vez mais humanizada.

Nossa legislação penal brasileira, que tem suas raízes no Código Criminal do Império do Brasil de 1830, avançou e foi influenciada pelas ideias iluministas europeias. No entanto, o código não abordava crimes cibernéticos, pois a tecnologia da época não permitia tais infrações. Em outras palavras, mesmo com o advento da internet e da tecnologia digital, surgiu a

necessidade de leis que abordassem os crimes cibernéticos. (Pedrosa, 2002, p. 430).

Em 2012, a Lei Carolina Dieckmann foi promulgada em resposta ao vazamento de fotos íntimas da atriz A lei torna crime a invasão de dispositivos eletrônicos para obtenção de dados pessoais. No ano seguinte, em 2013, o Marco Civil da Internet foi estabelecido, fornecendo uma base legal para a internet no Brasil. Ele aborda direitos e deveres dos usuários da internet, incluindo proteção de dados e privacidade.

No entanto, a legislação ainda enfrenta desafios, principalmente depois da pandemia. De acordo com os dados do Ministério Público, a internet avançou principalmente nesta época. Por conta disso, a natureza global da internet tornou difícil a aplicação das leis, e a rápida evolução da tecnologia muitas vezes supera a capacidade da legislação de acompanhar. Além disso, a falta de conhecimento técnico entre os profissionais do direito pode dificultar a compreensão e a aplicação eficaz das leis.

Apesar desses desafios, a legislação penal brasileira continua a evoluir para abordar os crimes cibernéticos. Com o aumento da digitalização, é provável que vejamos mais mudanças nessa área no futuro. Entende-se que os delitos digitais podem se manifestar de várias maneiras, causando graves consequências e danos às vítimas e estão constantemente presentes em toda a sociedade.

Em relação aos delitos digitais, esses infratores têm a percepção de impunidade, o que acaba sendo um incentivo muito forte para o aumento desse tipo de infração. As ameaças podem ser tanto por meio de vigilância não autorizada do sistema, quanto através de ataques mais complexos realizados por *hackers*[3]. Compreendemos que quando se trata de crimes cibernéticos exclusivos, ocorre apenas por meios digitais, que requer um computador para que esse crime seja exclusivo, ou seja, sendo realizado apenas por redes de computadores, os crimes que ocorrem de forma cibernética e sem ser de forma cibernética como crimes de violação de direitos são considerados crimes abertos, que podem ocorrer tanto pelo computador quanto pessoalmente.

Assim, pode-se entender dois modelos em relação aos crimes cibernéticos, sendo eles ocorrendo, sendo destacado por meio dos artigos 154 do Código Penal Brasileiro, que destaca sobre invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o objetivo de obter, adulterar ou destruir dados ou informações sem autorização expressa

[3]Para Castells (2003) hackers não passariam de uma comunidade contracultural específica de geeks e nerds2 . Sem a cultura hacker, as redes comunitárias na Internet não se distinguiriam de muitas outras comunidades alternativas. Assim como, sem a cultura hacker e os valores comunitários, a cultura empresarial não se pode caracterizar específica à Internet (CASTELLS, 2003, p. 34).

ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita, e pode ocorrer no meio aberto, como os crimes exemplificados na citação acima, como estelionatário que pode ocorrer pela internet e também fora dela. No entanto, ao contrário do Código de Hamurabi, a legislação brasileira evoluiu para além da Lei do Talião e busca proteger a dignidade humana e adaptar-se às mudanças tecnológicas.

2. A EVOLUÇÃO DA LEGISLAÇÃO PENAL E A EMERGÊNCIA DOS CRIMES CIBERNÉTICOS

No período antigo, a aplicação de punições era frequentemente cruel e desumana, servindo como um meio de intimidação e controle social. Na Grécia, por exemplo, a pena capital era uma prática comum para delitos graves como homicídio, roubo e traição. Em Roma, o Direito Penal se fundamenta em leis escritas e na figura do imperador, que detinha o poder de conceder ou negar misericórdia aos condenados. (Pedrosa, 2002, p. 97).

Durante a Idade Média, o Direito Penal foi caracterizado pela influência da Igreja Católica e pela imposição de penas físicas, como flagelação, mutilação e tortura. A Inquisição foi uma instituição significativa nesse período, encarregada de perseguir e julgar os hereges e outros crimes contra a fé católica.

Ao longo da história, o Direito Penal progrediu e se transformou, acompanhando as mudanças sociais, culturais e políticas de cada época. A evolução do Direito Penal reflete a busca da sociedade por uma justiça mais equitativa e humana, respeitando os direitos fundamentais. (Pedrosa, 2002, p. 456).

Compreender a história do Direito Penal é crucial para entender as raízes da justiça contemporânea e pensar em novas soluções para os desafios do século XXI. Porém, à medida que a sociedade continuava a evoluir, surge a era digital, uma nova categoria de delitos, conhecida como crimes cibernéticos, emergiu. Os crimes cibernéticos, também conhecidos como delitos digitais, são atividades ilegais que envolvem computadores ou redes de computadores, como a internet. Porém, é importante entender primeiro a diferença entre ‘dispositivo informático’ e ‘dispositivo eletrônico’. Um ‘dispositivo informático’ é qualquer dispositivo que pode receber, armazenar, processar ou enviar informações digitais, como um computador ou smartphone. Por outro lado, um ‘dispositivo eletrônico’ é um termo mais amplo que inclui qualquer dispositivo que usa eletricidade, o que significa que todos os dispositivos informáticos são dispositivos eletrônicos, mas nem todos os dispositivos eletrônicos são dispositivos informáticos.

É fácil ver que os delitos digitais podem abranger desde a entrada não permitida em sistemas até a disseminação de vírus e programas maliciosos, golpes na internet e assédio virtual. Um exemplo real de ataques digitais foi o que aconteceu na rede de computadores do Superior Tribunal de Justiça (STJ) em 2020, destacando a fragilidade das estruturas digitais, inclusive de órgãos governamentais de grande importância. Esse tipo de ocorrência pode resultar não só em danos financeiros, mas também em um impacto significativo na integridade das instituições e na confiança dos cidadãos.

Portanto, enfrentar os crimes cibernéticos requer ferramentas de investigação modernas e adaptáveis ao mundo digital em constante mudança. É crucial que as autoridades estejam preparadas não só para identificar e punir os infratores, mas também para coletar e guardar provas digitais para uso em processos legais.

A sensação de impunidade é outro fator que intensifica os crimes cibernéticos. Essa sensação é frequentemente decorrente da dificuldade em identificar e punir os autores e da falta de conhecimento por parte das vítimas sobre seus direitos e as medidas legais que podem adotar. Ainda numa perspectiva social, o avanço dos crimes cibernéticos tem afetado diretamente a vida privada das pessoas. Uma vez que a invasão de privacidade, o roubo de identidade e a difamação online são ameaças constantes na era digital, causando danos psicológicos e emocionais às vítimas.

Diante do exposto, a visão geral das legislações penais passadas reflete o quanto avançamos, tanto em relação às codificações quanto às penas aplicadas, derrubando conceitos obsoletos e infundados em relação aos delitos. Este progresso foi impulsionado pela secularização dos Estados e pelo reconhecimento da dignidade humana.

Retornando cronologicamente, ressaltamos as contribuições de cada Estado para a formação do que hoje conhecemos como Direito Penal. Este é uma compilação dos melhores princípios adotados pelos códigos anteriores. O objetivo é conferir legitimidade e eficácia a este instituto, que é um dos ramos mais importantes do Direito, pois protege os bens mais valiosos para o indivíduo, como a vida e o patrimônio. (Pedrosa, 2002, p. 457).

Percebe-se que a progressão dos delitos digitais e a subsequente demanda por um quadro legal específico para sua regulamentação e repressão são incontestáveis, visto que a legislação penal teve que evoluir para lidar com a emergência dos crimes cibernéticos.

Contudo, a implementação dessas leis enfrenta obstáculos, uma vez que a tecnologia se desenvolve em um ritmo mais acelerado do que as leis conseguem acompanhar. Além das perdas financeiras diretas, os crimes cibernéticos também implicam custos intangíveis para as empresas, como a deterioração da reputação, a desvalorização da marca e a perda de confiança

dos clientes. Este aspecto social é crucial, pois a confiança é um dos pilares do comércio eletrônico e das interações online.

A seguir, será realizada uma exposição sucinta das leis consideradas mais significativas, com o propósito de tentar avaliar a que distância estamos de alcançar uma proteção adequada dos interesses civis e governamentais, no que se refere à questão cibernética. Além disso, não está dentro do escopo deste artigo detalhar todo o cenário legislativo brasileiro, uma vez que as legislações mencionadas a seguir servirão apenas como referência para a leitura.

É importante destacar dois projetos de lei específicos que desempenham um papel crucial na legislação brasileira sobre crimes cibernéticos: o Projeto de Lei (PL) 84/99 e a Lei 12.735/12. O PL 84/99, inicialmente apresentado pelo ex-deputado federal Luiz Piauhylino e posteriormente modificado pelo então senador Eduardo Azeredo, propôs uma série de medidas para lidar com delitos cometidos no ambiente virtual. No entanto, este projeto enfrentou críticas devido à sua linguagem imprecisa e potencial impacto sobre a privacidade e a liberdade na Internet.

Por outro lado, a Lei 12.735/12, também conhecida como Lei Azeredo, trouxe mudanças significativas. Esta lei alterou o inciso II do § 3° do art. 20 da Lei n° 7.716/8918, conhecida como Lei do Crime Racial, para permitir que um pedido de retirada de conteúdo discriminatório não apenas de rádio, TV ou Internet, mas de qualquer meio possível, fosse feito pelo juiz. Além disso, determinou que os órgãos da polícia judiciária deveriam criar delegacias especializadas no combate a crimes praticados por meio da Internet ou por sistema informatizado.

Essas leis são fundamentais para entender o cenário atual dos crimes cibernéticos no Brasil e a evolução da legislação penal para lidar com esses novos desafios. Elas refletem a necessidade contínua de adaptar nosso sistema legal brasileiro à rápida evolução da tecnologia e aos novos tipos de crimes que surgem.

De coautoria do então Deputado Federal Paulo Teixeira, a Lei Dieckmann praticamente resgatou o que o PL 84/99 perdeu, contudo, sem as polêmicas da época, dispondo sobre delitos informáticos, tipificando condutas que não eram previstas, de forma específica, como infrações penais.

Foi criado o tipo penal “invasão de dispositivo informático”, previsto no art. 154-A do Código Penal Brasileiro, e sua respectiva modalidade de ação penal, prevista no art. 154-B do mesmo Código, que é, em regra, condicionada a representação. Acontece que com a inclusão desses dois dispositivos, a redação dos delitos previstos nos arts. 266 e 298, do mesmo diploma legal, foi ampliada. Assim, a categoria de crime de interrupção de serviço público agora inclui serviços de telemática ou informações de utilidade pública. Quanto ao crime de falsificação de

documento privado, a nova legislação adicionou a equivalência do cartão de crédito ou débito a um documento privado.

Apesar de parecerem suficientes, ambas as Leis 12.735 e 12.737 não conseguiram preencher todas as lacunas que a legislação brasileira tinha em relação ao combate aos crimes cibernéticos.

Na realidade, existem algumas falhas que precisam ser corrigidas imediatamente para evitar a impunidade. A Lei Dieckmann, por exemplo, não classificou como delito a interrupção de sistemas de informação de organizações privadas, como sites bancários. Ainda, houve uma negligência do legislador ao determinar que "obter, adulterar ou destruir", presentes no *caput* do art. 154-A do Código Penal, sejam elementares ao tipo penal de invasão a dispositivo, pois, dessa forma, o simples ato de vasculhar não se adequaria ao tipo penal. Sem contar que a Lei deixa os dispositivos que não têm mecanismos de segurança - como uma senha – completamente desprotegidos.

Vale trazer para complementar o artigo Marco Civil da Internet, por sua vez, originou-se do combate ao polêmico PL 84/99, por isso, teve grande participação popular. Durante sua elaboração, foram realizadas consultas públicas, que se dividiram em duas fases: uma com vasta diversidade de opiniões, incluindo a sociedade civil e as mais variadas empresas, nacionais e internacionais, do ramo digital, e outra, também com participação popular, mas discutindo cada dispositivo proposto na primeira fase.

Um dos objetivos do Marco Civil da Internet era indicar um documento que servisse como base para regular os princípios gerais do Marco Civil. O referido documento-base foi o publicado pelo CGI.br - Comitê Gestor da Internet no Brasil, chamado "Princípios para a Governança e Uso da Internet no Brasil".

Da mesma forma que a Lei 12.735 e a Lei Dieckmann, o Marco Civil é insuficiente, por mais que pareça ser eficaz ao tratar dos direitos do usuário. O ato de introduzir ferramentas judiciais do mundo físico – como a obtenção de ordem judicial – no mundo virtual é contraproducente, uma vez que as velocidades entre os dois mundos são incompatíveis, enquanto o primeiro é mais moroso, o segundo requer cada vez mais celeridade.

Portanto, observou-se que a concretude da prova nos delitos cibernéticos surge como um ponto fundamental. A conservação de provas digitais e sua aceitabilidade em processos judiciais são questões que exigem ponderação e ajustes no sistema jurídico, visando assegurar a justiça e a efetividade das sentenças. O ambiente digital, com suas particularidades, demanda uma abordagem jurídica adaptada, que leve em conta tanto as especificidades tecnológicas quanto às garantias processuais convencionais.

Em conclusão, a temática dos crimes cibernéticos e da desinformação no Brasil é um campo em constante evolução e que requer uma atenção cuidadosa do Direito. A interação entre tecnologia, sociedade e legislação deve ser harmonizada de maneira a assegurar uma internet segura, equitativa e livre para todos os seus usuários. A busca por esse equilíbrio, como demonstrado, é um percurso contínuo e indispensável no cenário atual.

CONSIDERAÇÕES FINAIS

O desenvolvimento da legislação penal brasileira em resposta aos crimes cibernéticos ilustra a capacidade do nosso sistema jurídico de se adaptar e resistir ao longo do tempo. Desde os primórdios do Direito Penal, onde as punições eram muitas vezes cruéis e desumanas, até a era moderna que busca uma justiça mais equitativa e humana, a legislação penal tem refletido as transformações sociais, culturais e políticas de cada período.

No entanto, conforme destacado na introdução, a legislação ainda enfrenta desafios significativos, especialmente na era digital. A rápida evolução da tecnologia, a natureza global da internet e a falta de conhecimento técnico entre os profissionais do direito são obstáculos que precisam ser superados. Além disso, a percepção de impunidade entre os infratores de crimes cibernéticos é um problema que precisa ser abordado.

Apesar desses desafios, a legislação penal brasileira tem demonstrado uma notável capacidade de evoluir e se adaptar. As leis 12.735 e 12.737, apesar de suas limitações, representam passos importantes na luta contra os crimes cibernéticos.

Da mesma forma, o Marco Civil da Internet, apesar de suas falhas, estabeleceu uma base legal crucial para a internet no Brasil. À verdade é que a mera elaboração de uma norma ainda não é suficiente para combater a violência, pois o Estado precisa dar mais conscientização à população, implementando mais conteúdos que eduquem nossa sociedade brasileira para que se possa evitar a prática de crimes ilícitos por meio da rede.

Com base na avaliação da legislação brasileira, este artigo deixa claro que, no direito brasileiro, algumas ações são cobertas pela legislação atual, mas outras ainda necessitam de novas leis. Neste contexto analisado, o Direito deve acompanhar a evolução da sociedade para que as relações entre os indivíduos que utilizam meios eletrônicos em seu cotidiano não se sintam inseguras em suas interações com terceiros em ambientes virtuais.

Diante disso, a criminalidade virtual tende a aumentar significativamente, uma vez que os avanços tecnológicos continuam a crescer. A legislação, doutrina e jurisprudência brasileira, que surgirão ao longo dos próximos séculos, devem se adaptar a essa realidade de maneira

proporcional, aumentando substancialmente as penalidades ou até criando um sistema de censura em relação às redes sociais e outros meios eletrônicos que estão na rede mundial de computadores. A criação de uma lei que combata a violência digital só se torna eficaz quando as autoridades públicas estão preparadas para lidar com o problema em questão. Apontamos a importância das delegacias de polícia especializadas em crimes cibernéticos, os juízes devem se atualizar nas jurisprudências e doutrinas que envolvem delitos informáticos e os advogados, públicos ou privados, devem acompanhar a evolução do Direito Digital para que possa haver uma melhora no funcionamento da Justiça no Brasil.

Portanto, apesar da evolução contínua do Direito Digital, ainda não existe legislação suficiente para combater a criminalidade digital. Nesse sentido, a lei 12.737/2012 representa um avanço legislativo, pois visa garantir a segurança e proteção do direito ao sigilo dos dados e informações dos indivíduos no ambiente digital, mas não podemos ignorar que a lei ainda precisa ser aprimorada, principalmente em termos de clareza e aplicabilidade de suas disposições.

REFERÊNCIAS

ANDRADE, M. M. de. **Introdução à metodologia do trabalho científico**. 6. ed. São Paulo: Atlas, 2003

ALMEIDA, Haian de Assis Lopes; DE OLIVEIRA, Tamar Ramos. CRIMES VIRTUAIS: O AVANÇO DOS CRIMES ELETRÔNICOS E A EVOLUÇÃO DAS LEIS ESPECÍFICAS NO BRASIL. **Revista Ibero-Americana de Humanidades**, Ciências e Educação, v. 8, n. 11, p. 277-294, 2022.

BECCARIA, Cessare. **Dos Delitos e das Penas**. São Paulo -SP: Ed. Martins Fontes, 1997.

BONINI, Luci Mendes et al. **Crimes Cibernéticos**. Diálogos Interdisciplinares, v. 7, n. 3, p. 223-236, 2018.

BRASIL. Código Penal. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Disponível em:<http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm> Acesso em: 19 jan. 2024.

BRASIL. **Constituição Federal de 1988.** Promulgada em 5 de outubro de 1988. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm> Acesso em 21 fev. 2024.

BRASIL. **Lei Ordinária nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 -Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra

sistemas informatizados e similares; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 25 de abril. 2024.

BRASIL. Lei Ordinária nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos**; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em: 25 de abril. 2024.

BRASIL. Lei Ordinária nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 26 de abril. 2024.

CASTELLS, Manuel. **A Galáxia da Internet**. Rio de Janeiro: Zahar, 2003.

CALGAROTO, Cleber. **O direito à privacidade na internet: panorama, responsabilização civil e inovações do marco civil da internet (Lei nº 12.965/2014)**. Direito-Unisul Virtual, 2021.

CAZAROTI, Tatiane Martins Barros; PINHEIRO, Eduardo Fernandes. C**rimes Cibernéticos. TCC-Direito**, 2021.

CERVO, A. L.; BERVIAN, P. A. **Metodologia científica**. 5ª Ed. São Paulo: Ed. Prentice Hall, 2003.

CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. R**evista Científica Eletrônica do Curso de Direito**, 2018.

DORNELAS, Natália Alves. **A Resposta Estatal Quanto Aos Crimes Cibernéticos: Uma Análise Direcionada Às Leis Nº 12.735/2012 E 12.737/2012**. Repositório de Trabalhos de Conclusão de Curso, 2019.

GATTI, B. A. **Estudos quantitativos em educação**. Educação e Pesquisa, São Paulo, SP, v. 30, n. 1, p. 11-30, jan, 2004.

GIL, A. C. **Método e técnicas de pesquisa social.** São Paulo, SP: Ed. Atlas. 1999.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 5ª Ed.São Paulo: Ed. Atlas,2010

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4ª Ed. São Paulo: Ed. Atlas, 2002.

GIL, A. C. **Como elaborar projetos de pesquisa.** Ed. Atlas, 2008.

GIL, A. C. **Métodos e técnicas de pesquisa social**. Ed. Atlas, 1999.

GOMES, Walyson Milhomem; MEDRADO, Lucas Cavalcante. CRIMES CIBERNÉTICOS UMA PONDERAÇÃO SOBRE A LEI 14.155 DE 2021 APLICÁVEL AO CRIME DE ESTELIONATO VIRTUAL. **Revista Ibero-Americana de Humanidades**, Ciências e

Educação, v. 9, n. 9, p. 1870-1894, 2023.

HERNANDEZ, Erika Fernanda Tangerino; DE TOLEDO, Nathália Karina Abucci. Crimes cibernéticos: seus efeitos revolucionários diante de uma legislação em constante evolução. **Revista Jurídica da UniFil**, v. 17, n. 17, p. 72-84, 2021.

KRIEGUER, André Lemuel Ferreira; CERON, Antonio Luciano Bairros; MARCONDES, Aldair. **A Acelerada Evolução Social E Tecnológica Global Como Viabilizadores De Crimes Cibernéticos, Frente Ao Lento Desenvolvimento De Freios Legais Para Sua Contenção**. Ponto de Vista Jurídico, p. 128-143, 2021.

LIMA, Yasmin Victoria et al. **Direito digital: aplicação nos crimes cibernéticos**. Anais da Semana de Pesquisa Jurídica, v. 1, p. 42-42, 2022.

MARCO, civil da internet entra em vigor. **Cultura Digital.** Disponível em: http://culturadigital.br/marcocivil/2014/06/23/marco-civil-da-internet-entra-em-vigor/. Acesso em: 26 fev. 2024.

MPF, Ministério Público Federal. **Combate aos Crimes Cibernéticos**. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/comissoes-e-grupos-detrabalho/combate-crimes-cirberneticos>. Acesso em: 28 fev. 2024.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro**. 3ª Edição. São Paulo- SP: Ed. Revista dos Tribunais, 2002.

PEDROSA, Ronaldo Leite. **Direito em História**. 4ª Edição. Nova Friburgo-RJ: Ed. Imagem Virtual, 2002.

ZAFFARONI, Eugênio Raúl; PIERANGELI, José Henrique. Manual de Direito Penal Brasileiro. 4ª Edição. São Paulo - SP: Ed. **Revista dos Tribunais**, 2002.