CRIMES CIBERNÉTICOS

Gabriela de Jesus, Bazilio de Alvarenga Coutinho Junior, e-mail: gabrieladejesus142@gmail.com

1 INTRODUÇÃO

Num mundo cada vez mais globalizado, as relações interpessoais têm se tornado cada vez mais acentuadas. Muito dessa nova realidade se deve, sobretudo, ao avanço tecnológico, principalmente no meio informático. Contribuindo assim com a propagação dos crimes cibernéticos, também conhecidos como crimes eletrônicos ou digitais, referem-se a atividades ilegais que são realizadas por meio de dispositivos eletrônicos e redes de computadores conectados com a rede mundial de internet para a prática de ações criminosas, que geram danos à pessoas e patrimônios. O impacto desses pode ser profundo, acarretando principalmente danos financeiros, mas também perda de confiança, estresse emocional e danos à reputação de vítimas expostas na Internet.

Se considerarmos que só no Brasil, mais de 81% da população acima de 10 anos têm acesso à rede. Só aqui, mais de 152 milhões de pessoa tem a facilidade de se conectar com a sociedade, entretanto, estão sujeitas a sofrerem com os cibercrimes, a alemã Roland Berger levantou estatísticas, e nelas apontam que o Brasil foi o 5° país no mundo que mais sofreu com crimes cibernéticos em 2021, esse ranking registrou cerca de 9,1 milhões de ataques, segundo a consultoria de Berger.

O objeto de estudo deste trabalho serão os Crimes Cibernéticos e suas considerações, bem como as novidades legislativas aqui no Brasil relacionadas a esse tema. Abordaremos as noções gerais desse tipo de crime, sua evolução em nosso país e também analisaremos como nossas leis estão lidando com essa onda de crimes virtuais.

Tais questões são relevantes para toda a sociedade, pois nos dias atuais a tecnologia está cada vez mais presente em nossas casas, em nossas famílias. O objeto deste estudo contribuirá para compreendermos e conhecermos essa prática criminosa, que está em constante evolução para prejudicar os usuários da rede. Por isso, vamos estudar esse mundo virtual para buscarmos uma solução possível para os crimes que vêm se

expandindo. Nosso estudo desenvolveu-se com base na população que faz o uso da internet aqui no Brasil.

2 MÉTODO

A metodologia utilizada para a realização do estudo será pelo método Pesquisa Bibliográfica. Ela foi construída por meio de leituras de leis da Constituição Federal, de obras doutrinárias, e de artigos científicos relacionados ao tema retratado.

A pesquisa foi elaborada através de buscas em base de dados, teve como fonte: Scielo; Google, dentre outros. O nosso ínterim de pesquisa foi entre os meses de Julho e Agosto de 2023

3 RESULTADOS E DISCUSSÃO

3.1 Noções gerais sobre cibercriminalidade

A primeira rede acadêmica brasileira, estabelecida em 1992, operava a uma velocidade de 64 Kb/s. Naquela época, era possível trocar mensagens de texto, enviar e-mails, realizar transferências de arquivos (com um pouco de paciência) e acessar sites relativamente simples. A abertura da internet para uso comercial ocorreu em maio de 1995, três anos depois. Com o passar do tempo, a rede evoluiu consideravelmente, permitindo um desempenho cada vez mais eficiente. No entanto, à medida que a internet passou a ser amplamente utilizada em diversas atividades, ressurgiu a preocupação genuína e familiar com a segurança das informações compartilhadas online. Essa preocupação não se restringia apenas aos governos, mas a todos os usuários que faziam uso da rede.

Certo é que, tal qual ocorre com a internet, essa evolução rápida e constante também acabam sendo um meio para fazer com que a criminalidade também evolua e consequentemente acaba dificultando o combate a esses crimes. Assim, aqueles indivíduos que possuem grande capacidade de utilizar a internet, são conhecidos como hackers e esses acabam usando esses conhecimentos para cometer crimes na internet, acreditando que estão impunes pelo fato de estarem acobertados pela dificuldade

de se buscar as pessoas e as origens das pessoas que estão atrás dos computadores (Jesus e Milagre, 2016).

Essas pessoas passaram a ser chamadas de hackers, um termo contemporâneo para indivíduos que sempre estiveram presentes na sociedade. Originado do inglês, o termo é empregado para descrever programadores altamente habilidosos e perspicazes. São pessoas que discretamente obtêm informações de sistemas informáticos pertencentes a outras pessoas, empresas, entidades governamentais e qualquer coisa ligada à internet. Essa obtenção de informações pode ter diversos objetivos, como visualização, utilização ou compartilhamento.

No Brasil há registro de que uma das primeiras ações de hackers no país foi a destruição de programas de computador da EMBRAPA (Empresa Brasileira de Agropecuária), causando diversos prejuízos (Jusbrasil 2016).

Outro caso emblemático ocorreu com o Hospital do Câncer de Barretos que teve seus computadores hackeados, impossibilitando assim o acesso a ficha de pacientes gerando uma série de transtornos para os doentes. Os hackers solicitaram um “resgate” para a devolução do acesso aos arquivos, valor esse que girava em torno de R$ 1.000,00 (mil reais) por computador e que deveriam ser pagos mediante “bitcoins” que são moedas digitais de difícil rastreabilidade.

Situação semelhante tem ocorrido em outros países em que os Hackers estão roubando os dados sensíveis de determinadas nações e em troca da devolução do acesso a tais dados os hackers têm pedido resgates milionários a essas nações.

Portanto vemos que o que difere os crimes comuns para dos cibercrimes não é a alteração da conduta típica, mas sim o meio empregado pelo criminoso para praticar a conduta ilícita, que, como vimos, é realizada na rede mundial de computadores.

3.2 Como estão nossas leis frente a essa onda de crimes virtuais. a lei mais rígida é aprovada e sancionada

O crime virtual deve ser analisado sob diferentes perspectivas por conta de suas peculiaridades comparando com o “crime real” que tem local precisado e mais fácil ação

pelas autoridades coatoras, o crime virtual dispensa o contato físico entre vítima e agressor, ocorrendo em um ambiente sem povo, governo ou território, além de não gerar, a princípio, sensação de violência para um segmento social específico não havendo padrões para o seu acontecimento (Sydow, 2009).

Nesse caso, podemos citar o caso da famosa Lei nº. 12.737/2012 conhecida como a Lei Carolina Dieckmann. Essa lei se deu em grande parte pelo fato da renomada atriz de televisão ter as suas fotos íntimas hackeadas e expostas por toda a rede sem a sua prévia autorização, fazendo com que o Congresso se atentasse para a dimensão do caso e na ocorrência do aumento de outros crimes digitais estarem ocorrendo.

Ela recebe este nome devido ao caso ocorrido com a atriz Carolina Dieckmann, que sofreu uma invasão de privacidade na qual um hacker não-ético, em maio de 2011, invadiu o computador pessoal da atriz. Ele conseguiu acesso a cerca de 36 fotos pessoais nas quais a atriz aparecia nua. A atriz prestou queixa para a Polícia, que verificou que a caixa de e-mail de Carolina Dieckmann havia sido violada pelo hacker.

De acordo com a denúncia, o criminoso pediu cerca de R$10 mil para que as fotos não fossem publicadas, porém, como a atriz recusou a exigência, elas foram divulgadas na Internet. Devido a esse acontecido, gerou-se uma enorme discussão sobre a situação em si, demandando que houvesse a criminalização sobre esse tipo de prática. Na época do crime o Brasil ainda não possuía lei específica para crimes de informática. E a justiça se baseou no código Penal Brasileiro, para resolver o caso que estava acontecendo, onde os envolvidos foram indiciados por furto, extorsão qualificada e difamação.

Soma-se a isso a Lei nº 14.155/2021 que tornou mais grave os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. Na presente lei que alterou o art. 154-A do Código Penal, prevê a penalidade de um ano a 4 anos, e multa nas situações em que se configura invasão de dispositivo informático (incluindo tablets, notebooks, entre outros) alheio, conectado ou não à Internet. Tal invasão deve servir como objetivo de obter, alterar, ou inviabilizar dados ou informações dou dono, sem sua expressa autorização.

Se tornou necessária a criação de uma norma que tratasse deste assunto devido ao avanço tecnológico e a democratização e acesso facilitado às redes sociais. Assim, a lei tipifica crimes cometidos nesse ambiente a fim de aplicar penas e punições para os que cometerem esses delitos.

Desta forma, o que se verifica com a entrada dessa norma no regimento jurídico brasileiro é buscar uma penalização para aqueles que utilizam os meios digitais com a finalidade de obter informações e imagens sigilosas de terceiros sem a devida autorização.

4 CONSIDERAÇÕES FINAIS

Concluindo, os crimes cibernéticos representam uma ameaça cada vez mais grave em nosso mundo digitalmente conectado. Para enfrentar esse desafio, é essencial que governos, empresas e indivíduos colaborem na implementação de medidas de segurança robustas, conscientização e educação sobre práticas online seguras.

Além disso, a aplicação eficaz das leis cibernéticas e da cooperação internacional são cruciais para dissuadir e punir os perpetradores. A rápida evolução do cenário tecnológico exige uma abordagem contínua e adaptável para combater esses crimes e proteger nossos dados, privacidade e infraestruturas digitais.

REFERÊNCIAS

BAPTISTA, Rodrigo. **Lei com penas mais duras contra crimes cibernéticos é sancionada.** Agência Senado. 28/05/2021. Disponível em: https://www.jornaljurid.com.br/blog/auxilium/quais-sao-as-leis-que-protegem-seus-dados-de-crimes-virtuais-no-ramo-juridico#:~:text=Este%20%C3%A9%20a%20Lei%20dos,sites%2C%20sejam%20governamentais%20ou%20n%C3%A3o. Acesso em: Julho de 2023.

BERGER, Roland. **Ranking de vulnerabilidade de cibercrimes.** 16/11/2022. Disponível em: https://blog.algartelecom.com.br/tecnologia/crimes-ciberneticos/. Acesso em: Julho de 2023.

BRASIL. **Lei nº 13.737 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: Agosto de 2023.

BRIZOLA, Fernando. Advocacia Direito Digital e Crimes Cibernéticos. **Primeiros casos interessantes de crimes na internet.** Disponível em: https://www.jusbrasil.com.br/artigos/primeiros-casos-interessantes-de-crimes-na-internet/393077456 Acesso em: Agosto de 2023.

CAPEZ, Fernando Prado. **Código Penal Comentado**. São Paulo: Saraiva, 2016.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais.** São Paulo: Saraiva. 2011.

Evolução da internet no Brasil. Disponível em: https://www.rnp.br/noticias/evolucao-da-internet-no-brasil#:~:text=A%20primeira%20rede%20acad%C3%AAmica%20brasileira,depois%2C%20em%20maio%20de%201995. Acesso em: Agosto de 2023.

JESUS, Damásio de. Milagre, José Antônio. **Manual de Crimes de Informáticos.** São Paulo: Saraiva, 2016.

Lei com penas mais duras contra crimes cibernéticos é sancionada — Senado Notícias. Disponível em:https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada Acesso em: Julho de 2023

OLIVEIRA JUNIOR, Eudes Quintino de. **A nova lei Carolina Dieckmann.** 2012. Disponível em:https://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann Acesso em: Agosto de 2023

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática.** 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. Acesso em: agosto 2023.