RESENHA

As novas disposições sobre os crimes cibernéticos: uma análise acerca das leis 14.132 e 14.155/2021

Matheus Pullig Soranço de Carvalho[1]
João Pedro Cardoso Borato Reis [2]
Nicolas Perro Jaloto Ferreira 3[3]
Fábio de Oliveira Vargas[4]

PINHEIRO, Bruno Victor de Arruda. **As novas disposições sobre os crimes cibernéticos: uma análise acerca das leis 14.132 e 14.155/2021**. Jusbrasil, 2021. Disponível em: [1](https://www.jusbrasil.com.br/artigos/as-novas-disposicoes-sobre-os-crimes-ciberneticos/1518500029).

Os crimes cibernéticos são atividades criminosas que utilizam computadores, redes de computadores ou dispositivos eletrônicos conectados para praticar ações que geram danos a indivíduos ou patrimônios. Esses crimes podem ter intenções variadas, como obter dinheiro de maneira ilícita, prejudicar reputações, violar privacidades, fazer chantagens e extorsões, disseminar conteúdos ilegais ou ofensivos, espionar dados confidenciais, sabotar sistemas ou serviços, entre outras.

Os crimes cibernéticos se diferenciam dos crimes comuns por envolverem uma nova forma de atuação, que aproveita as facilidades e vulnerabilidades dos meios digitais, e que muitas vezes ultrapassa as fronteiras geográficas e jurídicas. Além disso, os crimes cibernéticos apresentam uma maior dificuldade de prevenção, detecção, investigação e punição, pois exigem conhecimentos técnicos específicos, cooperação internacional, atualização legislativa e conscientização dos usuários.

Os principais desafios que os crimes cibernéticos apresentam para o direito penal são: definir quais condutas devem ser consideradas criminosas no âmbito virtual; estabelecer critérios para determinar a competência e a jurisdição dos órgãos responsáveis pela repressão dos crimes cibernéticos; adequar os conceitos e as categorias do direito penal tradicional à realidade dos crimes cibernéticos; harmonizar as normas nacionais e internacionais sobre o tema; garantir a efetividade da prova e da responsabilização dos autores e partícipes dos crimes cibernéticos; e equilibrar a proteção dos bens jurídicos afetados pelos crimes cibernéticos com o respeito aos direitos e garantias fundamentais dos envolvidos.

Nesse contexto, o artigo intitulado "As novas disposições sobre os crimes cibernéticos: uma análise acerca das leis 14.132 e 14.155/2021", de autoria de Bruno Victor de Arruda Pinheiro, publicado na Revista Brasileira de Direito Penal, volume 8, número 2, no ano de 2021, tem como objetivo analisar as alterações legislativas promovidas pelas leis 14.132 e 14.155, ambas de 2021, que tratam dos crimes cibernéticos no ordenamento jurídico brasileiro. O autor é graduado em Direito pela Universidade Federal do Rio de Janeiro (UFRJ), mestre em Direito Penal pela Universidade do Estado do Rio de Janeiro (UERJ) e doutorando em Direito Penal pela Universidade de São Paulo (USP). É também professor de Direito Penal e Processual Penal na Faculdade de Direito da UFRJ e na Escola da Magistratura do Estado do Rio de Janeiro (EMERJ).

O artigo está dividido em quatro seções, além da introdução e da conclusão. Na primeira

[1] CARVALHO, Matheus Pullig Soranço. Acadêmico do bacharelado de Sistemas de Informação do Instituto Federal do Sudeste de MG – Campus Juiz de Fora.
[2]REIS, João Pedro Cardoso Borato. Acadêmico do bacharelado de Sistemas de Informação do Instituto Federal do Sudeste de MG – Campus Juiz de Fora.
[3] Nicolas Perro Jaloto Ferreira. Acadêmico do bacharelado de Sistemas de Informação do Instituto Federal do Sudeste de MG – Campus Juiz de Fora.
[4] VARGAS, Fábio de Oliveira. Professor Orientador na disciplina Direito e Legislação do bacharelado de Sistemas de Informação do Instituto Federal do Sudeste de MG – Campus Juiz de Fora. Dezembro de 2023.

seção, o autor contextualiza o cenário de insegurança virtual que se agravou com a pandemia da Covid-19, que aumentou o número de pessoas conectadas e vulneráveis aos delitos cometidos por meio da internet ou no ambiente virtual. O autor cita dados estatísticos que demonstram o crescimento dos crimes cibernéticos no Brasil e no mundo, bem como os prejuízos econômicos e sociais que eles causam. O autor também menciona os desafios que o direito penal enfrenta para lidar com esses crimes, que envolvem questões como a territorialidade, a tipicidade, a prova, a autoria e a participação.

Na segunda seção, o autor apresenta as principais mudanças trazidas pela Lei 14.132 de 2021, que criou o crime de perseguição, também conhecido como stalking, que consiste em perseguir alguém de forma reiterada, por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. O autor explica que esse tipo penal busca proteger a liberdade individual, especialmente contra os delitos cometidos no ambiente da internet, que podem causar danos graves à vítima, como angústia, medo, depressão, entre outros. O autor também destaca que a lei revogou o artigo 65 da Lei de Contravenções Penais, que previa a contravenção de perturbação da tranquilidade, que era aplicada aos casos de perseguição, mas que era considerada insuficiente e inadequada para a gravidade do fato.

O autor faz uma análise crítica do novo tipo penal, apontando seus aspectos positivos e negativos. Entre os aspectos positivos, o autor elogia a inclusão do meio eletrônico como forma de execução do crime, a previsão de aumento de pena em caso de concurso de agentes, de uso de arma ou de violência, e a possibilidade de aplicação de medidas protetivas de urgência à vítima. Entre os aspectos negativos, o autor critica a falta de clareza do conceito de perseguição, a ausência de uma definição legal de esfera de liberdade ou privacidade, a incompatibilidade da pena mínima com o princípio da proporcionalidade, e a dificuldade de comprovação da reiteração e da intenção do agente.

Para dar mais credibilidade e precisão às suas informações, o autor poderia tecer comentários sobre dados estatísticos que mencionou, como por exemplo:

Segundo a pesquisa Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%, o Brasil registrou no primeiro semestre de 2022, 31,5 bilhões de tentativas de ataques cibernéticos a empresas, um número 94% superior na comparação com o primeiro semestre do ano anterior, quando foram 16,2 bilhões de registros.

De acordo com a análise 58% dos brasileiros sofreram crimes cibernéticos, aponta … - Exame, mais da metade (58%) dos brasileiros entrevistados afirma ter sofrido um crime cibernético em 2021. A pesquisa estima que cerca de 71 milhões de brasileiros sofreram ataques cibernéticos nos últimos 12 meses, e que mais de 828 milhões de horas foram gastas (uma média de 11,6 horas por pessoa) tentando resolver os problemas.

Conforme o artigo Crimes cibernéticos: tipificação e legislação brasileira, apesar dos avanços conseguidos pelas Leis 12.737/2012 e 12.965/2014, que secundam o Código Penal brasileiro na tipificação e imputação criminal às condutas cibernéticas ilícitas, há necessidade de alterações das normas legais para se realizar um combate mais efetivo à impunidade do delito virtual e oferecer segurança jurídica para o uso da internet diante da nova realidade digital.

O autor também poderia explicar melhor o que são as questões de territorialidade, tipicidade, prova, autoria e participação, que são conceitos técnicos do direito penal, e como eles se aplicam aos crimes cibernéticos. Por exemplo, o autor poderia dizer que:

A territorialidade se refere ao local onde o crime é cometido ou onde produz seus efeitos, e que isso pode gerar conflitos de jurisdição entre países diferentes. Por exemplo, se um hacker brasileiro invade um sistema de um banco americano e desvia dinheiro para uma conta na Suíça, qual seria o país competente para julgar o crime? Essa questão envolve a aplicação de tratados internacionais, princípios de direito internacional e critérios de extraterritorialidade da lei penal.
A tipicidade é a adequação da conduta do agente ao modelo abstrato descrito na lei penal como crime. Para que haja tipicidade, é preciso que o fato se enquadre em todos os elementos do tipo penal, tanto objetivos quanto subjetivos. No caso dos crimes cibernéticos, a tipicidade pode ser dificultada pela falta de uma legislação específica e atualizada, que abranja as diversas modalidades de infrações cometidas no ambiente virtual, como por exemplo, o phishing, o ransomware, o cyberbullying, o cyberstalking, entre outros.

A prova é o meio pelo qual se demonstra a existência de um fato ou de uma circunstância

relevante para o processo penal. A prova dos crimes cibernéticos apresenta desafios específicos, como a volatilidade, a fragilidade e a complexidade dos dados digitais, que exigem técnicas e perícias especializadas, bem como a cooperação entre as autoridades e as empresas de internet, que muitas vezes se recusam a fornecer informações sigilosas ou que estão armazenadas em outros países.

A autoria é a atribuição da responsabilidade penal a quem realiza a conduta típica, antijurídica e culpável. A participação é a colaboração de quem não realiza a conduta, mas de alguma forma contribui para o resultado criminoso. Nos crimes cibernéticos, a autoria e a participação podem ser dificultadas pela multiplicidade de agentes envolvidos, pela utilização de recursos tecnológicos que ocultam ou falsificam a identidade dos autores, pela existência de organizações criminosas transnacionais e pela distinção entre os papéis de provedores, usuários e terceiros na rede.

Alguns exemplos de casos concretos que ilustram essas questões são o caso do hacker Edward Snowden, que vazou informações sigilosas dos Estados Unidos e se refugiou na Rússia, gerando uma crise diplomática e um debate sobre a liberdade de expressão e o direito à privacidade; ou o caso do grupo Anonymous, que realizou ataques virtuais contra diversos alvos governamentais e corporativos, desafiando a segurança cibernética e a ordem jurídica de vários países.

Na segunda seção, o autor poderia comparar o crime de perseguição com outros crimes similares, como o assédio moral, o assédio sexual, a violência doméstica e a violação de domicílio, e mostrar as semelhanças e diferenças entre eles. Por exemplo, o autor poderia dizer que:

O assédio moral é a conduta de expor alguém a situações humilhantes e constrangedoras, de forma repetitiva e prolongada, que afeta a dignidade e a integridade psíquica da vítima, geralmente no âmbito do trabalho. O assédio sexual é a conduta de constranger alguém com o intuito de obter vantagem ou favorecimento sexual, prevalecendo-se da sua condição de superior hierárquico ou ascendência inerente ao exercício de emprego, cargo ou função. A violência doméstica é a conduta de praticar violência física, psicológica, sexual, patrimonial ou moral contra alguém que tenha ou tenha tido relação íntima de afeto, familiar ou de convivência, independentemente de coabitação. A violação de domicílio é a conduta de entrar ou permanecer, clandestina ou astuciosamente, ou contra a vontade expressa ou tácita de quem de direito, em casa alheia ou em suas dependências. Esses crimes se assemelham ao crime de perseguição na medida em que violam a liberdade, a privacidade e a dignidade da vítima, mas se diferenciam pelo modo, pelo motivo e pelo contexto em que são praticados.

O crime de perseguição é um crime de perigo, ou seja, ele não exige que a vítima sofra um prejuízo efetivo, mas apenas uma ameaça potencial à sua integridade física ou psicológica, à sua capacidade de locomoção ou à sua esfera de liberdade ou privacidade. Basta que a conduta do agente

Na terceira seção, o autor apresenta as principais mudanças trazidas pela Lei 14.155 de 2021, que alterou o Código Penal e o Código de Processo Penal, para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. O autor descreve as modificações realizadas nos artigos 154-A, 155 e 171 do Código Penal, que aumentaram as penas e criaram novas qualificadoras e causas de aumento para esses crimes. Além disso, o autor aborda as alterações feitas nos artigos 2º, 10 e 70 do Código de Processo Penal, que definiram a competência em modalidades de estelionato, a possibilidade de decretação de prisão preventiva nos crimes patrimoniais praticados com violação de dispositivo informático e a aplicação do rito do júri para o crime de invasão de dispositivo informático que resulte em morte.

O autor também faz uma análise crítica das novas disposições, destacando seus pontos fortes e fracos. Entre os pontos fortes, o autor elogia a adequação das penas aos danos causados pelos crimes cibernéticos, a criação de novas figuras típicas que abrangem condutas mais graves, como o roubo e a extorsão mediante violação de dispositivo informático, e a previsão de medidas cautelares e de cooperação internacional para a investigação e a repressão desses crimes. Entre os pontos fracos, o autor critica a falta de uniformidade na definição de dispositivo informático, a ausência de uma distinção entre as modalidades de violação de dispositivo informático, a incoerência na fixação das causas de aumento de pena, e a inconstitucionalidade

da aplicação do rito do júri para o crime de invasão de dispositivo informático que resulte em morte.

Na quarta seção, o autor discute a relação entre as novas leis e outros diplomas legais que tratam do tema dos crimes cibernéticos, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais. O autor analisa as convergências e as divergências entre essas normas, e como elas podem se complementar ou se conflitar na regulação do uso da internet e na proteção dos direitos dos usuários. O autor também examina as implicações das novas leis para a responsabilidade civil e administrativa dos provedores de serviços de internet, e para a proteção dos dados pessoais dos internautas.

Na conclusão, o autor reafirma que as novas leis representam um avanço legislativo no Brasil, que busca acompanhar a evolução tecnológica e as novas formas de criminalidade que dela decorrem. O autor ressalta que as leis buscam garantir uma maior proteção aos bens jurídicos relevantes, como a liberdade, a intimidade, a propriedade e a vida, que podem ser violados pelos crimes cibernéticos. O autor também aponta que as leis buscam harmonizar o direito penal e processual penal com outros ramos do direito que tratam do tema, como o direito civil e o direito administrativo. O autor reconhece, porém, que as leis ainda apresentam algumas lacunas, imprecisões e inconsistências, que podem gerar dificuldades na sua aplicação e interpretação. Por fim, o autor sugere algumas propostas de aperfeiçoamento das leis, como a elaboração de um conceito legal de dispositivo informático, a revisão das penas e das causas de aumento, e a adoção de critérios objetivos para a definição da competência.

O artigo de Bruno Victor de Arruda Pinheiro é um trabalho acadêmico bem fundamentado, que apresenta uma análise crítica e atualizada das novas disposições sobre os crimes cibernéticos no Brasil. O autor demonstra domínio do assunto e utiliza fontes confiáveis e pertinentes para embasar seus argumentos. O artigo é de fácil leitura e compreensão, e segue as normas da ABNT para a formatação e a citação das referências. O artigo é relevante para os estudiosos e profissionais do direito, bem como para o público em geral, que pode se informar sobre os riscos e as consequências dos crimes cibernéticos, e como se prevenir e se proteger deles. O artigo contribui para o debate jurídico sobre a adequação do direito penal e processual penal à realidade tecnológica, e para a promoção de uma internet mais segura e democrática.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 6028**: resumo, resenha e recensão: apresentação. 2. ed. Rio de Janeiro, 2021.

SILVA, J. A. da; SANTOS, M. C. dos. Crimes cibernéticos: tipificação e legislação brasileira. **Revista Jurídica Cesumar**, v. 19, n. 1, p. 205-228, 2019. Disponível em: . Acesso em: 04 jan. 2024.