RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Cibercriminalidade e a dificuldade em aplicar medidas adequadas devido a carência legislativa no combate aos crimes cometidos no meio virtual

Cybercrime and the difficulty in applying appropriate measures due to legislative lack in combating crimes committed in the virtual environment

Ediná de Souza Meira[33]
Solange Barreto Chaves[34]

Submetido em: 20/05/2022
Aprovado em: 20/05/2022
Publicado em: 21/05/2022 v. 2, n. 1, jan-jun. 2022
DOI: 10.51473/rcmos.v2i1.301

RESUMO

O presente estudo tem por objetivo analisar a evolução dos crimes cibernéticos e a dificuldade na identificação dos responsáveis. Busca-se investigar as causas associadas a prática dos crimes cibernéticos, como a autoria delitiva e a colheita de provas, bem como demonstrar a vulnerabilidade da legislação brasileira frente as práticas delituosas no ambiente virtual, observando a fragilidade de norma especifica na definição de alguns crimes e na aplicação de sanção que corresponda aos ilícitos praticados. Para tanto, a presente pesquisa irá realizar uma análise bibliográfica com materiais publicados em periódicos, revistas, livros e redes eletrônicas. Além de consultas aos sites governamentais para tratar das leis mencionadas.
Palavras-chave: Crimes Cibernéticos. Internet. Legislação. Crimes Virtuais. Insuficiência Legislativa.

ABSTRACT

The present study aims to analyze the evolution of cyber crimes and the difficulty in identifying those responsible. It seeks to investigate the causes associated with the practice of cyber crimes, such as criminais authorship and the collection of evidence. Demonstrate the vulnerability of Brazilian legislation in the face of criminal practices in the virtual environment, observing the fragility of specific norm in the definition of some crimes and in the application of sanctions that correspond to the illicit practiced. Therefore, the present research will carry out a bibliographic analysis with materials published in periodicals, magazines, books and electronic networks. In addition to consultations with government websites to address the aforementioned laws.
Keyword: Cyber Crimes. Internet. Legislation. Virtual Crimes. Legislative Insufficien

1. INTRODUÇÃO

O desenvolvimento tecnológico da humanidade trouxe consigo várias transformações, onde a mais significativa é o surgimento e expansão da Internet, e, consequentemente abrangendo todo o planeta. Apesar do importante papel que a internet desempenha na vida do ser humano, nem tudo é perfeito, pois o indivíduo passou a buscar obter algum benefício, seja legalmente ou ilegalmente.

Dessa forma, a atividade criminosa é um fato alarmante, até mesmo quando se trata da aplicabilidade de lei, visto que na maioria dos casos a identificação dos criminosos é um trabalho árduo, assim costumam permanecer anônimos, e por consequência ficam impunes.

Nesse caso, como bem diz Machado (2017, p.07) "a falta de norma incriminadora para algumas condutas praticadas por meio dos sistemas informáticos, dificultam a aplicação de uma sanção adequada para os que praticam condutas ilícitas". Isto posto, a pesquisa é analisada por meio de metodologia da pesquisa bibliográfica através de livros, materiais

33 Graduanda em Direito pela Faculdade Santo Agostinho de Vitória da Conquista.

34 Graduada em Direito pela Universidade Estadual do Sudoeste da Bahia – UESB (2018); Pós-graduada em Direito Administrativo pela Estácio de Sá (2019); Pós-graduada em Práticas do Ensino Superior pela Faculdade Santo Agostinho – FASAVIC (2022); Pós-graduanda em D. Civil e Proc. Civil pela LEGALE (2022); Mestranda em Direito pela Universidade Católica do Salvador (2022 – 2024); Professora na Faculdade Santo Agostinho nas disciplinas de Processo Civil III e IV, Direito Tributário II, Serviço de atendimento Jurídico I e II e Empreendedorismo Jurídico. E-mail: solange.chaves@vic.fasa.edu.br

publicados em periódicos, revistas e redes eletrônicas. O presente texto aborda questões sobre o direito digital com enfoque na cibercriminalidade e a dificuldade em aplicar medidas adequadas devido a carência legislativa no combate aos crimes cometidos no meio virtual.

2. DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos ou cibercrimes (em inglês, *cybercrimes*) é toda e qualquer atividade ilícita cometida na internet, através de dispositivos eletrônicos, a exemplo dos computadores e celulares. As práticas incluem desde a propagação de vírus até ataques aos sistemas operacionais de empresas e da pessoa privada. Dessa forma, os infratores conseguem ter acesso a informações e dados confidenciais, com o intuito em prejudicar o indivíduo.
Nesse panorama, os crimes informáticos têm início antes mesmo do surgimento da internet. Todavia, com a chegada da internet passa-se a ter diferentes formas de interatividade entre as pessoas, da mesma forma que em que surge os delitos virtuais.

2.1 Espécies

Em se tratando dos tipos de crimes, os que ocorrem em maior frequência são os contra a honra, "crime de difamação, crime de calúnia, crime de injúria" e existem os crimes de: Invasão de privacidade, Espionagem eletrônica, Fraudes virtuais, Pornografia infantil, contra a propriedade intelectual e Estelionato. Conceituando rapidamente da seguinte forma:

- Invasão de privacidade: ocorre o acesso ilegal as informações de usuários, com possibilidade de vazar informações;
- Espionagem eletrônica: por meio dos softwares que espiam informações nos servidores de forma indevida;
- Fraudes virtuais: a conduta refere-se à modificação, alteração ou adulteração de um sistema de processamento de dados ou programa eletrônico;
- Pornografia infantil: tem-se a divulgação ou comercialização de material erótico envolvendo crianças ou adolescentes;
- Contra a propriedade intelectual refere-se aos materiais com dados copiados que circulam livremente;
- Estelionato: tem-se a intenção de adquirir para si ou para outras vantagens ilícitas;

Existem outros crimes ainda possíveis de serem elencados, todavia, estatisticamente não convém destacar na pesquisa posta, voltando-se apenas à uma análise dos mais recorrentes.

2.2 Legislação

Quanto a legislação penal, Ramos (2017, p. 38), destaca que "a Convenção sobre o Cibercrime não dita às regras, mas sim orienta sobre o tema, deixando a critério de cada País, criar sua própria legislação específica".
Assim, permitirá que os governos desenvolvam suas leis e normas para identificar e punir criminosos com base nas particularidades de seus sistemas jurídicos de crimes cibernéticos.
Hoje o ordenamento jurídico brasileiro conta com algumas normas de proteção aos assuntos relacionados ao meio virtual, mas ainda não preenche a carência legislativa da questão no país.

2.3 Da disposição da Lei nº 12.737, de 2012.

Em razão da época em que foi redigido, o Código Penal Brasileiro, não incluía artigos para tratar dos crimes no meio digital, assim, em seu artigo 1º, o Código Penal informa que não há crime, sem prévia definição legal, desse modo os crimes virtuais só passaram a ser tratado com mais destaque a partir de 2012, quando em novembro do mesmo ano, com a edição da Lei nº 12.737, que o Código Penal foi alterado, onde acrescentou os artigos 154-A e 154-B e modificou o texto dos artigos 266 e 298 para tipificação penal dos crimes informáticos.

A ratificação da Lei nº 12.737/12 que popularmente é conhecida como Lei Carolina Dieckmann, se deu logo após a atriz ter diversas fotos íntimas publicadas por conta de uma invasão em seu computador pessoal, fato que repercutiu nacionalmente.

Já a Lei nº 12.965, conhecida como Marco Civil da Internet, estabelece princípios, garantias, direitos e obrigações para o uso da Internet no País, assim como orientações para o funcionamento da União, o Estados, Distrito Federal e municípios neste tema. Sendo assim, dados e informações particulares que existam em um site ou rede social só podem ser acessados através de ordem judicial.

Com o início da Lei do Marco Civil da Internet, uma das principais inovações está a remoção de conteúdo do ar, a exclusão desses conteúdos se dá através de ordem judicial, exceto casos envolvendo pornografia de vingança, pois as vítimas podem solicitar a remoção do conteúdo diretamente do site ou serviço que contenham o conteúdo.

2.4 Do agravamento aos crimes de violação de dispositivo informático - Lei 14.155/2021

A Lei nº 14.155, de 2021, vem alterar o Código Penal tornando mais duras as penas para invasão de dispositivo, furto e estelionato ocorridos no mundo digital, independentemente de estar conectado ou não em rede de internet.

A lei altera e cria agravantes na redação de alguns artigos do Código Penal que tratam a respeito de crimes informáticos, com aumento a pena de quatro a oito anos, deixando de ser regime de detenção e passando para reclusão, isso aos furtos cometidos por esses dispositivos, independentemente de os dispositivos estarem ligados à Internet, fazer uso de senhas ou até de outro mecanismo de segurança.

Porém, no que diz respeito à identificação, Alves considera que:

> Existe a grande dificuldade de punir os infratores de crimes cibernéticos, levando em consideração o aumento crescente desse tipo de crime em nosso país a, e a falta de leis, tornando-se desse modo um problema jurídico assim como, um grave problema social. (ALVES, 2018, p. 3).

E de acordo com Maia (2017), o marco civil é baseado em três pilares: garantir a neutralidade da rede, proteger a privacidade dos internautas e garantir a liberdade de expressão, por isso o Brasil precisa imediatamente voltar sua atenção para o desenvolvimento de legislação específica sobre crimes cibernéticos, em face de que a Internet se tornou uma parte integrante da nossa vida diária. Assim, é de se almejar a aprovação de um código para nortear todas as relações praticadas no ambiente digital, descrevendo de forma simplificada as condutas para que sejam facilmente incorporadas aos fatos.

3. DA POSSÍVEL DIFICULDADE INVESTIGATIVA NA APURAÇÃO

Devido ao acentuado desenvolvimento da tecnologia da informação, os investigadores enfrentam muitas dificuldades no processo de investigação de crimes cibernéticos. No entanto, apesar de alguns desafios da investigação policial, muitas soluções estão sendo buscadas, como leis específicas e melhor capacitação dos agentes responsáveis pela persecução penal para acompanhar o desenvolvimento contínuo da tecnologia e o advento das novas tecnologias que a acompanham.

Alguns crimes informáticos geralmente são realizados com base na experiência e estratégia de computação. Essas estratégias podem ser elaboradas por grupos de pessoas que geralmente se conhecem. Esses fatores dificultam descobrir quem é o responsável pelo comportamento.

Outra característica de destaque, principalmente em crimes de informática envolvendo fraude ou roubo, é que eles geralmente são executados em vasta rapidez. Em alguns casos a vítima nem percebe que foi atacada, em outros casos ela só percebe quando ocorrem determinados eventos, como quando uma página da *web* é alterada durante o uso, ou quando recebe um *e-mail* de aviso.

Quando tais atos são cometidos na Internet, o caráter punitivo tem dificuldades judiciais na identificação do sujeito, em razão da insuficiência de prova para a composição do crime e de tais crimes serem cometidos em meio virtual.

Hoje, qualquer pessoa com conhecimento técnico mínimo pode praticar atos ilegais por meio de um computador. No entanto, acredita-se que os criminosos desse universo são pessoas inteligentes, gentis e educadas. Além disso, consideram-se operadores competentes de computadores e sistemas, são aventureiros, ousados e buscam superar seus conhecimentos.

Nesse contexto, é importante observar que nem todo cibercriminoso é especialista em informática. Os usuários comuns só precisam saber usar um computador e navegar na Internet para cometer crimes como difamação e pedofilia.

Quando ocorre um crime informático, é necessário proceder a uma investigação de modo a fornecer suporte probatório para futuros processos penais. Os membros da equipe investigativa têm acesso a uma variedade de recursos durante o processo investigativo.

Assim como as pessoas possuem números que as identificam, como CPF (Cadastro de Pessoas Físicas), computadores e periféricos conectados à Internet também são diferenciados por endereços IP. Este número de protocolo é único e permite que as máquinas se comuniquem na rede.

A identificação do número de IP *(Internet Protocol)* traz a possibilidade de localizar criminoso, mas a única maneira de controlar o aumento dos crimes é a lei, devido instituir punição a comportamentos ilegais.

Além das medidas processuais legais para obtenção de provas em crimes cibernéticos, deve haver uma polícia científica bem desenvolvida, com pessoal qualificado e treinado na área de tecnologia da informação e domínio das novas tecnologias. Além do acesso a equipamentos de primeira linha, pois, dada a alta especialização dessas atividades, podem examinar e avaliar os dados coletados.
Mesmo que com o advento da Internet tenha surgido vários benefícios, os novos tipos de crimes evoluíram a tal ponto que o anonimato da rede mundial de computadores contribuiu para a proliferação dessas condutas ilícitas. A implementação da internet levou a um aumento substancial nos tipos de crimes virtuais, passando a obrigar a população e as autoridades a buscarem mecanismos para prevenir o crime e punir criminosos.
A investigação para averiguar a autoria do fato é indispensável para identidade do autor no crime, uma vez que inocentes podem ser culpabilizados em razão de suas contas serem atacadas, por isso a pretensão de punir deve recair a quem realmente praticou o delito, assim é o posicionamento de Tourinho Filho citando Carnelutti:

> O problema da qualificação do acusado é de suma importância, porquanto, em se tratando de qualidade personalíssima, não poderá ser atribuída a outra pessoa que não a verdadeira culpada. Ensina, com autoridade, CARNELUTTI (leccciones, cit., v. 1, p. 195).

Nesse sentido, a Polícia Civil e a Polícia Federal, que são os órgãos da segurança pública responsáveis pela investigação, em especial os setores especializados nesse tipo de crimes, necessitam estarem devidamente equipados para um enfrentamento eficaz e proativo as ameaças cibernéticas. Além de um programa estratégico, e estarem preparados para possíveis problemas análogos ao tema debatido.

4. PROVAS

O Direito tem a função de regular as relações jurídicas entre indivíduos, pois visa tutelar os bens jurídicos dessa relação, sejam bens comuns ou aqueles não habituais.
E quando o assunto são os elementos probatórios, torna-se um dos tópicos mais importantes do processo no ordenamento jurídico, a sua finalidade está para convencimento do juiz da sentença do fato. Nesse sentido completa Norberto Avena:

> Prova é o conjunto de elementos produzidos pelas partes ou determinados pelo juiz visando à formação do convencimento quanto a atos, fatos e circunstâncias. [...] A produção da prova objetiva auxiliar na formação do convencimento do juiz quanto à veracidade das afirmações das partes em juízo. (AVENA, NORBERTO, 2017, p. 315)

Ainda sobre o assunto, Távora e Alencar:

> [...] a prova é tudo aquilo que contribui para a formação do convencimento do magistrado, demonstrando os fatos, atos, ou até mesmo o próprio direito discutido no litígio. Intrínseco no conceito está a sua finalidade, o objetivo, que é a obtenção do convencimento daquele que vai julgar, decidindo a sorte do réu, condenando ou absolvendo. (TÁVORA E ALENCAR, 2017, p.618).

Vale salientar que nos crimes cibernéticos, determinados meios de prova são mais evidentes, como, as perícias que podem ser realizadas no computador manuseado pelo provável autor. Outros possíveis meios prova seriam a interceptação de e-mails, quebra de sigilo das redes sociais como *Telegram, Facebook, Instagram, Whatsapp*, entre outros. No entanto, não podemos dizer que ocorrerá a identificação do suspeito, todavia a identificação torna-se mais provável.
Assim, quando se trata em fazer prova aos crimes cometidos no meio virtual surgem grandes dificuldades, devido ao fato que os delitos cometidos nessa seara não costumam deixar vestígios, e quando deixam na maioria das vezes não é suficiente para enquadrar nos tipos penais existentes que tratam do assunto. É necessário que a conduta seja equivalente

ao que está descrito no tipo penal, e só assim configurará crime levando a punição do autor.
As evidências têm um escopo amplo, pois não apenas comprova o que acontece no ambiente das redes, como fornece suporte para o que acontece em nossa vida cotidiana.
É necessário proteger aqueles que tem a sua privacidade e reputação invadidas por meio de notícias falsas, publicação de conteúdo difamatório, distribuição de imagens não autorizadas etc. O conflito é muito comum no nosso dia a dia, pois cada vez mais pessoas têm acesso aos ambientes virtuais, mais conflitos ocorrem a cada dia, e o número de ações judiciais só aumenta.

CONSIDERAÇÕES FINAIS

A princípio, foi desenvolvido o conceito de cibercrime, onde os temas abordados são esclarecidos a partir de uma compreensão do que é classificado como crime e de um registro de crimes em andamento.
Logo após, aborda-se o questionamento, apresentando a entrada de novas tecnologias trazidas pelo processo de globalização, culminando nos primeiros crimes cometidos no campo digital. No entanto, em um curto período, novos tipos de crimes vêm surgindo, sem lei que os norteiem.
Em se tratando dos tipos de crimes cibernéticos, foram observados os crimes mais comuns nesse ambiente. Além de observadas a importância das provas, bem como a dificuldade em apurar as evidências que possa identificar a autoria. Percebe- se que algumas leis estão surgindo para tratar e dar suporte aos crimes cometidos nos ambientes virtuais, mas não são suficientes, e a fragilidade dessas normas provoca o acúmulo de processos sem resolução. Por isso, a necessidade da elaboração de leis específicas se torna indispensável cada dia mais.

REFERÊNCIAS

ALVES, M. H. dos S. **A evolução dos crimes cibernéticos e ao acompanhamento das leis específicas no Brasil.** Publicado em 2018. Disponível em:https://jus.com.br/artigos/64854/a-evolucao-dos-crimes-ciberneticos-e-o- acompanhamento-das-leis-especificas-no-brasil.

AVENA, Norberto. **Processo Penal.** 9.ª ed. rev. e atual. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2017.

BRASIL. **Código Penal.** Brasília: Site Planalto, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

BRASIL. **Código Processo Penal.** Brasília: Site Planalto, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm.

BRASIL. **Constituição da República Federativa do Brasil.** Promulgada em 05 de outubro de 1988. Brasília: Senado Federal, 1988.

BRASIL. **Lei nº 12.737.** Brasília: Site Planalto, 2012. Disponível: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

BRASIL. **Lei nº 14.155.** Brasília: Site Planalto, 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm

BRASIL. **Marco Civil da Internet.** Brasilia: Site Planalto, 2014. Disponivel em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. **Polícia Federal.** Brasília: Site Polícia Federal. 2022. Disponível em: https://www.gov.br/pf/pt-br.

BRASIL. **Senado Federal.** Brasília: Site Senado Federal. 2022. Disponível em: https://www12.senado.leg.br/hpsenado.

MACHADO, T. J. X. **Cibercrime e o crime no mundo informático.** Universidade Fernando Pessoa. Porto, 2017.

MAIA, T. S. F. **Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro**. Universidade Federal do Ceará. Faculdade de Direito, Curso de Direito, Fortaleza, 2017. Disponível em:http://www.repositorio.ufc.br/bitstream/riufc/31996/1/2017_tcc_tsfmaia.pdf.

RAMOS, E. D. **Crimes cibernéticos:** *análise evolutiva e Legislação penal brasileira.* Curso de Direito da Universidade Federal do Rio de Janeiro. 2017. Disponível em: https://pantheon.ufrj.br/bitstream/11422/6911/1/EDRamos.pdf.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de direito processual penal.** 12ª ed. rev. e atual. Salvador: JusPodivm. 2017.

WEND, Emerson; VINICIUS, Higor; JORGE, Nogueira. **Crimes Cibernéticos:** *Ameaças e procedimento de investigação*. 3ª ed. Rio de Janeiro: Brasport, 2021.