

## **CIBERCRIMINOLOGIA: o crime cibernético e sua responsabilidade civil**

*Bruna Mykaella Botelho Braga*<sup>1</sup>

*Humberto César Machado*<sup>2</sup>

**RESUMO:** A presente pesquisa tem como objetivo apresentar um estudo sobre a cibercriminologia: o crime cibernético e sua responsabilidade civil, ou seja, mostrar mais sobre o mundo virtual e seus perigos, e como a sociedade lida com esses ataques que a cada ano só aumenta. Essa pesquisa busca estudar sobre as leis que defendem os cidadãos, é onde abordaremos se temos uma educação virtual adequada? E Como a legislação está lidando com os crimes cibernéticos em termos de responsabilidade civil? O projeto irá se desenvolver através de estudos bibliográficos. Vale ressaltar que este artigo servirá também como forma de alerta a todos que tem o hábito de ficar na internet.

**PALAVRAS-CHAVE:** Crime cibernético. Virtual. Privacidade. Internet.

### **1 INTRODUÇÃO**

Este presente trabalho irá falar sobre a cibercriminologia: o crime cibernético e sua responsabilidade civil, e alertar os usuários de internet sobre os tipos de crimes que pode lhe acontecer virtualmente, visto que nos últimos anos as pessoas estão gastando cada vez mais o seu tempo no mundo digital, preenchendo talvez algum tipo de estresse causado pelo cotidiano, e assim encontrando uma forma de alívio ali, nesse universo. Visto que esse estresse vem sendo cada vez mais comum na sociedade contemporânea, e isso leva as pessoas a tentar preencher a qualquer custo, sem se quer imaginar o lado obscuro da web, que são os crimes cibernéticos. Não pode se quer ter uma ideia de quão perversa pode ser a mente de um criminoso *hacker*, as habilidades e meios pelo qual uma pessoa pode ser exposta.

---

<sup>1</sup> Acadêmico (a) do curso de Direito do Centro Universitário Alfredo Nasser. E-mail: bruna.mbbbraga@gmail.com.

<sup>2</sup> Pós-Doutor em Psicologia pela Pontifícia Universidade Católica de Goiás – PUC-GO (2016); Doutor em Psicologia pela PUC-GO (2013); Mestre em Psicologia pela PUC-GO (2006); Especialista em História pela Universidade Federal de Goiás - UFG (2002); Graduado em Filosofia pela UFG (1996); Graduado em Pedagogia pela ISCECAP (2018); Elemento Credenciado Fatores Humanos e Prevenção de Acidentes Aéreos pelo CENIPA (Centro de Investigação e Prevenção de Acidentes Aeronáuticos); Professor Coreógrafo e Dançarino de Salão; Professor da PUC-GO; Membro do Comitê de Ética e Pesquisa, Professor do Centro Universitário Alfredo Nasser – UNIFAN e orientador da pesquisa. E-mail: humberto.cesar@unifan.edu.br.

Nos tempos atuais o crime virtual não é mais sobre aquele cara *hacker* que invadia um sistema cheio de segurança, a invasão cibernética hoje é aquele crime que acontece com tudo mundo de maneiras diferentes, e que vai levar a ter investigações distintas para este dispositivos informáticos. E a forma como o Estado responsabiliza esse tipo de ação conscientiza muito a todos sobre futuros delitos, pois o que pode ser observado nos dias atuais em relação a esses ataques, e que a vítima está sendo lesada, mas não restituída, já que na maioria das vezes tem que se processar os autores na vara civil para ter de volta aquele valor ou bens que foram furtados.

## **2 METODOLOGIA**

A metodologia usada neste trabalho acadêmico, ou seja, o caminho percorrido para o entendimento dos objetivos desse projeto, baseiam-se em pesquisas bibliográficas relacionadas ao tema, leituras de livros e de artigos científicos que abordam temas similares para um melhor desenvolvimento desse projeto.

## **3 DISCUSSÕES, RESULTADOS E/OU ANÁLISE DE DADOS**

A tecnologia, sem dúvida, foi uma das maiores evoluções que se teve nos últimos tempos, antes o único modo de comunicação rápida era através de telefonemas, no Brasil à internet surge em 1988, desde então, os números de provedores desse serviço e de usuários que o utilizam aumentam a cada ano. Hoje em dia você pode pagar uma contar por um aplicativo do banco que pode ser instalado por você mesmo, sem ter o incômodo de se locomover até a uma lotérica, e enfrentar uma fila para pagar um boleto, poupando assim uma grande parte do seu dia, ou até mesmo um envio de um documento importante, que você simplesmente tirar uma foto e envia diretamente para a pessoa, e ela recebe na mesma hora.

Porém todo esse benéfico da facilidade, trouxe também consigo a vulnerabilidade de ser exposto a um criminoso, que pode estar acompanhando o dia a dia de sua vítima, e fazendo tudo isso do sofá de casa. Essa prática delitativa é diferente nesse sentido, pois um criminoso não precisa te abordar na rua e lhe apontar uma arma para roubar suas informações mais preciosas, ele pode fazer isso de casa, com uma facilidade absurda e sem a menor chance de uma presa se defender. Os usuários da internet se isolam do resto do mundo conforme o

tempo se passa, e ali acaba depositando uma confiança que não deveria, tendo uma falsa sensação de segurança, e compartilhando uma série de informações como: fotos, endereços, dados pessoais, e às vezes acaba expondo até uma outra pessoa ao perigo, ao divulgar seu dia a dia e automaticamente mostrando pessoas do seu convívio social.

A princípio a internet tinha como objetivo facilitar a entrega de dados importantes, mais utilizadas para trabalho, como envio de e-mails de um lugar para outro, porém como nada permanecer igual por muito o mundo virtual que era usado antes só como uma ferramenta de trabalho foi sendo usado para outros fins, as redes sociais, e assim conseguindo um novo público, as crianças e os jovens. Eles que antes brincavam no quintal de casa começou a não querer sair mais do quarto, e sem nenhuma educação previa sobre esse mundo cibernético, acessando de forma desenfreada. E acaba tendo muitas informações disponíveis que na maioria das vezes não sabe se são de fato verdadeiras, mas só por estar na *web* se confia de olhos fechado, e aí que o lado obscuro da internet entra, jogando rios de informações cibernéticas falsas, que induz o ser humano ao erro, e ao clicar em apenas um *link* você perde tudo.

E com o aumento dos crimes virtuais, temos cada vez mais denúncias sendo levadas ao judiciário, isso pode acarretar em um grande congestionamento financeiro para a economia publica, gerando mais demandas policiais, e isso tudo tem um preço muito alto, inclusive para o consumidor e os bancos em casos de furtos de dados bancários, no qual o consumidor perde dinheiro com o golpe, e ainda tem que os advogados para recuperar seus bens matérias, já as instituições financeiras sofrem também financeiramente por ter que ressarcir as vítimas que acessarão sites enganosos e passarão dados bancários para os criminosos, que seria de responsabilidade dos próprios bancos não ter réplicas de sites fraudulentos com o nome de instituições financeiras na internet. Para se ter uma ideia, um crime virtual para ser oferecido a denúncia precisa ter uma materialidade que justifique a ação penal, não basta apenas saber quem foi o autor, precisa de uma série de provas que comprovem a materialidade, porque precisa se ter elementos para condenação, é nesse momento que a vítima se sente devastada, e injustiçada com as leis. E aqui que Estado tem que conscientizar a sociedade que esse tipo de crime não tem rosto ou um gênero específico, esse tipo de golpe pode ser praticado por qualquer pessoa.

Por se tratar de um crime virtual a grande maioria das pessoas acha que quem o pratica está sempre em casa, trancado no quarto em frente a um computador o dia todo vestindo um moletom com capuz, e não é assim, muito se engana quem pensa isso, este delito não tem rosto, para cada tipo de crime tecnológico temos rostos diferentes, e com intenções

diferentes, quem pode estar por trás de um ataque cibernético pode ser um namorado que está ameaçando de postar fotos íntimas da sua namora, até um estelionatário profissional, percebe-se que não tem um estilo específico para se cometer este crime. E como Ivette Senise Ferreira (2001, p. 208) infere que: As várias possibilidades de ação criminosa na área informática, assim entendida em seu sentido lato, abrangendo todas as tecnologias da informação, do processamento e da transmissão de dados, originaram uma forma de criminalidade que, apesar da diversidade de suas classificações.

#### **4 CONSIDERAÇÕES FINAIS**

O crime cibernético e a mesma coisa que crime virtual, crime da internet, crimes eletrônicos, quando se fala em dispositivos informáticos se entende que tudo que você consegue conecta a um dispositivo de dados. Um ataque desse tipo pode ser feito estando seu aparelho conectado ou não a uma rede. A internet nos tempos de hoje tem uma influência muito grande sobre as pessoas, pode-se ser praticados inúmeros crimes pelo meio virtual, temos de furto de dados desde *bullying* virtual, até a pornografia infantil. O que dificulta hoje uma denúncia a se levada a sério no meio judiciário e o fato da comprovação mínima a ser exigida, não basta o ofendido saber quem foi o autor, precisa-se ter comprovações concretas de que o autor praticou o crime.

Hoje tem delegacias no país que tratam desse assunto, mais na sua maioria não estão capacitadas para esse tipo de crime, por não se encontra o criminoso de imediato através do endereço de IP usado para o delito, não se aprofunda uma investigação, deixando assim as presas vulneráveis a outro ataque virtual, que sempre causam danos a honra e quase sempre danos materiais, pois além do alvo estar sofrendo pelo ataque, ele ainda tem que entrar com um processo judicial para conseguir restituir a coisa lesada, também temos os bancos que acabam sendo responsabilizados civilmente pelo uso de nome da instituição financeira para o fim de enganar a vítima e induzi-la a depositar uma quantia de dinheiro ou a pagar alguma conta, e assim os bancos acabam tendo que acionar o judiciário da empresa e também sendo lesados financeiramente.

As leis contra crimes digitais são leves, ainda mais pelo uso cada vez maior de pessoas que acessam a internet, e de dados que são compartilhados, e que podem estar sendo usados para fins ilícitos, o mundo cibernético trouxe uma grande facilidade de vida para todos, no âmbito profissional e no pessoal, o problema é que esse mundo também é usado para cometer

crimes, como: golpes, furtos de dados, *cyberbullying*, difamação, tudo isso através de uma invasão de servidores que podem está sendo usados por qualquer lugar do mundo, e é isso que traz aquela falsa sensação de que o criminoso nunca vai ser punido, o governo não investe tanto quanto deveria investir na segurança virtual, e assim deixando enfraquecida a responsabilidade que o autor faz na vida do seu alvo.

Em algumas situações, a própria vítima acaba sendo responsabilizada por algo que não fez, visto que no crime virtual é tudo feito através de confirmações que partem do dispositivo da pessoa, o que dificulta a materialidade do crime, em razão de tudo que está sendo cometido pelo criminoso ficará registrado em nome do titular da conta, e tudo isso talvez pudesse ter sido evitado se já houvesse uma educação virtual sobre o que pode acontecer com qualquer no ciberespaço. Sempre que se vê na mídia algo sobre condenação de algum ato que envolve crimes digitais, o responsável só é penalizado no âmbito penal, enquanto no âmbito civil se nota uma negligência com a vítima, já que para recuperar o dano material e moral, na maioria das vezes a mesma tem que pagar advogados para ter seus direitos validados, e assim gastando mais tempo e dinheiro.

## REFERÊNCIAS

AUMENTO do uso da internet faz crescer o número de crimes cibernéticos. **Jornal Opção**, 2022. Disponível em: <https://www.jornalopcao.com.br/ultimas-noticias/aumento-do-uso-da-internet-faz-crescer-o-numero-de-crimes-ciberneticos-374687/-2022>. Acesso em: 14 ago. 2022.

BARBOSA, Mateus Israel Alves Crivinel. **Crimes virtuais**: a evolução dos crimes cibernéticos no combate. 25 nov. 2020. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/105>. Acesso em: 14 ago. 2022.

CRUZ, Bianca Beatriz Barbosa da; FIGUEREIDO, Cristiano Lázaro Fiúza. **Crime cibernético**: a pornografia de vingança como violência de gênero contra a mulher e a prática de divulgação disciplinada na lei 13.718/18. 16 dez. 2020. Disponível em: <http://ri.ucs.br:8080/jspui/handle/prefix/2808>. Acesso em: 14 ago. 2022.

FERREIRA, Aurélio Buarque de Holanda. **Dicionário da língua portuguesa**. Rio de Janeiro: Nova Fronteira, 2001.

FRANÇA, Marlene Helena. A responsabilidade civil e criminal na internet: o papel do judiciário brasileiro. **Revista Quaestio Iuris**, [S.l.], v. 13, n. 1, p. 480-507, jun. 2020. ISSN 1516-0351. DOI: <https://doi.org/10.12957/rqi.2020.41943>. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/41943>. Acesso em: 31 ago. 2022.

OLIVERIA, Geovana Xavier de. **Crimes cibernéticos**: direito digital e os novos paradigmas da investigação criminal. 21 maio 2020. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/4132>. Acesso em: 15 ago. 2022.

PEREIRA, Kamille da Silva; OLIVEIRA, Fábio Machado de. Perícia forense computacional e crimes cibernéticos. **Revista Interdisciplinar Pensamento Científico**, v. 5, n. 2, jul.-dez. 2019. Disponível em: <http://reinpeconline.com.br/index.php/reinpec/article/view/292>. Acesso em: 16 ago. 2022.

SODRÉ, Ludmilla Gonçalo da Silva. **As dificuldades na colheita de elementos de autoria e materialidade delitiva dos Crimes Cibernéticos**. Orientador: Danilo Rinaldi dos Santos Junior. 21f. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Centro Universitário do Planalto Central Aparecido dos Santos, Gama – DF, 2021.