REVISTA DA ANINTER-SH
Volume 1, 2024 – Artigo: 11
ISSN: 2965-954X
Received: 07/12/2023
Accepted: 02/04/2024
D.O.I. http://dx.doi.org/10.69817/2965-954X/v1a11

A CRIMINALIDADE E AS NOVAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

CRIMINALITY AND THE NEW INFORMATION AND COMMUNICATION TECHNOLOGIES

Lidiane Medeiros de Souza
Graduanda do Curso de Direito da FAMESC - Faculdade Metropolitana São Carlos, Bom Jesus do Itabapoana, RJ, 2023.
lidi–bjn@hotmail.com

Mariana Verinesi Vieira Medeiros
Mestranda do Programa de Pós-Graduação em Segurança Pública, Universidade de Vila Velha, UVV.
maari.veronesi@gmail.com

Fabio Machado de Oliveira
Doutor em Cognição e Linguagem, professor do Pós-Graduação em Segurança Pública, Universidade de Vila Velha, UVV.
fabiomac@gmail.com

RESUMO
Este trabalho, baseado exclusivamente em técnicas de pesquisas bibliográficas e eletrônicas, trata de dissertar sobre os crimes cibernéticos especialmente no Brasil, mas ao final relata o caso de Lucas Michael Chansler, que foi contado em 2014 pelo agente do FBI encarregado da investigação, Larry Meyer, no Discovery ID, e na mídia para posterior conhecimento das vítimas que ainda não sabem da prisão do criminoso. O crime é relatado não só para acrescentar exemplo ao trabalho, mas também para divulgar e ser visto por pessoas que possam identificar alguma das vítimas em algum momento e servir de utilidade pública. Iniciado com a definição de crimes virtuais, conhecimento do assunto no Brasil e de como são investigados, o crescimento destes nas redes de sociais, o papel do investigador, e as questões legais envolvidas.

Palavras Chave: crimes cibernéticos, criminalidade, tecnologia.

ABSTRACT
This work, based exclusively on bibliographic and electronic research techniques, deals with cybercrime especially in Brazil, but at the end it reports the case of Lucas Michael Chansler, who was told in 2014 by the FBI agent in charge of the investigation, Larry Meyer, on Discovery ID, and in the media for later awareness of victims who still don't know about the criminal's arrest. The crime is reported not only to add an example to the work, but also to publicize it and be seen by people who can identify one of the victims at some point and serve a public

utility.Started with the definition of virtual crimes, knowledge of the subject in Brazil and how they are investigated, their growth in social networks, the role of the investigator, and the legal issues involved.

Keywords: cyber-crimes, criminality, technology.

1. INTRODUÇÃO

Levando em conta a velocidade com a qual evolui a sociedade e a internet nas últimas décadas, as tecnologias para averiguar e punir os crimes do ambiente virtual também evoluíram, dado a necessidade urgente de elucida-los, em defesa do direito e da segurança do indivíduo.

A falsa impressão de que é difícil punir quem comete estes crimes é falsa, pois a legislação nacional e internacional é incansável na criação de leis que possam elucidar esta modalidade de crime, adaptando-se a essa nova realidade.

Nosso trabalho reporta-se a elucidar e compreender alguns aspectos dessa relação de trabalho de investigação, em questões de direito, que tanto impacta na vida das pessoas devido ao processo de globalização que interconecta indivíduos de várias nacionalidades, contextos sociais e econômicos.

Usamos fundamentalmente a metodologia de pesquisa bibliográfica, descritiva, quantitativa e qualitativa e também dos meios eletrônicos, inspirados nas obras dos autores pesquisados.

Nosso objetivo com essa pesquisa, é explorar os tipos de crimes virtuais, o avanço destes no Brasil, e as leis específicas criadas para solucionar e defender os direitos das vítimas destes.

Nosso país possui uma grande concentração de crimes na internet[1] também chamados de crimes cibernéticos. Somos diariamente vítimas de fraudes e malware no sistema bancário, em redes sociais, sites de compras na internet, etc. A velocidade com que se realiza a perícia destes crimes não é proporcional ao avanço dos mesmos. Sendo assim, temos uma grande quantidade de profissionais que não estão preparados para combater este tipo de violação aos direitos e privacidade de nossa população cibernética.

É preciso conhecer os tipos de crimes cibernéticos cometidos, a legislação específica no combate aos mesmos, para se preparar ferramentas e profissionais competentes, necessários e eficazes, ao seu combate.

Necessitamos de muita parceria e troca de experiências que contribuam no entendimento deste espaço ainda tão pouco conhecido.

[1] https://stats.cert.br/

É nessa descoberta e reflexão que encontraremos possibilidades e recursos tecnológicos que sugiram possíveis e urgentes soluções.

A ciência da investigação terá um trabalho minucioso e árduo na solução destes que ora parecem insolúveis.

2. DESENVOLVIMENTO

2.1. DEFINIÇÃO DE CRIMES VIRTUAIS E TIPOS MAIS COMUNS

Os crimes cibernéticos são todos aqueles cometidos através de computadores conectados à internet e tiveram origem nos Estados Unidos a partir de 1960, pautados em crimes de espionagem e afins.

No Brasil os mais praticados são os relacionados a perfis falsos nas redes sociais, calúnia, difamação ou injúria, estelionato, apologia ao crime, furto de dados pessoais de usuários incautos, divulgação de fotos íntimas das pessoas, plágio, pedofilia, etc.

Em geral, esses crimes são punidos com reclusão de um a quatro anos de prisão além de multa. A pena é aumentada de um ou dois terços se a vítima for prejudicada financeiramente.

A primeira lei criada no Brasil para combater os crimes cibernéticos foi a Lei dos Crimes Cibernéticos ou Lei Carolina Dickmann de nº 12 737. Em 2021 foi aprovada uma mais recente, pelo Senado Federal que é a Lei 14 155. A intenção é tratar com mais rigor estes crimes que segundo os especialistas aumentam consideravelmente devido ao uso e à evolução das tecnologias.

O combate aos crimes cibernéticos, assim como a qualquer crime, é feito com a prevenção, ou seja, cuidados das pessoas no uso da internet, preservando seus dados pessoais, não se relacionando com pessoas desconhecidas através das redes sociais, monitorando o uso de internet pelos filhos, etc.

As medidas de prevenção são importantes, pois dificultam a ação dos criminosos, não só nos crimes virtuais como em qualquer outro tipo de crime.

A respeito de crimes cibernéticos Almeida e Oliveira (2022) acreditam que a prática criminosa aumenta porque o uso da internet também aumentou. No artigo intitulado “Crimes Virtuais: o Avanço dos Crimes Eletrônicos e a Evolução das Leis Específicas no Brasil” afirmam:

> “Acredita-se que o aumento da prática criminosa virtual esteja diretamente relacionado ao aumento do uso da Internet pelas pessoas. Portanto, é fundamental para o bom desenvolvimento da “sociedade digital” compensar os prejuízos causados por esses criminosos. Para que essa ideia se torne realidade, leis mais rígidas devem estar em vigor. É necessária uma regulação efetiva do crime virtual, levando-nos a refletir sobre as medidas de contingência que podem tornar a sociedade mais segura. Não há dúvida de que a Internet é uma das maiores invenções do século XX. Desde o seu

> surgimento, abriu as portas para o desenvolvimento de novas tecnologias, e essas evoluções continuam até os dias de hoje, mudando nossas vidas e a forma como interagimos. Esse crescimento tecnológico, no entanto, além de proporcionar diversos benefícios, também facilitou a prática de delitos. Os chamados crimes virtuais, ou crimes cibernéticos. Durante o enfrentamento da pandemia pela COVID-19, os ataques cibernéticos se tornaram constantes. O Brasil está no epicentro de uma onda global de crime cibernético, ou cibercrime. O país é uma das maiores vítimas das fraudes bancárias online e de malware financeiro, e o problema continua a se agravar. O número de ataques cibernéticos no país e as fraudes bancárias online cresceram muito ao longo dos últimos anos Todavia, grande parte da população brasileira ainda ignora a escala do problema". (ALMEIDA, 2023, p.2).

Rebeca Assis cita sete crimes virtuais como os que mais acontecem na atualidade (os mais comuns): plágio, furto de dados, calúnia, difamação e injúria, incitação e apologia ao crime, racismo, homofobia, misoginia (ódio ou aversão às mulheres), pirataria digital, divulgação de fotos íntimas, criação de perfil falso, etc.

Lazzarini, em seu trabalho de final de curso, (bacharelado em direito na Universidade de Mackenzie em 2020) observa sobre a ausência ou carência de leis para punir os crimes virtuais, fazendo uma análise dos crimes virtuais anda cita a pornografia infantil, pedofilia.

De maneira geral os autores que pesquisamos são unânimes em alguns aspectos deste tema: o aumento dos crimes virtuais nas últimas décadas, a falta de legislação adequada para investigação e punição, a falta de orientação dos internautas quanto aos cuidados que devem tomar para se prevenirem destes crimes, e criatividade dos criminosos cada vez mais aguçada, no sentido de alcançar seus objetivos, ou seja, prejudicar de alguma forma os incautos.

Sobre a legislação já existente, vale observar a análise que Varela em 2019 bem soube realizar em seu trabalho científico "Crimes Virtuais e a Legislação Brasileira". Citamos algumas abaixo:

- ✓ Decreto-Lei Nº 2.284 de 1940 (Código Penal)
- ✓ Lei nº 11.829 de 2008
- ✓ Projeto de Lei do Senado n° 236, de 2012.
- ✓ Lei nº 12735 de 2012
- ✓ Lei 12.737 de 2012
- ✓ PL 7758/2014
- ✓ Lei nº 12965 de 2014
- ✓ PL 6989/2017 apensado ao PL 8833/2017
- ✓ Lei nº 13.772 de 2018

Vale ressaltar que seu trabalho é um pouco mais extenso. Aqui relacionamos as leis e decretos que julgamos mais relacionados ao tema pesquisado.

3. O EXPRESSIVO CRESCIMENTO DOS CRIMES VIRTUAIS NO BRASIL

O país que mais sofreu com crimes virtuais do tipo ransomware[2] na primeira metade do ano de 2021 com mais de nove milhões de casos foi o Brasil, colocando-se em 5º lugar no mundo. O relatório foi divulgado em vinte e nove de julho de 2021 pela SonicWall. São mais de 300 milhões deste tipo no mundo nos primeiros meses deste ano. Na frente do Brasil estão Estados Unidos, Reino Unido, Alemanha e África do Sul.

Podemos citar aqui três tipos de ataques cibernéticos:

Ryuk - tem poder de infectar todos os arquivos do sistema fazendo com que se tornem inacessíveis.

Cerber - capaz de crioptografar (converter) os dados dos arquivos para torná-los reféns e pedir resgate dos mesmos.

SamSam – tem poder de controlar o sistema explorando sua vulnerabilidade.

As áreas mais atingidas no Brasil por estes ataques virtuais foram instituições governamentais, na área de educação e saúde com violações de segurança e cujos ataques ultrapassaram no ano de 2021 mais de 500% de todo volume do ano anterior nestes setores.

A pandemia fragilizou estes usuários aumentando a procura por seguros para indenizar pelos prejuízos e riscos causados e também para preveni-los dos mesmo.

As seguradoras se mobilizaram na busca de soluções para proteger as empresas públicas e privadas destes crimes.

O Brasil foi o 2º país no ranking de ataques cibernéticos em 2022 com mais de 100 bilhões de tentativas e com aumento de quase 17% em relação ao ano anterior. O país que liderou o ranking neste ano foi o México com quase 188 bilhões no mesmo ano.

O assunto está em categoria de urgência em todas as empresas de seguro pela rapidez com que evoluem e causam prejuízos financeiros de ordem considerável. Foram mais de 60 milhões de indenizações pagas no ano de 2022 causando impacto negativo nas finanças das seguradoras.

3.1. UM CRIME CIBERNÉTICO DE REPERCUSSÃO MUNDIAL - Red de mentiras - Lucas Michael Chansler

Na cidade de Jacksonville, Florida, em 2010 foi preso e condenado por extorsão sexual na internet, um jovem de 31 anos chamado Lucas Michael Chansler. Foram aproximadamente três anos de atuação, a partir de 2007 em três países: Estados Unidos, Canadá e Reino Unido. Depois de fazer mais de 300 vítimas foi condenado a 105 anos de prisão. Ele se conectava com as jovens de idade entre 12 e 16 anos de idade na maioria, com um perfil falso nas redes sociais. Fazia amizade com elas, e depois de conquistá-las com frases

[2] Usuários que utilizam malware para criptografar os dados e arquivos das vítimas.

galanteadoras, pedia que mostrassem os seis. As garotas achavam divertido e cediam à vontade dele. Mas logo depois ela as chantageava, dizendo que mostraria para todos os seus contatos e amigos se elas não fizessem tido que ele mandasse.

O FBI divulgou nomes endereços sociais e eletrônicos das vítimas encontrados nos arquivos pessoais do criminoso, para que a noticia de sua prisão chegasse até elas. Ele usava vários perfis falsos (cerca de 135) para se comunicar com as meninas. Todos foram divulgados pelo FBI dentro os quais: CaptainObvious, sk8er4life2021, victorhugo, nas redes sociais extintas

MySpace e Stickam.

Foi denunciado por uma das vítimas e pela mãe dela, mas até hoje o FBI procura mais vítimas, para informar que ele foi preso e que elas não precisam mais temê-lo.

Três delas denunciaram e se expuseram para tal finalidade. Samantha Chonski, de 26 anos foi uma delas. Ela o conheceu na plataforma Stickam com perfil CaptainObvious. Era amável, até ela ceder a um capricho dele de mostrar os seios. Aí ela descobre que ele conhecia todos os seus amigos, família, sabia onde ela morava e estudava. Daí em diante a vida dela virou um inferno. Ele a chantageou de todas as formas com pedidos de fotos e vídeos de origem sexual.

A mãe de uma das meninas, Ângela Reynolds descobre ao investigar o comportamento estranho da filha. Ela examina o laptop da filha e vê escandalizada as imagens que ela era obrigada a fazer para ele. Ainda relutou em denunciar porque a filha temia a divulgação das imagens e tinha vergonha. Mas com o passar do tempo foram obrigadas a ligar para o Centro Nacional para Crianças Desaparecidas e Exploradas (NCMEC).

O caso foi gravado e relatado sob o título de Rede de Mentiras, pelo agente especial Larry Meyer, encarregado da investigação, em um vídeo da campanha lançada na página do FBI. Essa campanha visa encontrar as vítimas que ainda não sabem que ele foi preso e condenado e possam seguir a vida em paz, sem o medo de ele aparecer de repente e seguir com as torturas psicológicas às quais foram submetidas anteriormente.

4. O PAPEL DO INVESTIGADOR

É de grande relevância o papel deste profissional na atualidade, dado o aumento de usuários de redes sociais, internet e nos ambientes virtuais de forma geral. Com o aumento destes, aumentou também a quantidade de crimes nos meios eletrônicos e a necessidade de se ter alguém para elucidá-los.

O perito forense digital tem competências/habilidades e funções como:

- ✓ Ser organizado, metódico, curioso, autodidata, comunicativo, além de ter qualificações na área tecnológica e outras especificidades.
- ✓ Ter fluência em inglês e espanhol.
- ✓ Averiguar autoria de crimes.
- ✓ Coletar e analisar imagens e dados de computadores e outros dispositivos que contenham informações sobre o crime cometido.
- ✓ Arquivar tudo que for coletado para ser analisado ao final das investigações realizadas.
- ✓ Recolher dados e equipamentos para posterior análise.
- ✓ Saber usar tecnologias e ferramentas para recuperação de dados perdidos.
- ✓ Habilidade para armazenamento dos dados analisados em outro equipamento para preservar a segurança dos mesmos.
- ✓ Realizar cruzamento de informações para acareação dos fatos e pessoas envolvidas.

As principais caraterísticas são a honestidade e conhecimentos aprofundados para poder atuar. Não se restringe portanto, apenas ao conhecimento técnico, mas principalmente ao caráter do indivíduo. Tem de ter também conhecimento na área de processos judiciais para não se limitar apenas a uma assistência técnica e perícias internas. O campo se estende para fora dos domínios internos da polícia civil, necessitando de colaboração do mesmo em pesquisas externas.

O mercado de trabalho exige domínio amplo de táticas e tecnologias, assim como intensa dedicação ao trabalho para alcançar objetivos sérios que envolvem a vida e segurança do público alvo de proteção que são os usuários de redes sociais e internet de forma geral.

Nos últimos anos, somente no Brasil foram milhões de vítimas de links maldosos e que tiveram dados roubados, convertidos em prejuízos financeiros e psicológicos. Mais de 70% de empresas brasileiras relataram prejuízos por fraudes digitais nos últimos anos. Sendo assim, a demanda para este tipo de serviço cresce a cada dia, tornando o mercado de trabalho muito promissor para o perito forense digital.

5. AS QUESTÕES LEGAIS, POLÍTICAS E SOCIAIS ENVOLVIDAS

Não só na esfera nacional como na internacional, debatem-se questões relativas à segurança nas informações da internet e o grande número de crimes ocorridos nela. Principalmente para soluções viáveis com maior eficácia seja na esfera repressiva como na preventiva desses crimes. Inclusive para educar os usuários no uso destas tecnologias

digitais e evitar maiores danos a si, aos seus e a todo contexto envolvido nas tramas. A educação para inclusão digital é de vital importância para evitar estes crimes, para que os usuários se protejam.

Antes de 2020 não existia uma legislação específica para punir crimes virtuais. A partir daí criou-se projetos específicos para este tipo de crime. As principais leis e projetos de lei que julgam estes crimes são:

- ***LEI Nº 11.829***, DE 25 DE NOVEMBRO DE ***2008***. Altera a Lei noº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.
- Em 2012 foi criada a Lei de Crimes Cibernéticos 12 737/2012 ou lei Carolina Dieckman tipificando os atos cibernéticos criminosos com invasão de dispositivos, violação de dados, interrupção de sites de qualquer espécie.
- Lei 12 965 de 23 de abril de 2014 – "Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil".
- Projeto de Lei 4 554/2020 pelo Senador Izalci Lucas, que foi aprovada alterando texto do código penal criado pelo Decreto se Lei 2 848/1940 que penaliza invasões de dispositivos, fruto qualificado e estelionato em meio digital.
- A partir de maio de 2021 foi criado outro projeto de Lei de nº 14 155/2021, sancionada pelo Presidente Jair Bolsonaro, com penas mais duras, com mesmos objetivos da lei anterior.

No Jornal do Senado de 28 de maio de 2021, foi publicado um texto, que dispõe sobre os crimes relacionados à inovação dos dispositivos de informática:

> "... tem punição de até quatro anos de reclusão com multa e se o crime de invasão trouxer prejuízo pra vítima a pena aumenta de dois terços. A pena anterior era de até um ano de reclusão. Essa penalidade é imputada para quem invadir o dispositivo alheio para conseguir, modificar ou apagar conteúdos cibernéticos sem licença do dono, ou hospedar vírus ou qualquer outro Malware para prejudicar ou obter vantagens ilicitamente no dispositivo de outra pessoa. Se desse ato criminoso houver obtenção de conteúdo privado das redes eletrônicas privadas, a pena será de dois a cinco anos, somada à multa".

A partir desta data não existe nenhuma inovação nas leis relativas aos crimes cibernéticos.

6. CONSIDERAÇÕES FINAIS

Antes de 2020 não existia uma lei objetiva que realmente pudesse tipificar e punir os crimes virtuais. A partir de então tendo como primeira iniciativa a Lei Carolina Dieckman a legislação foi evoluindo de forma gradativamente, mas sabemos que ainda não chegamos a um patamar/resultado ideal.

Como toda lei brasileira ainda precisamos evoluir com mais agilidade e precisão nas investigações, tipificação e punição de crimes cibernéticos. A invasão de dispositivos é cada vez mais frequente causando prejuízos aos seus donos e usuários.

Apesar de avançada tecnologia em todos os ramos de atividade humana, na área criminal esse avanço é lento, pois qualquer erro pode ferir direitos ao invés de defendê-los ou preserva-los.

Na esfera internacional, vemos que o FBI agiu com habilidade, mas ainda não conseguiu se comunicar com todas as vítimas do crime, para levar a notícia da prisão do criminoso e tranquiliza-las para que possam seguir suas vidas. Isso se deve principalmente ao fato de que as redes sociais que ele usou para isso estão extintas, dificultando o acesso a essas pessoas.

REFERÊNCIAS

ALMEIDA, Haian de Assis Lopes de, OLIVEIRA, Tamar Ramos de. **Crimes Virtuais: o Avanço dos Crimes Eletrônicos e a Evolução das Leis Específicas no Brasil.** Disponível em: https://www.periodicorease.pro.br/rease/article/download/7554/2937 . Acesso em: 14 de março de 2023.

ASSIS, Rebeka. **Crimes Virtuais: Descubra quais são os 7 mais cometidos. jusbrasil**.com.br. Disponível em: < https://rebekaassis.jusbrasil.com.br/artigos/784440112/crimes-virtuais-descubra-quais-sao-os-7-mais-cometidos>Acesso em: 27 de fev de 2023.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet**. 2ª ed. atual. e ampl. São Paulo. Editora Juarez de Oliveira, 2009.

KAUARK Fabiana da Silva, MANHÃES Fernanda de Castro e MEDEIROS, Carlos Henrique, **Metodologia da Pesquisa, Um Guia Prático**, Via Litterarum Editora, 2010.

LAZZARINI, Gabriel Augusto Gonçalves. **Artigo Científico (Bacharelado em Direito)** – Universidade Presbiteriana Mackenzie, São Paulo-SP. 2020.

VALERA, Paulo Vinicius de Carvalho. **Crimes Virtuais e a Legislação Brasileira**. Trabalho Científico, bacharelado em Direito. Centro Universitário Toledo. Araçatuba. 2019.

Lei com penas mais duras contra crimes cibernéticos é sancionada. Senado Federal. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada>. Acesso em: 22 nov. 2023.

NULL. FBI busca vítimas de extorsão sexual de homem condenado a 105 anos de prisão. Gazeta do Povo. Disponível em: <https://www.gazetadopovo.com.br/mundo/fbi-busca-vitimas-de-extorsao-sexual-de-homem-condenado-a-105-anos-de-prisao-956gg9skq35d0w8sw6xe605tx/>. Acesso em: 22 nov. 2023.

Red de mentiras - Lucas Michael Chansler. [s.l.: s.n., s.d.]. Disponível em: <https://www.youtube.com/watch?v=ddeErOWtDmw>. Acesso em: 22 nov. 2023.

SENGUPTA, Sounak. Where is Sextortionist Lucas Michael Chansler Now? The Cinemaholic. Disponível em: <https://thecinemaholic.com/where-is-sextortionist-lucas-michael-chansler-now/>. Acesso em: 22 nov. 2023.