CRIMES CIBERNÉTICOS NA LEGISLAÇÃO PENAL BRASILEIRA: PREVENÇÃO E REPRESSÃO

Gabriel Faria Ziviani; Ms. Fábio Luís Guimarães

Crimes cibernéticos ou cibercrimes são aqueles praticados mediante a utilização da internet, rede de computadores ou dispositivos conectados em rede. A globalização econômica e a revolução tecnológica, marcas do século XXI, deram origem a mundo virtual, sem barreiras geográficas e com interações sociais que potencializaram práticas criminosas, via internet. Assim, mundialmente, a legislação penal precisou se adequar para a prevenção e a repressão de crimes desta natureza. O presente trabalho analisa a evolução da legislação penal brasileira que trata de crimes cibernéticos, com o objetivo geral de discutir sua efetividade no combate e repressão dos mesmos. A pesquisa incluiu o estudo da legislação pertinente e uma análise crítica de sua efetividade, a partir da revisão bibliográfica de autores que abordam a temática. Os resultados da pesquisa indicam avanços importantes na tipificação dos crimes cibernéticos, mas apontam desafios significativos para a identificação e a devida punição daqueles que os praticam.

PALAVRAS CHAVE: Crimes cibernéticos; prevenção e repressão.

INTRODUÇÃO

A globalização econômica e a revolução tecnológica, marcas do início século XXI, estabeleceram um grande paradoxo mundial: de um lado, possibilitaram um extraordinário avanço das relações entre pessoas, países e culturas, mas, de outro, acirraram a exclusão social daqueles que não se adequaram ao novo mundo digital e estabeleceram um novo cenário para crimes de abrangência transnacional, pelas redes de internet: os crimes cibernéticos ou cibercrimes.

Crimes cibernéticos ou cibercrimes referem-se a toda atividade ilícita praticada na internet, por meio de dispositivos eletrônicos, como computadores e celulares. Neste sentido, atos realizados via rede mundial de computadores com o objetivo de roubar, ofender, prejudicar, abusar psicológica ou fisicamente outro indivíduo, caracterizam-se como crimes cibernéticos.

Muitos crimes praticados no mundo “real” foram introduzidos no mundo “virtual”, mas há crimes que têm no ambiente virtual seu *locus* privilegiado, como o cyberbullying; a invasão de dispositivos informáticos e furto de dados; a publicação não autorizada de fotos da vítima nua ou em situações vexatórias (revenge porn); a espionagem e o terrorismo cibernético; a interferência em sistemas de modo a comprometer uma rede.

Já as fraudes bancárias; a falsificação e supressão de dados; a ameaça, a incitação e apologia de crime; a publicação, troca, obtenção, posse de vídeos e imagens contendo pornografia infantil; o assédio e aliciamento de crianças; o discurso do ódio: discriminação e preconceito; a injúria racial; os crimes contra a propriedade intelectual e artística; a venda ilegal de medicamentos e os jogos de azar, crimes previstos e tipificados no Código Penal Brasileiro, foram potencializados com a velocidade da obtenção e circulação de dados e informações, via sistemas informatizados e com a natureza transfronteiriça da internet.

Nesse contexto, em 2012, o ordenamento brasileiro ganhou duas legislações especialmente dedicadas à prevenção e à repressão de crimes cibernéticos:

A **Lei 12.735/2012**, que alterou o Código Penal, o 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;

A **Lei 12.737/2012**, conhecida como Lei Carolina Dieckmann, que dispôs 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.

Em 2014, foi sancionada a **Lei 12.965/2014**, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e ficou conhecida como Marco Civil da Internet.

Em 2021, a **Lei 14.155/2021** 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; e o Código de Processo Penal, para definir a competência em modalidades de estelionato.

Não obstante o avanço alcançado com o ordenamento brasileiro, no tocante à tipificação e o estabelecimento de penas para as condutas ilícitas por meios virtuais, um passo importante para o fortalecimento das estratégias nacionais de combate e repressão aos crimes virtuais só foi dado em 2023, com o **Decreto 11.491/2023**, que promulgou a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001.

Em síntese, a adesão à Convenção de Budapeste

> "as autoridades brasileiras poderão contar com mais um recurso nas investigações de crimes cibernéticos, assim como de outras infrações penais, que demandem a obtenção de provas eletrônicas/digitais armazenadas em outros países. Prevê-se uma cooperação "mais intensa, rápida e eficaz". (BRASIL: 2023).

Em se tratando de crimes cibernéticos, por mais que os governos e legisladores procurem aperfeiçoar as medidas para a repressão e o combate, dificilmente têm sua abrangência e eficácia asseguradas, tendo em vista a rapidez do surgimento de novos crimes e a facilidade com a qual os criminosos conseguem burlar os mecanismos de defesa e de segurança dos sistemas informatizados. Assim, a identificação e a punição destes, configura-se um dilema mundial.

Dados de uma pesquisa divulgada em outubro deste ano pelo Instituto DataSenado indicam que golpes digitais vitimaram 24% dos brasileiros com mais de 16 anos, no último ano, ou seja, mais de 40,8 milhões de brasileiros foram lesados em função de algum crime cibernético, como clonagem de cartão, fraude na internet ou invasão de contas bancárias.

Pelas redes sociais, perfis falsos espalham injúrias, calúnias e notícias falsas (fake news), provocando gravíssimos danos psicológicos e emocionais em pessoas de várias faixas etárias. As vítimas, muitas vezes, sequer têm informações e recursos

para denunciar os crimes, prevalecendo um sentimento de impotência e o descrédito nas autoridades e leis brasileiras.

Assim, aliada à legislação, faz-se necessária e urgente a adequação e modernização tecnológica dos equipamentos públicos e a formação continuada dos agentes que atuam no combate a esses crimes.

Nesta mesma perspectiva, é fundamental o investimento público em campanhas de conscientização da população sobre a tipificação dos crimes cibernéticos, os meios e canais para a denúncia e as penas previstas para sua punição.

MÉTODO

A metodologia utilizada para a elaboração do presente trabalho serviu-se de uma abordagem descritiva, com o estudo da legislação penal brasileira afeta aos crimes cibernéticos e a revisão da literatura, para a análise crítica do contexto atual.

RESULTADOS E DISCUSSÕES

A legislação brasileira vem buscando se adequar, desde a primeira década dos anos 2000, aos novos desafios impostos pelas interações via rede mundial de computadores: os crimes cibernéticos ou cibercrimes. Nesse sentido, ainda que tardiamente, o Brasil regulamentou, em 2023 a adesão à Convenção de Budapeste.

Os resultados alcançados com esse trabalho indicam que apesar da evolução no ordenamento jurídico no tocante a crimes cibernéticos, a efetividade das leis está restrita à previsão legal e tipificação dos crimes. No campo da repressão e punição dos criminosos, ainda há muito o que se alcançar, em especial quanto ao aparelhamento dos órgãos de segurança e de polícia para a rápida identificação, busca e apreensão destes.

CONCLUSÕES

O Brasil avançou muito, nas últimas décadas, na previsão legal e no estabelecimento de punições para os crimes cibernéticos. No entanto, em se tratando de crimes cibernéticos, não basta ter um ordenamento jurídico, é preciso

aparelhar os órgãos de fiscalização e de segurança para garantir o cumprimento ágil e eficaz das leis, com a rápida identificação e punição dos culpados.

Além disso, é preciso investir em campanhas de conscientização da população sobre o teor das leis.

Para isso, o Brasil precisa avançar na mesma velocidade da internet e contar com a cooperação dos países que estão à frente nessa batalha do mundo real contra o submundo virtual.

REFERÊNCIAS

ARAÚJO, Iran Carlos da Silva. **Os Crimes Cibernéticos e o Direito Penal Brasileiro: proteção pra quem?** Disponível em**: <https://www.jusbrasil.com.br/artigos/os-crimes-ciberneticos-e-o-direito-penal-brasileiro/1894019562>. Acesso em 10/10/2024.**

BRASIL, Código Penal. **Lei 2.848 de 1940**. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm> Acesso em 14/11/2024.

BRASIL, **Lei 12.735/2012.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm#art6 Acesso em 20/11/2024.

BRASIL, **Lei 12.737/2012.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em 20/11/2024.

BRASIL, **Lei 12.965/2014.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 14/11/2024.

BRASIL, **Decreto 11.491/2023** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.> Acesso em 14/11/2024.

BRASIL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Convenção de Budapeste é promulgada no Brasil: Autoridades brasileiras poderão contar com mais um recurso nas investigações de crimes cibernéticos**. Disponível em <https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em 20/11/2024.

BRASIL, AGÊNCIA SENADO. **Golpes digitais atingem 24% da população brasileira, revela DataSenado**. Disponível em <https://https://www12.senado.leg.br/noticias/materias/2024/10/01. Acesso em 14/10/2024.

BRITO, A. **Direito Penal Informático**. São Paulo: Saraiva. 2013.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. 1ª ed. Rio de Janeiro: Brasport, 2014.