CENTRO DE EDUCAÇÃO SUPERIOR REINALDO RAMOS/CESREI

FACULDADE REINALDO RAMOS/FARR

CURSO DE BACHARELADO EM DIREITO

ROGERIO LIMA NASCIMENTO

CRIME CIBERNÉTICO:

Legislação e incidência na pandemia do COVID 19

CAMPINA GRANDE-PB

2020

ROGERIO LIMA NASCIMENTO

CRIME CIBERNÉTICO NA PANDEMIA DO COVID 19

Trabalho Monográfico apresentado à Coordenação do Curso de Direito da Faculdade Reinaldo Ramos - FARR, como requisito para a obtenção do grau de Bacharel em Direito.

Orientador: Prof. Me. André Gustavo Santos Lima Carvalho

CAMPINA GRANDE-PB

2020

N244c Nascimento, Rogerio Lima.
Crime cibernético: legislação e incidência na pandemia do COVID 19 / Rogerio Lima Nascimento. – Campina Grande, 2020.
55 f. : il. color.

Monografia (Graduação em Direito) – Faculdade Reinaldo Ramos-FAAR, Centro de Educação Superior Reinaldo Ramos-CESREI, 2020.
"Orientação: Prof. Me. André Gusttavo Santos Lima Carvalho".

1. Crimes Cibernéticos. 2. Crimes Virtuais – Legislação Brasileira. 3. Pandemia – Crimes Cibernéticos. I. Carvalho, André Gusttavo Santos Lima. II. Título.

CDU 343.63:004.738.5(81)(094.4)(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

ROGERIO LIMA NASCIMENTO

CRIME CIBERNÉTICO:

legislação e incidência na pandemia do COVID 19

Aprovada em: ___/___/_____.

BANCA EXAMINADORA

_____

Prof. Me. André Gustavo Santos Lima Carvalho
Faculdade Reinaldo Ramos – FARR
Orientador

_____

Prof. Me. Rodrigo Araújo Reul
Faculdade Reinaldo Ramos – FARR
1° Arguidor

_____

Prof. Me. Vinicíus Lúcio de Andrade
Faculdade Reinaldo Ramos – FARR
2° Arguidor

Dedico este trabalho a Deus, a minha Esposa, minha Filha, meus Pais e todos meus familiares, pois sem vocês eu não teria capacidade para desenvolver este trabalho.

AGRADECIMENTOS

Sempre que nos deparamos com momentos que nos conduzem a uma nova etapa da vida, nos lembramos de que não atingimos nossas metas sozinhos. Para alcançarmos nossos objetivos, grandes pessoas estão ao nosso lado e colaboram para que os resultados sejam os melhores possíveis.

Portanto meu sinceros agradecimentos a todos aqueles que me incentivaram por essa conquista. Em primeiro lugar agradeço a Deus nosso Pai Celestial, por nos conceder o dom da vida e poder lutar todos os dias pelos nossos sonhos. A Nossa Senhora, por interceder por nós e engrandecer a nossa fé.

A minha esposa Moniky e minha filha Sofia, por serem o principal combustível da realização do meu sonho, pois essa conquista não é só minha, também é de vocês e para vocês.

A meus pais, Roberto e Socorro, por serem exemplos para nossa família e por me darem a educação adequada para poder chegar a esse estágio da vida, vocês foram fundamentais para este acontecimento.

A meus irmãos, cunhadas e sobrinhos por acreditarem em mim. A toda minha família pelo carinho e incentivo, em especial a minha Vó Carminha, por me colocar em suas orações.

A meu professor André, por aceitar meu convite para me orientar nesse trabalho.

Aos meus amigos que de alguma maneira incentivaram para realização desse sonho. Serei eternamente grato a todos vocês por essa conquista.

“Onde há fé há sonhos e uma força capaz
de os concretizar”.

(AUTOR DESCONHECIDO)

RESUMO

A presente pesquisa acadêmica gira em torno das discussões referentes ao problema do crescimentos dos crimes cibernéticos nos últimos anos e as grandes incidências no período da pandemia do novo coronavírus no Brasil, mostrando que trata-se de um problema à ser observado e discutido na tentativa de encontrar soluções viáveis, ou seja, buscar meios de solucionar a problemática em questão. Desta maneira, essa pesquisa científica, tem como finalidade apontar os dados relativos ao crescente de crimes cibernéticos no Brasil, ou seja, analisar dados de fontes confiáveis. Além disso, verificar a relação entre os crimes cibernéticos e o volume crescente de internautas, principalmente no período de quarentena e a necessidade de uma legislação especifica de combate aos crimes cibernéticos além das normas já existente. Em relação a metodologia empregada, usou-se o método dedutivo (levantamento de dados); pesquisa aplicada na tentativa de encontrar solução para o problema em questão; quanto aos objetivos, utilizou-se o exploratório e o explicativa. No que diz respeito aos resultados da pesquisa, foi observado a incidência de estatísticas crescente referente aos crimes cibernéticos no Brasil e, principalmente, na pandemia do novo coronavírus. Portanto, conclui-se que os números crescentes dos crimes cibernéticos estão relacionados com as crescente facilidades de acesso aos computadores, smartphones e a internet. Desta forma, ver-se que há a necessidades de legislações cada vez mais especificas, inclusive, leis temporárias a serem aplicadas no período crises como a pandemia.

Palavras chave: Crimes cibernéticos. Legislações. Pandemia.

ABSTRACT

The present academic research revolves around the discussions regarding the problem of the growth of cybercrimes in recent years and the great incidences in the pandemic period of the new coronavirus in Brazil, showing that it is a problem to be observed and discussed in an attempt to find viable solutions, that is, look for ways to solve the problem in question. In this way, this scientific research, aims to point out the data related to the growing cyber crimes in Brazil, that is, to analyze data from reliable sources. In addition, to verify the relationship between cyber crimes and the growing volume of Internet users, especially in the quarantine period and the need for specific legislation to combat cyber crimes in addition to the existing rules. Regarding the methodology used, the deductive method (data collection) was used; applied research in an attempt to find a solution to the problem in question; as for the objectives, the exploratory and the explanatory were used. With regard to the results of the research, an increasing incidence of statistics was observed regarding cyber crimes in Brazil and, mainly, in the pandemic of the new coronavirus. Therefore, it is concluded that the increasing numbers of cyber crimes are related to the increasing access to computers, smartphones and the internet. Thus, it can be seen that there is a need for increasingly specific legislation, including temporary laws to be applied in the period of crises such as the pandemic.

Keyword: Cyber crimes. Legislation. Pandemic.

SUMÁRIO

INTRODUÇÃO

A referida pesquisa trata dos crimes cibernéticos levando em consideração as legislações e incidências na pandemia do COVID 19, neste sentido, com as diversas possibilidade trazidas pela internet (estudar, trabalhar, estudar, pesquisar e outras), tornando-se possível conecta-se em tempo real com pessoas de todas as partes do mundo dados as facilidades e a quantidade de usuários no planeta.

Desta maneira, em virtudes dos grandes volumes de pessoas conectadas ao mesmo tempo, em uma ambiente que possuem pessoas bem e má interinadas, fazendo surgir assim, as incidências de crimes no mundo virtual, principalmente em virtude da pandemia do novo coronavírus.

Nesse diapasão, a presente pesquisa possui como escopo contextualizar a ocorrência dos crimes cibernéticos, de modo a ressaltar os perigos causados por um regramento insuficiente no tocante ao tema.

Diante disso, essa pesquisa acadêmica tem por objetivo analisar as grandes incidências dos crimes cibernéticos no período da pandemia do COVID 19 no Brasil, além disso, apontar o crescimento dos crimes cibernéticos e as legislações de combate, procurando assim, verificar e analisar possíveis formas de solucionar as problemáticas em questão.

Tais objetivos visam confirmar ou negar à possiblidade de uma legislação especifica de combate aos crimes cibernéticos no Brasil mesmo diante da legislação vigente. Tendo como problemática o crescimento dos crimes virtuais no Brasil. Nesta perspectiva, esse trabalho acadêmico foi dividido em três capítulos.

O primeiro capítulo traz os dados referente ao crescimento dos crimes cibernéticos no Brasil nos últimos anos, apontando que o crescimento dos crimes virtuais estão atrelados aos crescimentos dos números de internautas, gerando assim, uma preocupação frente a essas realidades, além disso, esse capítulo procura mostrar o conceito de crimes cibernéticos e o contexto histórico sobre o surgimento da internet.

Já o segundo capítulo, trata de identificar as principias legislações de combate ao crimes virtuais no Brasil, ou seja, discute sobre o Marco Civil da internet, Lei Carolina Dieckmann e outra referente a temática em questão, tendo como

objetivos verificar a necessidade ou não de mais legislações ou aperfeiçoamento das normas já existente.

E por fim, o terceiro capítulo, que procura estabelecer uma discussão referente ao crimes cibernéticos praticados no Brasil durante a pandemia do novo coronavírus, apontando assim, o contexto de surgimento da pandemia e as grandes incidências de crimes cibernéticos na pandemia.

Nesse sentido, destacam-se como objetivos gerais realizar uma análise sobre os crimes cibernéticos e apontar os principais entraves à identificação e punição dos criminosos. A fim de se chegar a tais objetivos, foi necessário traçar um contexto conceitual e histórico sobre internet e o desenvolvimento dessas condutas em tal meio, juntamente com uma exposição acerca da (insuficiente) legislação que versa sobre o tema, além dos desdobramentos dessa falta de especificidade no contexto da produção de provas e processamento dos crimes virtuais.

Metodologia

Quanto ao método da pesquisa, foi utilizado o método dedutivo, ou seja, levantamento de dados referente a temática em questão, a saber, crimes cibernéticos. No que diz respeito a natureza da pesquisa, usou-se a pesquisa aplicada com o objetivo de buscar conhecimento para aplicar na solução da problemática da pesquisa.

Quanto aos objetivos metodológicos, se fez necessário a utilização do exploratório e explicativa. Em relação aos procedimento técnicos, foram usados a análise de documentos (dados estatísticos); revisão bibliográfica, levando em consideração os principais doutrinadores sobre a temática em questão.

1 CRESCIMENTO DOS CRIMES CIBERNÉTICOS NO BRASIL

Com o surgimento das ideias de globalização (interdependência entre país), surgiu paralelamente, uma sociedade que a cada dia vem vivenciando a chamada revolução da informática, trazendo consigo diversas inovações no cenário da informatização, onde, tornou–se possível até mesmo a substituição da mão-de-obra humana por máquinas informatizadas.

> Com a existência da evolução da tecnologia muitos são os casos conhecidos em que o ser humano é trocado pela máquina. Nestes momentos a nossa tecnologia está avançada a ponto de as nossas máquinas conseguirem comunicar entre elas, mas será que é assim tão favorável esta substituição? Nós com o nosso lado humano tentamos sempre proteger a nossa parte, e em vários casos conseguimos obter o resultado desejado, temos alguns argumentos para nos defendermos, mas por outro lado, as pessoas que oferecem os empregos têm outra mentalidade. Apenas têm um objetivo, obter o máximo de lucro possível, e principalmente a nível de grandes empresas a substituição do homem pela máquina tem resultado na perfeição (GOMES, 2020, p. 2).

Sendo assim, pode-se entender que Revolução da Informática foi o principal movimento da sociedade se interessar cada vez mais por tecnologias e serviços ligados a informatização e que de certa forma, possa facilitar o cotidiano cidadão.

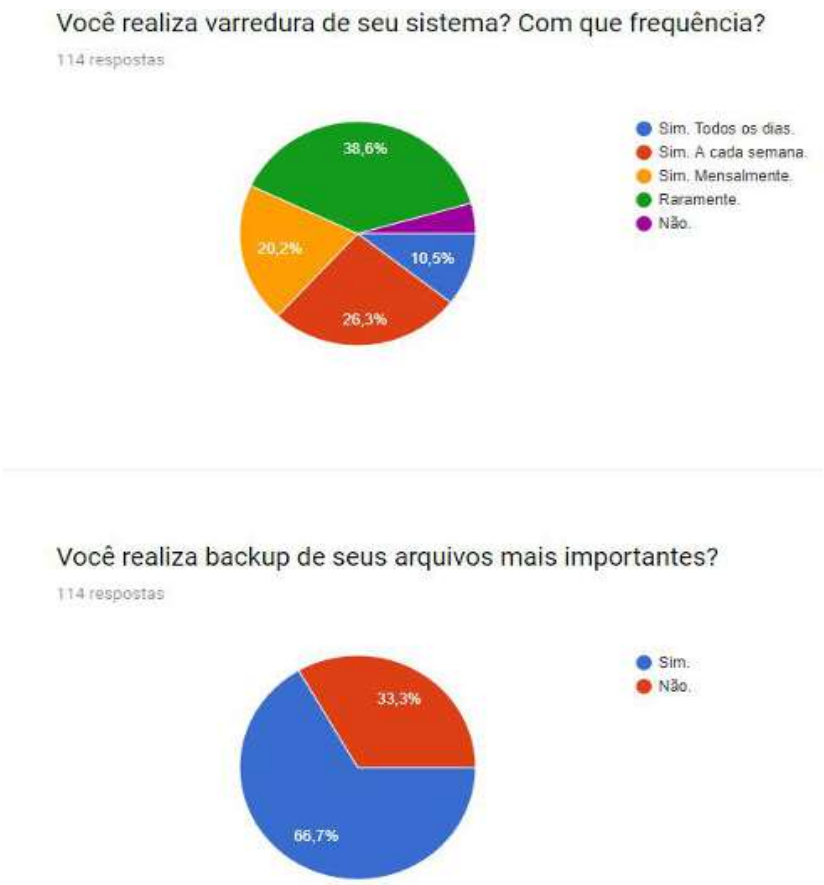
No passado, era normal uma comunicação que usava papel, cola, envelope, selo e o correios, diferentemente da atualidade, onde basta tão somente dois celulares como internet, digitar e enviar.

> Enquanto a maioria dos bens antigamente era representada por átomos, hoje boa parte deles é representada por bits. No passado, era necessário tinta, papel, cola, selo, envelope e correios para se comunicar, hoje, para o envio de uma mensagem eletrônica, basta que cada indivíduo a digite em seu teclado e clique em enviar. Mais modernamente, basta falar (MACHADO, 2018, p. 5).

Desta maneira, tornou-se usual a utilização de smartphones em substituição dos computadores, tornando-se cada vez mais fácil pesquisar um preço de um produto ou serviço, fazer transações financeiras, investir no exterior, estudar na modalidade EAD, fazer pesquisas acadêmicas, enfim, há diversas possibilidades.

Porém, essas possibilidades vieram atreladas aos riscos ou a vulnerabilidade de estar em um mundo virtual e que, há uma incidência baixa de atitudes que traz uma proteção significativa como mostra gráfico abaixo.

Gráfico 01: Varredura e backup



Fonte: Meorin (2019)

1.1 CONSIDERAÇÕES HISTÓRICAS SOBRE O SURGIMENTO DA INTERNET E A IDEIA DE CIBERCRIME

No meio da Guerra Fria, na década de 1950, já existia a ideia de criar a internet. Mas somente na década de 1960 ela teve um grande desenvolvimento. Foi criada na região militar dos Estados Unidos durante a guerra para proteger o país e evitar publicar dados relacionados à segurança nacional e também perda de documentos importantes. Desde tempos remotos até tempos longínquos, o ser humano foi criado para o desenvolvimento e tem procurado a inovação para alcançar a tecnologia, que também faz parte do desenvolvimento da sociedade. Assim,

> Em 1946, foi desenvolvido o primeiro computador digital, intitulado ENIAC. Por volta de 1950, iniciou-se sua produção para comercialização. O então presidente dos Estados Unidos, John Kennedy, comprometeu-se a criar um satélite de defesa à prova de destruição, para a concretização de sua promessa e impulsionar a evolução tecnológica foi criada a Agência de Investigação de Projetos Avançados (Advanced Research Project Agency – ARPA). Esta agência foi responsável pelo desenvolvimento da Internet, que foi originada no período de Guerra Fria, especificamente em 1969, denominada “ArpaNet”. Sua principal finalidade era manter comunicação entre as bases militares dos EUA. (SANCHES, 2018, p. 5).

Com o desenvolvimento da Rede Nacional de Ensino e Pesquisa, a internet no Brasil surgiu por volta de 1980 e se expandiu para todo o país em 1997. Esse é o progresso da humanidade, ele moderniza a forma de interação entre as pessoas, e assim proporciona comodidade. As cartas que costumavam levar meses para chegar ao destinatário agora chegam imediatamente.

Por sua vez, a história do cibercrime pode ser rastreada na década de 1970, quando o termo “hacker” foi definido pela primeira vez porque indivíduos com conhecimentos técnicos puderam facilitar a invasão de sistemas operacionais privados e a proliferação de pragas virtuais.

Como todos já sabemos que o progresso tecnológico marca a história da humanidade e está gradualmente se tornando uma ferramenta necessária e indispensável para a vida normal.

No entanto, a conveniência e velocidade da informação no compartilhamento via internet causa grandes dificuldades no controle de atividades do usuário, pois permite o anonimato. Por isso que esse tipo de crime permite que os criminosos escapem na maior parte do tempo. Diante deste cenário, ver-se

> Atualmente, nosso país ocupa o quarto lugar em número de usuários de internet, segundo dados da Conferência das Nações Unidas sobre Comércio e Desenvolvimento. Os crimes cibernéticos crescem de forma proporcional a quantidade dos adeptos virtuais. Tais ilícitos geralmente se referem a condutas que lesionam a esfera íntima e pessoal das vítimas. Busca-se enquadrar as ilicitudes nas figuras penais típicas, porém, o Código Penal vigente é de 1940, desta forma, não abarca determinados comportamentos da sociedade moderna. (SANCHES, 2018, p. 5).

Diante do que está acontecendo no mundo devido a pandemia do covid-19, onde teve o aumento do confinamento familiar e todos se recolheram nos seus ambientes virtuais. Analisaremos como o sistema jurídico brasileiro está organizado para combater essas condutas ilegais cada vez mais frequentes.

1.2 CONCEITOS DE CRIMES CIBERNÉTICOS

Primeiramente, é interessante apontar que há uma diversidade de denominações e conceituais quando o assunto diz respeito aos crimes praticados no território da virtualidade. Desta maneira, ver-se que as denominações são:

> As denominações quanto aos crimes praticados em ambiente virtual são diversas, não há um consenso sobre a melhor denominação para os delitos que se relacionam com a tecnologia. Entre outros, temos crimes de computação, delitos de informática, abuso de computador, fraude informática, em fim, os conceitos ainda não abarcam todos os crimes ligados à tecnologia, e, portanto, deve-se ficar atento quando se conceitua determinado crime, tendo em vista que existem muitas situações complexas no ambiente virtual. (SCHMIDT, 2015, p. 3).

Essas são as principais denominações usadas para apontar os indivíduos que praticam crimes no mundo virtual, contudo, vale indicar ainda, que há uma denominação que é bastante utilizada no Brasil, a saber, crime cibernético e que é justamente a temática desta pesquisa acadêmica, inclusive,

> Não há uma nomenclatura sedimentada pelos doutrinadores acerca do conceito de crime cibernético. De uma forma ou de outra o que muda é só o nome atribuído a esses crimes, posto que devem ser observados o uso de dispositivos informáticos, a rede de transmissão de dados para delinquir, o bem jurídico lesado, e ainda deve a conduta ser típica, antijurídica e culpável. (DA SILVA, 2015, p.39).

Além destas denominações citadas por Schmidt (2015), há outras que são mais usadas pelos internautas brasileiros, apontando assim, práticas recorrentes no mundo virtual.

> Profusas são as denominações para os crimes eletrônicos. São chamados cibercrimes ou, há quem prefira chamá-los de crimes virtuais, entretanto, não importa qual o nome se dê para esta pratica ilícita, pois seu conceito é bem simples de ser compreendido. Ao lado dos benefícios que surgiram com a disseminação dos computadores e do acesso à Internet, surgiram crimes e criminosos especializados

> na linguagem informática, proliferando-se por todo o mundo. Tais crimes são chamados de crimes virtuais, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, fraude informática, delitos cibernéticos, crimes transnacionais, dentre outras nomenclaturas. (DUARTE, 2018, p. 3).

A denominação cibernética faz relação aos sistemas informatizados e de armazenamento de dados no campo virtual, vale ressaltar que, quando associado a questões criminais, tal concepção se torna mais complexa, tendo em vista que não é um crime tão simples de encontrar e punir seus autores, pois, com a revolução da computação e da internet, veio paralelamente, o surgimento de crimes e suas complexidades no mundo virtual.

Assim, esses crimes no ambiente virtual, chamados de crimes cibernéticos, pode ser entendido ou conceituado como aqueles que

> [...] poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança Informática [...]. (ROSSINI, 2004, p. 110).

Nesta concepção, percebe-se que os crimes cibernéticos de uma forma geral podem ser entendidos como aqueles crimes praticados no ambiente virtual pela pessoa física ou jurídica de forma omissiva ou comissiva.

Desta maneira, “através do conceito analítico finalista de crime, pode se chegar à conclusão de que crimes cibernéticos são todas as condutas típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática”. (SCHMIDT, 2015, p. 1). Neste mesmo perspectiva, tem-se o conceito de Rossini (2004), trazendo a ideia de que o delito de informática

> Poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade. (ROSSINI, 2004, p. 110.)

Além deste conceito, tem-se também a concepção conceitual de Machado (2014) que traduz os crimes cibernéticos como aqueles praticados com finalidades diversas, a saber, adquirir dados, violar comunicação e outras ideias citadas pela autor.

> “Cibercrimes”, “Crimes Cibernéticos”, “Crimes Digitais”, “Crimes Informáticos”, “Crimes Eletrônicos”, são termos para definir os delitos praticados contra ou por intermédio de computadores (dispositivos informáticos, em geral), importam nas menções às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, bullying, terrorismo, entre outros. (MACHADO, 2014, p. 4).

Inclusive, como visto na citação acima, os cibercrimes podem e/ou há a possibilidade também de estarem relacionados a incitação ao ódio, discriminação, pornografia infantil e desprezo a religião de terceiro, levando a entender que não se trata somente de crimes de invasão de sistemas. Porém, vale ressaltar que o artigo 154-A do Código Penal, traz a ideia de crimes cibernéticos como a violação de sistemas e fatores interligados.

1.3 ÍNDICES DOS CRIMES CIBERNÉTICOS

As incidências dos crimes cibernéticos tem se mostrado crescentes no Brasil, tendo em vista que são registrados números significativos em todo o país. No ano de 2018 ocorreram diversas denúncias no Brasil referentes a crimes cibernéticos, tais reclamações envolvem números alarmantes e que necessitam de uma rápida intervenção das autoridades públicas.

Em uma pesquisa divulgada em 2012 demonstrou um alto números de registos das incidências de ataques a sistemas de alguns países, ataques esses, relacionados à instituições de grande importância no cenário local, a saber, emissoras de televisão, sistemas hospitais, sistema do governo, dentre outros como mostra tabele abaixo deste incidentes.

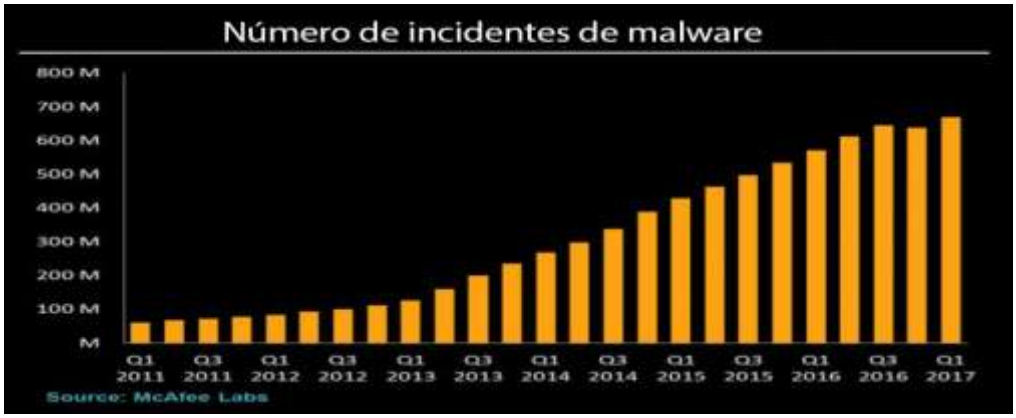
Tabela 01: Ataques à sistemas em vários países

MAIO 2012	Ataque	País	Mercado	Tipo de Dado	Registros
27	Hacker	USA	TV	Email, nome e senha de usuários	32
26	Hacker	USA	Financeiro	Número do Seguro Social, Nome e endereço	123.000
24	Perda e/ou vazamento	USA	Saúde Hospitalar	Informações pessoais e prontuários	2159
22	Exposto por acidente ao público	UK	Saúde Hospitalar	Informações pessoais e prontuários	59
20	ND	USA	Imigração Governo	Nomes e senhas de	51
			(Greencard)	usuários / emails	
19	Hacker	INDIA	Educação	Senhas de emails	500
17	Roubo de computador	USA	Saúde Hospitalar	Informações pessoais e securitárias	34.000
14	ND	USA	Governo da Califórnia	Informações pessoais e securitárias e	700.000

Fonte: Morais (2012).

Inclusive, pesquisas demonstraram um volume muito alto de ataques aos conectados no Brasil, ou seja, houve um crescimento muito grande nos números de ataques maliciosos envolvendo a incidências de malware como mostra gráfico abaixo, a saber, de 2011 à 2017 houve um crescimento espantoso.

Gráfico 01: Ataques maliciosos



Fonte: Christou (2017).

Para se ter uma ideia, cerca de 336 casos de crimes cibernéticos são registrados diariamente no país, inclusive, a associação SAFERNET apontou estatísticas que chegam à números extremamente preocupantes, onde, foram contabilizados cerca 133.732 (cento e trinta e três mil e setecentos de trinta e dois) casos que envolvia crimes virtuais.

> Diariamente, são registrados pelo menos 366 crimes cibernéticos em todo o país. O levantamento mais recente, feito em 2018 pela associação SaferNet Brasil, em parceria com o Ministério Público Federal (MPF), contabilizou 133.732 queixas de delitos virtuais, como pornografia infantil, conteúdos de apologia e incitação à violência e crimes contra a vida e violência contra mulheres ou misoginia e outros. (VEIGA, 2020, p.3).

É interessante observar ainda, que nos meses de janeiro à abril deste ano (2020) foram detectadas diversas incidências envolvendo spams, malwares e link maliciosos.

> De janeiro a abril, a Interpol detectou mais de 907 mil “spams”, 737 incidentes relacionados a malwares (softwares maliciosos) e 48 mil links suspeitos, todos relacionados à covid-19. A expectativa é que os números cresçam nos próximos meses. (VITTA, 2020 p. 5).

Tais crescimento das incidências podem estar relacionados, também, ao número cada vez mais crescente de usuários dos meios de comunicação relacionados a informática.

Notadamente, ver-se que houve um crescimento significativo no ano de dois mil e dezoito quando relacionado com o ano de dois mil e dezessete, com percentuais alarmantes, ou seja, crescimento de 110%, assim, houve 133.732 reclamações em 2018 e 63.698 reclamações em 2017.

> Em comparação ao ano anterior, a quantidade de ocorrências deu um salto de quase 110% – em 2017, a associação registrou 63.698 denúncias. Um fator que contribui para a ação criminosa, na visão de especialistas, é o descuido da população quanto ao uso de ferramentas que protejam os aparelhos celulares das invasões de hackers. Apesar de ser impossível estar 100% a salvo, o mínimo de precaução pode reduzir as ameaças à privacidade de cada um. (VEIGA, 2020, p. 3).

A utilização intensa dos celulares contribuem para a elevação dos crimes cibernéticos, pois o brasileiro passa muitas horas no celular, ou seja, nas redes sociais, executando trabalhos, estudando, enfim, o aparelho celular é um equipamento que faz parte da vida e do cotidiano dos brasileiros.

Esses equipamentos eletrônicos (smartfone e tablets) comportam informações ou dados pessoais (senhas, fotos, aplicativos bancários e etc), que podem sofrer ataques de criminosos que atuam no mundo virtual a procura de vítimas que não procuram investir ou buscar formas de se proteger, pois navegar na redes informatizadas demanda a necessidade de cuidados específicos.

> O cibercrime tem se modernizado e atingido cada vez mais alvos em todo o mundo. Os dispositivos móveis passaram a estar na mira desses ataques e muitos usuários ainda não conhecem as falhas na proteção de seus smartphones. Uma recente forma de invadir o sistema por meio dos sensores do mobile tem obtido muito êxito e preocupado especialistas de segurança em todo o mundo. Hackers têm conseguido descobrir senhas e códigos PIN (usados para bloquear a tela e até aplicativos bancários), ao acessarem os sensores de movimento dos aparelhos. Isso é feito remotamente, diretamente de um navegador da internet, sem a necessidade de que qualquer vírus seja instalado. (SANTOS, 2020, p.1).

Os crimes cibernéticos vem crescendo junto com um volume grande de denúncias, faz surgir, paralelamente, uma sociedade que procura vigiar e tomar cuidados nos acessos à internet. Tais cuidados, são necessários pelo fato dos números crescentes de ataques aos usuários da internet.

Essa realidade criminosa tem se intensificado pela utilização do home office no Brasil, essa forma de executar o trabalho tem sido alvo da criminalidade virtual no mundo.

> A adoção do home office em grande parte do mundo, uma das estratégias para evitar aglomerações em locais de trabalho e diminuir a propagação do vírus, está sendo explorada pelos hackers em busca de dados. O aumento da dependência de sistemas virtuais, segundo a Interpol, cria novas oportunidades para que esse tipo de crime seja cometido. Por isso, a agência alerta que empresas e trabalhadores atualizem programas que podem prevenir ataques. (VITTA, 2020 p. 5).

Um metodologia bastante utilizada pelo criminosos, também chamados de hackers, é justamente induzir a utilização de e-mails fraudulentos, onde a pessoa lesada chega a pensar que foi determinada empresa que enviou aquele e-mail, desta maneira, informam dados pessoais e até mesmo senhas.

Sendo assim, além dos cuidados supracitados, há outros que se fazem necessários dada a gravidade destes crimes, o que leva a entender que os internautas precisam tomar uma diversidade de cuidados para evitar certos incidentes, a saber,

Figura 01: Cuidados para evitar incidentes no mundo virtual

Fonte: Diário da Região (2019)

Esses cuidados são importantes pelo fato de evitar problemas gerados por criminosos que vivem nas redes da internet procurando vítimas em potencial de serem lesadas e até mesmo serem extorquidas por criminosos.

Assim, além dos crimes que envolve a violação de sistemas, há também um volume grande de reclamações que envolvem questões relacionadas à pornografia infantil, apologia à violência, à violação de privacidade, intimidade e ofensa, inclusive, esses crimes são praticados diariamente no mundo virtual em todo o pais, onde pessoas são vítimas de todo as formas de crimes virtuais. Abaixo, ver-se os índices destes crimes cometidos no ambiente digital e algumas dicas.

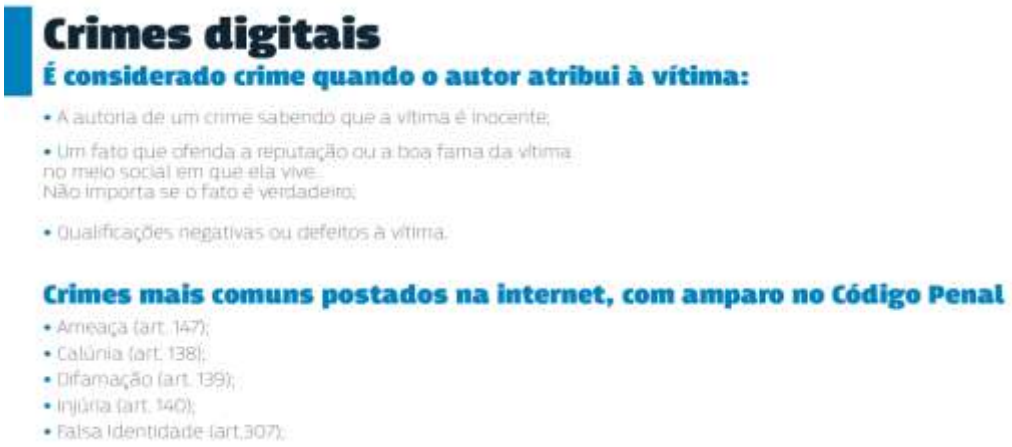
Figura 02: Crimes denunciados e dicas de segurança

Fonte: Estadão de Minas (2020)

Vale ressaltar, que se faz necessário o surgimento de políticas públicas de segurança voltas para essa realidade. Abaixo, alguns crimes que são praticados diariamente no ambiente digital e que necessita de uma atuação forte do Estado.

Caso contrário, haverá cada vez mais um crescimento significativo das incidências de diversos crimes desta natureza.

Figura 03: Crimes digitais.



Fonte: CNJ (2018).

A maioria destes crimes supracitados, são praticados nas redes sociais no Brasil e podem ser entendido como uma violação dos direitos a honra e a dignidade humana, assim, tais crimes serão discutidos de uma forma mais abrangente no capítulo dois.

2 LEGISLAÇÕES DE COMBATE AOS CRIMES VIRTUAIS

2.1 CRIMES COMUNS COMETIDOS NO AMBIENTE VITUAL

Com o mundo cada vez mais conectado à internet, ou seja, as pessoas estão conectadas entre si através de redes sociais, contando com um volume de milhares de indivíduos conectados ao mesmo tempo e em tempo real, inclusive, há também aqueles que não usam as redes sociais, mas se conectam para finalidade (transações bancárias, prestar serviços e outras finalidades).

Assim, levando a entender que a internet passou a ser considerada como essencial na vida dos indivíduos e que, tornou-se quase impossível não estar conectado de alguma forma na sociedade moderna.

> A internet se tornou uma parte essencial da vida moderna, mesmo havendo lugares em que as pessoas não possuem o acesso tão facilitado. Desde 2005, no dia 17 de maio, é comemorado o Dia Mundial da Internet em vários países. E uma pesquisa feita pelo Internacional Communications Union mostra como o universo online cresceu de forma impressionante nos últimos anos. (NOGUEIRA, 2019, p. 8).

Essa importância dada as conectividades e o volume de contentados passou a ser uma porta de entrada para as práticas de crimes, assim, pessoas más intencionadas passaram a praticar crimes no ambiente virtual e trazendo consigo uma diversidade de medos e inseguranças por parte da população em geral.

Abaixo ver-se a tabela dos principais crimes cometidos e os percentuais de incidência no ambiente virtual e que serão discutidos posteriormente, tendo em vista a sua gravidade.

Tabela 02: Crimes praticados no ambiente virtual

tema	denúncias	aumento/queda em relação a 2017
pornografia infantil	60.002	79,5 %
apologia e incitação a crimes contra a vida	27.716	154,4 %
violência contra mulheres	16.717	1639,5 %
xenofobia	9.705	567,9 %
racismo	8.337	37,7 %
LGBTfobia	4.244	59,1 %
neonazismo	4.244	51,7 %
maus tratos contra animais	1.142	-77 %
intolerância religiosa	1.084	-27,8 %
tráfico de pessoas	509	-14,4 %

Fonte: Rodrigues (2018)

A maioria destes crimes cometidos no ambiente virtual já eram previstos nas legislações penais, ou seja, já eram crimes antes da revolução mundial da informática. Assim, esses crimes passaram a ser praticados no ambiente digital, inclusive, são os mais praticados nas redes sociais.

Além destes (tabela 02), tem-se também os ataques a sistemas com a finalidade de adquirir dados pessoais, ou seja, senhas bancarias, CPF, endereços, números de cartões de créditos, enfim, qualquer coisa que possa trazer vantagem financeira ou prejuízo. Abaixo ver-se o gráfico com os principais links maliciosos que tem por finalidade invadir sistemas para adquirir dados pessoais.

Gráfico 02: Links maliciosos

Fonte: Iumiun (2018).

Porém, há alguns crimes que são cometidos e que, frequentemente, são vistos nas redes sociais do Brasil, inclusive, são crimes que mexem muitas vezes com o psicológico das pessoas que são vítimas de criminosos do mundo da virtualidade, a saber, são crimes de calúnia, ofensas, ameaças e falsidade ideológica.

Esses são os principais crimes cometidos no âmbito virtual, ou seja, são vistos com frequência nas redes sociais brasileira, inclusive, devem ser denunciados o mais breve possível para que as autoridades competentes possam tomar as medidas cabíveis.

> Quem sofre um ataque nas redes sociais deve denunciar e fazer valer seus direitos. No entanto, nem todos sabem que estão sendo vítimas de um crime virtual. Os principais delitos na Internet são relacionados aos crimes contra a honra (injúria, difamação e calúnia), contra a liberdade pessoal e à falsidade ideológica: injúria: ofender, xingar, chamar alguém de algo que se considera ofensivo, atingindo sua honra. Difamação: afirmar que alguém cometeu algo desonroso, como a traição, afetando sua reputação. Calúnia: acusar alguém de um crime que não cometeu. Dos três crimes contra a honra, é o mais grave. Ameaça: ameaçar alguém, por escrito, palavra ou gesto. É um crime contra a liberdade pessoal. Falsidade ideológica: criar um perfil falso nas redes sociais se passando por outra pessoa. (MUNDO ADVOGADOS, 2018, p. 6).

Desta maneira, muitos internautas as vezes não sabem que estão sendo vítima de um crime, ou seja, são indivíduos leigos e com pouca instrução educacional, assim, terminam sendo caluniados, por exemplo, e nem percebem.

Sendo assim, um dos crimes que frequentemente se ver nas redes sociais é a calúnia, ou seja, a atribuição da autoria de um crime (definido em lei) a algum, inclusive, tendo ciência que tal indivíduo não é autor, caracteriza desta forma o crime de Calúnia prevista na legislação penal.

> Portanto, para que se configure a calúnia, deve existir sempre uma imputação falsa de um fato, definido como crime. Caso não seja um fato, mas, sim, um atributo negativo quanto à pessoa da vítima, o crime será de injúria sendo um fato que não se configure em crime, podendo até mesmo ser uma contravenção penal, o delito será o de difamação; acreditando o agente que o fato definido como crime é verdadeiro, incorrerá em erro de tipo, afastando o dolo do art. 138, podendo, contudo, ainda ser responsabilizado pelo delito de difamação (GRECO, 2007, p.432).

Tal conceito relativo a calúnia está previsto no Código Penal, artigo 138 e que, tem a penalidade entre seis meses e dois anos de prisão, além do pagamento de possíveis multas.

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa. § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga. § 2º - É punível a calúnia contra os mortos. § 3º - Admite-se a prova da verdade, salvo: I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível; II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141; III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível. (BRASIL, 1940).

Outro crime visto nas redes sociais é o de difamação, que está positivado no artigo 139 do Código Penal, onde consiste na atribuição de um fato ofensivo em relação à reputação ou honra de uma pessoa, como por exemplo, boatos que afete a permanência no trabalho, na igreja ou na associação que determinada pessoa participa.

Veja que há um diferença entre o crime de calúnia e a difamação, o primeiro está previsto em lei e o segundo não está previsto na lei, ou seja, se determinada afirmação estar positivado em lei, trata-se de calúnia (ex. afirmação de furtou) e se não estiver positivado na lei, trata-se de difamação (ex. chamar alguém de prostituta). Assim, o crime de difamação consiste, pautado na legislação penal, em:

> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa. Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções. (BRASIL, 1940).

Esse tipo de crime, tem uma penalidade inferior ao crime de calúnia, ou seja, a difamação tem a penalidade entre três meses e ano de prisão, tendo ainda, a possibilidade do pagamento de multa.

O terceiro crime visto nas redes sociais refere-se a injúria, ou seja, ofensa relacionada à dignidade de uma pessoa, através de humilhação, insultos e outras questões semelhantes. Tal crime está positivado no artigo 140 do Código Penal.

> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa. § 1º - O juiz pode deixar de aplicar a pena: I - quando o ofendido, de forma reprovável, provocou diretamente a injúria; II - no caso de retorsão imediata, que consista em outra injúria. § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes: Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência. § 3o Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência: Pena - reclusão de um a três anos e multa.

Vale ressaltar, que a ofensa à dignidade do indivíduo, levando em consideração questões de raça, cor, etnia, religião ou condição de pessoa idosa e portadora de deficiência, esses casos, podem ser vistos pela legislação penal como Injúria qualificada (§ 3º do artigo 140 do Código Penal). Inclusive, tem uma penalidade superior, a saber, de um a três anos de reclusão.

É interessante apontar que esses crimes praticados no ambiente digital são relativos à opinião de pessoas referentes à questões de atribuição físicas e morais, afetando diretamente a autoestima e a honra de pessoas que são vítima destes crimes.

> É importante registrar que estes crimes dizem respeito à opinião de terceiros no tocante aos atributos físicos, intelectuais e morais da pessoa, ou seja, quando falamos que determinada pessoa tem boa ou má reputação no meio social, referindo-se a seus conceitos perante a sociedade; e referem-se também à opinião que a pessoa tem de si mesmo, atingindo seu amor próprio, sua autoestima. A honra nada mais é do que o conjunto de qualidades físicas, morais e intelectuais do ser humano, que o fazem merecedor de respeito no meio social em que vive. Honra, melhor dizendo, é um sentimento

> natural, inerente a todo ser humano, cuja ofensa produz uma significativa dor psíquica, um abalo moral, geralmente acompanhados de atos de repulsão ao ofensor. (CORREA, 2015, p. 08).

Portanto, a honra trata-se de um patrimônio moral e que, é indicado na Constituição Federal como um direito fundamental, previsto no artigo 5º, inciso X, assim, “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. (BRASIL, 1988).

Assim, publicações de cunho ofensivo contra a honra tem se tornado frequente nas redes sociais e nos aplicativos que conectam pessoas entre si, inclusive, tem sido objeto de demandas judiciais indenizatórias e até criminal, isso ocorre justamente pelo excesso da liberdade de expressão, gerando violações constitucionais e preceitos penais.

Além destes crimes supracitados (crimes contra a honra), tem-se também outros crimes que são praticados no ambiente digital, a saber, a ameaça (artigo 147 do Código Penal) e a falsa identidade (artigo 307 do Código Penal).

2.1 LEGISLAÇÕES DOS CRIMES CIBERNÉTICOS

Pelo fato dos brasileiros estarem cada vez mais conectados ao mundo digital, tornou-se comum o surgimento dos crimes cibernéticos na sociedade atual, dado ao volume de pessoas conectadas sem tomar os devidos cuidados citados anteriormente nas discussões.

Desta maneira, as ideias de “proteção” através do anonimato tem incentivado milhares de internautas a acharem que podem publicar conteúdos de forma ofensivas à toda e qualquer pessoa conectada sem ser notada a origem das ofensas. Além disso, tem-se o furto de senhas e invasões indevidas de páginas de pessoas famosas para extorquir ou denegrir suas imagens pela internet.

> Está bastante difundida na mídia e no senso comum que a sensação de anonimato proporcionada pela Internet facilita a prática de ilícitos na rede. Não raro encontramos quem defenda que o "anonimato online" é proibido ou vedado pela Constituição que teria criado uma condição para o exercício da liberdade de expressão, qual seja, a identificação pessoal e inequívoca de todo e qualquer autor de uma manifestação. (SHINCARIL, 2020, p. 01).

É interessante apontar, que muitos cidadãos brasileiros não sabem que podem recorrer à Justiça com o objetivo de garantir a reparação de direitos lesados por pessoas anônimas que cometem crimes no mundo virtual. Abaixo serão discutidas as principais leis que combatem os crimes cometidos no ambiente da internet brasileira.

2.1.1 Principais legislações de combate aos crimes virtuais

Há atualmente duas legislações especificas que tratam dos crimes praticados no mundo virtual, e que, inclusive, foram aprovados no ano de 2012, sendo assim, tais legislações especificas alteraram o Código Penal no sentido de atribuir penas especificas para crimes praticados no ambiente virtual e, constitui a obrigatoriedade de delegacias especializadas em crimes virtuais.

Porém, o período anterior à 2012 não se tinha uma legislação especifica que viesse a punir os criminosos do mundo virtual, eventos negativos na internet abriram espaço para discussões envolvendo os crimes cibernéticos e a necessidade de ações do legislativo em promover uma legislação que punissem os crimes virtuais, tendo em vista, os anos anteriores à 2012 não havia

> Até 2012, não havia legislação específica para punir os crimes cibernéticos próprios, mas apenas legislação para crimes cibernéticos impróprios. Foi em decorrência de alguns episódios, como os ataques a sites do governo e divulgação de fotos íntimas da atriz Carolina Dieckmann, com alta repercussão, em diversos sites, que se abriram as discussões para punir os autores de condutas infracionais no meio virtual. Foram propostas e sancionadas, em caráter de urgência, duas leis que cobriam deficiências no ordenamento jurídico brasileiro: a Lei 12.735/2012 e a Lei 12.737/2012. (BRAIDA, 2020, p. 05).

Desta maneira, surgiu a Lei dos Crimes Cibernéticos, ou seja, a Lei nº 12.737/2012, tal lei ficou conhecida também como a Lei Carolina Dieckmann, assim, tipificou como crime as práticas de invasão de computadores que objetiva o furto de senhas, violação de dados ou divulgação de conteúdos privadas nas redes.

Porém, já havia uma reivindicação forte por parte do sistema financeiro brasileiro que houvesse uma lei que combatesse os grandes números de golpes e

furtos de senhas dos clientes dos bancos. Contudo, é notório que a repercussão do caso da atriz Carolina Dieckmann contribuiu para o surgimento deste lei.

> A atriz global Carolina Dieckmann teve 36 fotos íntimas roubadas após uma invasão no seu e-mail pessoal. O hacker exigiu dez mil reais da atriz para que não publicasse as fotos. Logo, Carolina foi à polícia e realizou a denúncia. Por pressão midiática e por ter acontecido com uma mulher com grande influência e apelo popular, a lei foi votada e sancionada pela ex-presidenta Dilma Rousseff rapidamente. (VITORIANO, 2018, p. 03).

Desta maneira, os crimes virtuais da Lei de Crimes Cibernéticos e que, foram acrescentados ao Código Penal diz respeito aos artigos 154-A e art. 298. Assim, o primeiro expressa a ideia que,

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (BRASIL, 1940).

Nesta perspectiva, a violação de sistemas sem a devida autorização, com o objetivo de adquirir senhas e criptografia por exemplo, passaram a constituir um crime com penalidade de 3 (três) meses a 1 (ano), inclusive, a incidência de multa, vale ressaltar ainda, que os criminosos utilizam de artefatos maliciosos para colocar vírus ou deixar vulnerável algum dispositivo específico.

Diante disso, se o criminoso furtar conteúdos ligados as comunicações privadas, segredos de cunho indústria, comercial e sigilosas, nestes casos, a legislação de crimes cibernéticos considera como um delito maior e consequentemente, atribui uma penalidade mais alta.

> Art. 154-A, § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (BRASIL, 1940).

Além disso, produção e venda de programa de computadores que tenha como finalidade cometer crimes positivados no artigo 154-A, também culmina na mesma pena supracitada, inclusive, haverá um aumento da pena casa haja prejuízos econômicos.

> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. (BRASIL, 1940).

Outro artigo que tem uma importância no cenário de combate aos crimes cibernéticos, faz menção a falsificação de cartões de créditos e de débitos, acrescentado o parágrafo único do artigo 298, incluso pela Lei nº 12.737/2012 no Código Penal.

> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena - reclusão, de um a cinco anos, e multa. Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito (BRASIL, 1940).

No mesmo ano de 2012, surgiu a Lei nº12.735/12 como o objetivo de instalar delegacias especializadas no combate aos crimes digitais, desta forma tornou-se mais acessível a busca por ajuda e a possibilidade de policiais especializados na investigação dos crimes cibernéticos.

2.1.2 Marco Civil da internet

Entende-se por Marco Civil da Internet o sancionamento da Lei 12.965 em 2014, ou seja, tal lei regulamentou os direitos e deveres dos indivíduos que navegam na internet (internautas), além disso, protege os dados e privacidade dos usuários da internet.

Nesta perspectiva, a quebra do sigilo somente é possível através de ordem judicial, assim, dados e informações de particulares são mantidos em segrego nos sites e redes sociais, gerando assim, garantias democráticas como mostra Martins (2018).

> É uma lei (número 12.965/14) que regulamenta a utilização da internet, estabelecendo princípios e garantias que tornam a rede livre e democrática no Brasil. Em vigor desde 23 de junho de 2014, ela assegura os direitos e os deveres dos usuários e das empresas provedoras de acesso e serviços online. Antes de virar lei, a proposta foi lançada pela Secretaria de Assuntos Legislativos do Ministério da Justiça, em outubro de 2009. Nessa fase, os temas abordados foram desenvolvidos com ajuda da população por meio de audiências públicas em todo o Brasil. (MARTINS, 2018, p. 2).

Nesta lei, é possível ver uma grande inovação em relação a retirada de determinados conteúdos do ar, ou seja, são retirados do ar aqueles conteúdos impróprios ou que ferem alguns preceitos, trazendo assim, uma maior segurança para que os internautas possam navegar com mais tranquilidade mesmo diante dos crimes cibernéticos.

É interessante observar que antes do sancionamento da Lei 12.965 em 2014, não se tinha qualquer regra em relação aos procedimentos referentes a retirada de conteúdos do ar, porém, com a lei em questão, tornou-se possível a retirada de conteúdos que não cumprem as exigências cabíveis.

> O Marco Civil não exige ordem judicial para a remoção de conteúdo da Internet. O provedor de aplicações de internet poderá indisponibilizar ou remover determinado conteúdo se ele ofender os termos de uso e políticas da plataforma. (TEFFÉ, 2017, p. 3).

Essa retirada de conteúdos do ar se mostra uma ferramenta importante no combate aos crimes cibernéticos, como por exemplo, no combate a divulgação anônima de conteúdos de pornografias relacionadas a crianças e adolescentes.

Desta maneira, os sites ou servidores que armazenam esses conteúdos impróprios podem livremente retirar do ar sem a necessidade de autorização judicial, tendo em vista, que trata-se de crimes ou violação de políticas de uso do site, aplicativo ou servidor.

> Passados mais de dois anos da entrada em vigor do Marco Civil, o tema da responsabilidade dos provedores ganhou os tribunais e o texto da lei foi progressivamente sendo aplicado e interpretado pelas cortes brasileiras. A partir dessa experiência podemos apontar cinco questões importantes sobre responsabilidade civil na internet relacionadas ao artigo 19 do MCI. (TEFFÉ, 2017, p. 3).

Vale ressaltar ainda, que a partir da Lei 12.965/2014 (Lei do Marco Civil da Internet), que em alguns casos, a retirada de conteúdos é feita través ordem judicial, como por exemplo, discussão referente a autoria de uma publicação, contudo, casos de postagens de fotos íntimas por vingança podem ser retiradas do ar através de solicitação da vítima, site ou aplicativo.

2.1.3 Marco Civil da internet e competência jurídica

É importante apontar que, com Marco Civil da Internet e suas regulamentações, vieram também as indicações da competência pra julgar as demandas relativas as violações de direitos, assim, tornou-se competentes os Juizados Especiais para julgarem as demandas, ou seja, são os responsáveis por sentenciar ilegalidade, inclusive, sobre a retirada ou não dos conteúdos questionados judicialmente

Assim, questões de ofensa à honra ou injúria do ambiente virtual poderão ser retiradas do ar através dos juizados especiais como aponta o artigo 19 da Lei 12.965/2014

> Art. 19, § 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais. (BRASIL, 2014).

Além disso, é interessante apontar que a competência independe da localização do provedor do acesso à internet, ou seja, o lugar da consumação da ilicitude deverá ser aquele estabelecido nos parâmetros do artigo 70 do Código de Processo Penal, assim, “a competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução”. (BRASIL, 1941).

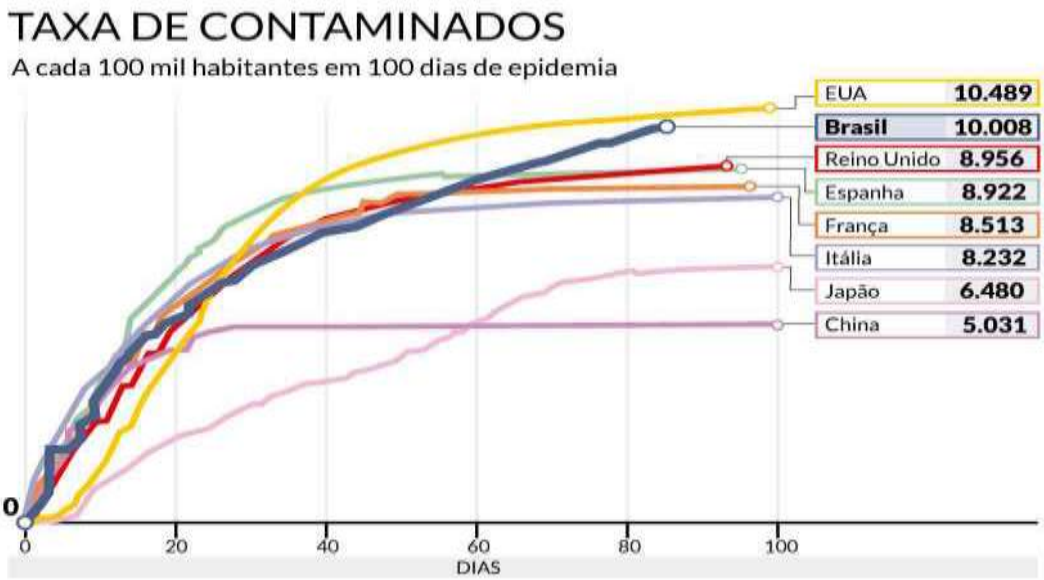
3 CRIMES CIBERNÉTICOS DURANTE A PANDEMIA DO COVD 19

3.1 PANDEMIA DO NOVO CORONA VÍRUS

A pandemia do novo corona vírus foi justamente um “evento” planetário que atingiu milhares de pessoas em todo o mundo, pandemia essa conhecida pela sigla COVID-19, inclusive, começou a tomar proporções significativas a partir de janeiro de 2020 e junto com essa expansão, trouxe também uma diversidade de transtornos pelo mundo.

É interessante apontar, que em 100 (cem) dias das atividades do vírus no mundo, como mostra o gráfico abaixo, já era possível ver uma quantidade alarmante de casos em todo o planeta e que, gerou preocupações notórias, inclusive, por órgão de saúde de cunho internacional (ex. Organização Mundial de Saúde).

Gráfico 03: crescimento da pandemia em 100 (cem) dias



Fonte: Dias (2020).

Segundo pesquisas (DIAS, 2020), as infecções tiveram início na China e tomaram proporções alarmantes em uma escala planetária no mundo, onde se fez necessária a utilização da quarentena em uma tentativa de diminuir os efeitos do COVID-19, atitudes essas, utilizadas praticamente em todos os países que sofrem com a contaminação.

> O primeiro caso da pandemia pelo novo coronavírus, SARS-CoV2, foi identificado em Wuhan, na China, no dia 31 de dezembro do último ano. Desde então, os casos começaram a se espalhar rapidamente pelo mundo: primeiro pelo continente asiático, e depois por outros países. Em fevereiro, a transmissão da Covid-19, nome dado à doença causada pelo SARS-CoV2, no Irã e na Itália chamaram a atenção pelo crescimento rápido de novos casos e mortes, fazendo com que o Ministério da Saúde alterasse a definição de caso suspeito para incluir pacientes que estiveram em outros países. No mesmo dia, o primeiro caso do brasil foi identificado, em São Paulo. (BARRETO, 2020, p. 9).

Uma das primeiras medidas tomadas pelo governo chinês foi justamente colocar o país em isolamento social (*lockdown*), tal medida colocou a população chinesa em casa, ou seja, fichou-se as fábricas, o comércio local e também, restrições referentes a visitação de amigos e parentes.

Outra medida que o governo chinês decretou foi justamente a suspensão temporária da venda de animais considerados selvagens, tendo em vista, que as autoridades sanitárias e governamentais tinham suspeitas de que o vírus tinha relação com a comercialização de animais exóticos.

> As medidas de prevenção e controle foram implementadas rapidamente, desde os estágios iniciais em Wuhan e outras áreas-chave de Hubei até o nível nacional. As medidas adotadas podem ser divididas em três fases. (RIBEIRO, 2020, p. 3).

Dentre essas medidas, tem-se a suspensão das atividades nas Universidades e Faculdades e da circulação de transportes que não fossem essenciais. Além disso, houve também o monitoramento dos viajantes e verificação da temperatura corporal.

Mesmo diante de todos esses cuidados, o vírus causou problemas diversos na saúde, comércio e economia do país, além disso, não conseguiram conter que o vírus chegasse a outras regiões do planeta, chegando assim, na Ásia e Europa, o continente europeu causa preocupação. Na Itália, país esse com um grande número de idosos no mundo, passou e ainda passa restrições.

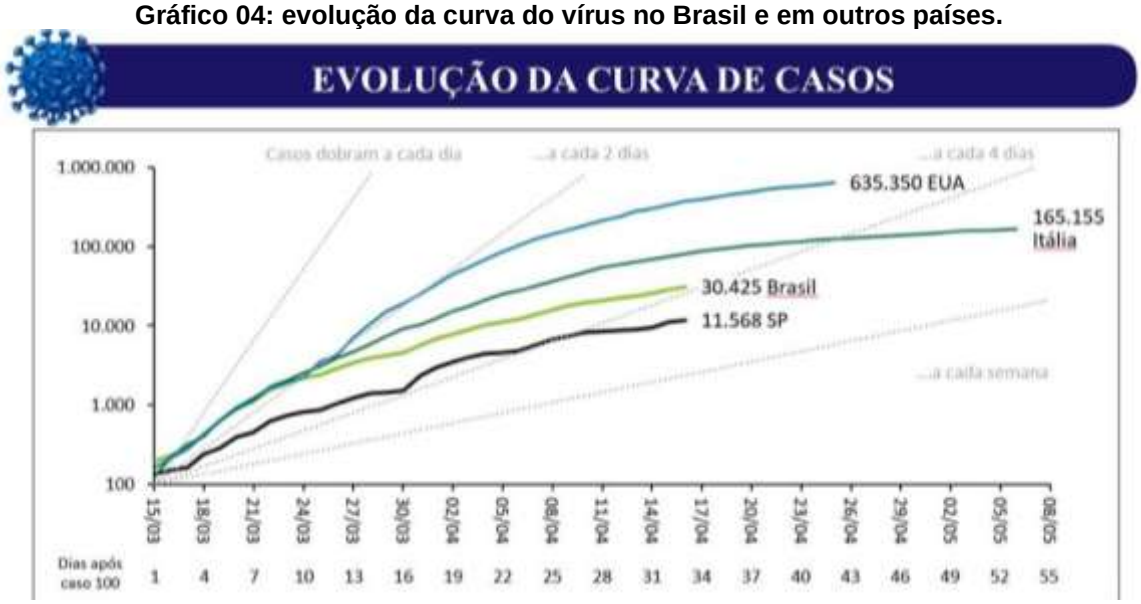
> Na Espanha, os números também estão aumentando rapidamente. O número de infectados passa dos 11 mil. Bares, restaurantes, serviços de entrega, escolas e faculdades estão fechados. Por outro lado, o Reino Unido segue com a estratégia de não interromper suas atividades, pedindo o isolamento apenas de idosos e grupos de risco. Os jovens seriam responsáveis por adquirir uma “imunidade de grupo”, ou seja, eles seriam infectados, ficariam resistentes, e não passariam para os outros. Cientistas argumentam que milhares de

> pessoas podem ser prejudicadas por causa da medida. (FIORATTI, 2020, p. 1).

Assim, a pandemia no novo coronavírus chegou ao Brasil e da mesma forma que nos outros países, trouxe um cenário de devastação de serem humanos, chegando a níveis alarmantes e que necessitou de ações rápidas do governo atual. Desta maneira, São Paulo foi o Estado brasileiro em que registrou o primeiro caso de COVID-19 no país.

Nos períodos inicias da pandemia no Brasil, foi possível visualizar números crescentes entre o dia 15 (quinze) de marco e 17 (dezessete) de abril, como mostra a curva ascendente do vírus no Brasil.

Gráfico 04: evolução da curva do vírus no Brasil e em outros países.



Fonte: Borges (2020).

Inclusive, foi no Estado de São Paulo que concentrou o maior número de casos no pais, depois, o vírus se espalhou pelos estados brasileiros e causou enormes problemas sociais e econômicos, tendo em vista, que os brasileiros passaram cerca de quatros meses em isolamento social.

3.2 CRIMES CIBERNÉTICOS NO PERÍODO DA PANDEMIA DO NOVO CORONAVÍRUS

Com o crescimento do isolamento social por conta da pandemia, ou seja, as pessoas passaram a ficar mais tempo em casa e consequentemente, houve uma aumento significativo da utilização das redes da internet. Desta maneira, houve também um crescimento de “oportunidades” relativas aos ataques dos criminosos no mundo virtual.

Nesta perspectiva, subiu drasticamente as práticas de crimes virtuais ou crimes cibernéticos no período da pandemia.

> O número de vítimas de crimes praticados pela internet aumentou drasticamente no período de pandemia. O aumento do tempo de tela — período em que as pessoas passam conectadas — e os novos comportamentos impostos em função do novo coronavírus, como maior adesão da população às compras pela internet, têm contribuído para a ação de criminosos. (FONSECA, 2020, p. 3).

Conforme aponta a Polícia Civil do Distrito Federal, ocorreu no período que corresponde a março e junho deste ano (2020), um crescimento assustador do crimes de estelionatos através da internet, ou seja, aumenta de 198,95% e os furtos através de fraudes na internet aumentaram 310,97% (FONSECA, 2020, p. 3), números que causam espanto e a necessidade de cuidados por parte dos internautas.

Essa realidade do Distrito Federal se configura também em muitos estados brasileiros, além disso, a sociedade vive um período que nunca foi enfrentando anteriormente, inclusive, vive-se um momento de incertezas (econômicas e de saúde) e ainda assim, tem-se que enfrentar os ataques cibernéticos em um período tão difícil para a população mundial.

> A determinação da quarentena, o isolamento social, o desemprego, a autorização para cortes de salários e jornada de trabalho reduzida, a dificuldade para obtenção do auxílio emergencial do Governo Federal, tudo somado à diminuição de investimento em policiamento, causado, inclusive, mas não se limitando, pela baixa arrecadação de impostos em razão da crise, geram um ambiente propício a prática de crimes, mas, de todos, um em específico cresce: o cibernético. (RIBEIRO, 2020, p. 2).

As condições atuais, ou seja, lockdown, desemprego, cortes salariais, redução da carga horária e problemas no sistema de auxilio emergencial, gerou um ambiente ideal para as práticas de crimes cibernéticos relacionados a questões financeiras, assim, os criminosos “andam” a procura de vítimas em potencial nesta pandemia do COVID-19.

Infelizmente há uma grande correlação entre a economia com a criminalidade, na verdade, essas correlação já vem de muitos tempos atrás

> Não é de agora que se correlaciona economia e criminalidade. É um tema complexo, multifacético e polêmico, mas defendido por muitos estudos das ciências criminais, como a Teoria Econômica do Crime proposta por Gary S. Becker, economista ganhador do prêmio Nobel de Economia em 1992, resumida no entendimento de que o agente criminoso avalia e confronta, entre outros aspectos, os potenciais ganhos resultantes da ação criminosa pelo salário alternativo no mercado de trabalho. (RIBEIRO, 2020, p. 2).

Desta maneira, preferindo o salário da criminalidade em relação as alternativas de salários do mercado brasileiro, atrelado as crises econômicas, isolamento social, fechamento de fronteiras que prejudicam o tráfico de drogas, surgiu na pandemia novos padrões para a prática de crimes virtuais, assim, utilizam o home office para agir de forma ilícita. Essa modalidade é conhecida como crimes cibernéticos.

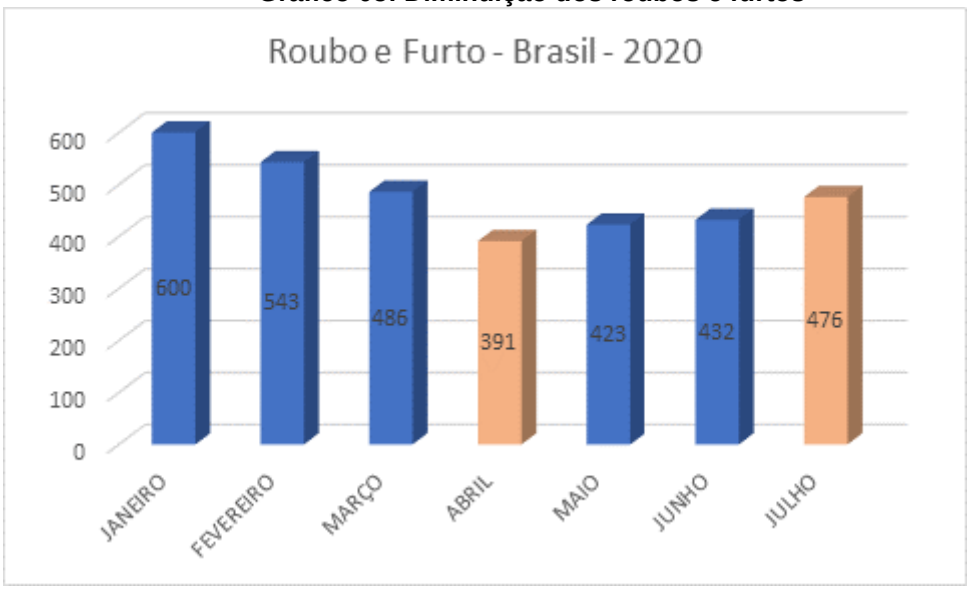
Sendo assim, espalham vírus, violação de sistemas, comentem fraudes, furtam dados e dão golpes através da redes sociais e por intermédio de ligações feitas a possíveis vítimas, inclusive, utilizam infelizmente, artifícios que convencem suas vítimas que já estão fragilizadas pelos efeitos da pandemia no Brasil.

> Em um mundo onde a tecnologia está cada vez mais avançada, crimes virtuais ganham espaço nas redes, fazendo várias vítimas diariamente. Os famosos golpistas estão sempre atentos, principalmente em um momento delicado como esse em que vivemos. A pandemia da Covid-19 trouxe ao mundo pânico, medo, incertezas e desinformação. Em consequência do isolamento social, as pessoas estão cada vez mais conectadas e acabam correndo mais riscos. Ao pagar uma conta, ao fazer uma compra pela internet ou até mesmo ao acessar links, é preciso cuidado absoluto, pois é nessas horas que os bandidos entram em ação. (RIZZO, 2020, p. 7).

Diante da pressa das empresas em retomar o funcionamento, paralisados em virtude do isolamento social, atrelado a necessidade de manter os funcionários e colaboradores trabalhando em home office, assim, não houve tempo, a princípio, de garantir a segurança necessária para que os colaboradores não fossem vítimas de ataques virtuais por parte criminosos cibernéticos.

Assim, tornou-se extenso os números de crimes virtuais cometido por esses criminosos especializados em violar sistemas e causar problemas a sociedade no período da pandemia no Brasil. Contudo, houve uma diminuição dos percentuais relacionados a roubos e furtos

Gráfico 05: Diminuição dos roubos e furtos



Fonte: Revista Apólice (2020)

Desta maneira, pode-se observar no gráfico acima que houve uma diminuição nos números referentes aos roubos e furtos no período que correspondem fevereiro à junho relacionados com o mês de janeiro.

Outros dados importantes e que se faz necessário, diz respeito a três cidades do Estado de São Paulo, ou seja, por mais que tenha havido uma redução de alguma modalidade de crimes, porém, outras ainda continuaram com percentuais crescentes ou iguais ao ano passado.

Tabela 03: diminuição e crescimento de alguns crimes

CRIMES	ARUJÁ		STA ISABEL		IGARATÁ	
	2019	2020	2019	2020	2019	2020
ROUBOS	177	156	63	24	14	7
FURTOS	338	242	217	180	59	44
ESTUPRO	25	13	11	19	2	3
HOMICÍDIO	3	4	2	3	1	1
TOTAL	543	415	293	226	76	55
REDUÇÃO %	23,6%		22,8%		27,6%	
A tabela leva em consideração os crimes registrados entre janeiro e julho de 2020 e o mesmo período de 2019						

Fonte: Jornal Ouvidor (2020)

Assim, paralelamente ao crescimento dos crimes cibernéticos no Brasil, houve também a diminuição dos números de roubos e furtos nos estados brasileiros, realidade que veio atrelada ao *lockdown* (isolamento social), tal realidade é apontada também pelo corregedor nacional de Justiça, ou seja. Ministros Humberto Martins

> O isolamento social decorrente da epidemia de Covid-19 fez cair significativamente o número de roubos e furtos nas cidades brasileiras, devido à baixa circulação das pessoas, mas abriu espaço para o desenvolvimento de outras práticas criminosas, como os crimes cibernéticos. [...] os criminosos, percebendo o uso mais intenso da internet por grande parte da população mundial, procuraram se adaptar rapidamente à nova realidade, para cometer fraudes eletrônicas. (MARTINS, 2020, p. 02).

Sendo assim, ver-se que há uma percepção dos criminosos em relação ao uso da internet pela população mundial diante da pandemia, ou seja, os criminosos entenderam que há um volume muito alto de acesso as redes mundiais de computadores e passaram a atuar nesta área, tendo como objetivos adquirir vantagens econômicas.

Desta maneira, procuram se adaptar e se especializar à essa nova realidade mundial, assim, passaram a praticar fraudes eletrônicas. “Cabe ao Estado brasileiro aprimorar seu arcabouço normativo para impedir que esses crimes sejam praticados, evitando prejuízos financeiros e patrimoniais às pessoas, às empresas e ao próprio poder público” (MARTINS, 2020, p. 02).

> Uma característica do crime cibernético é a inexistência de fronteira territorial. A vítima pode estar em Goiânia e o autor em outro país. Somente a investigação delimitará como será feita a abordagem. A conta beneficiada, que recebeu o dinheiro, determina o local de investigação. Uma vítima pode estar no Ceará, por exemplo, enquanto a conta aqui em Goiás, assim, nós investigaremos. (PINHEIROS, 2020, p. 4).

Essa inexistência de fronteira tem elevando os incides dos crimes cibernéticos na pandemias do COVID-19, ou seja, já havia uma crescimento antes da pandemia como mostra o capítulo primeiro desta pesquisa acadêmica, mostrando números preocupantes.

Nesta perspectiva, já era notório o crescimentos dos crimes virtuais e que, com a chegada do coronavírus no Brasil, veio também um aumento de 200 (duzentos) por cento dos crimes cibernéticos entre janeiro e abril, elevando ainda mais o percentuais.

> Segundo levantamento de empresa especializada em segurança digital, os crimes cibernéticos aumentaram mais de 200%, entre janeiro e abril deste ano. Para se ter ideia do tamanho, foram registrados mais de 14 milhões de acessos e compartilhamentos de links maliciosos com a palavra coronavírus. (PINHEIROS, 2020, p. 4).

Há diversos casos emblemáticos envolvendo crimes virtuais, como por exemplo, uma professora de 36 (trinta e seis) anos de idade que foi vítima de criminosos do mundo virtual e que passou a fazer parte das estatísticas.

Essa professora recebeu várias ligações de pessoas perguntando se ela estava pedido ajuda financeira em um grupo de WhatsApp para ajudar em diversas questões escolares, nesta hora, a professora percebeu que tinha cedo vítima de uma golpe cibernético

> A professora M. (ela não quis que o nome fosse publicado) não foi pega necessariamente neste tipo de golpe, mas em um propício para o momento de isolamento social em período de pandemia: em compra online. Ela comprou um produto em uma grande loja de varejo, que foi entregue com defeito. No momento de fazer a reclamação entrou em um canal não oficial da loja e pediram um número de protocolo a ser enviado por SMS. Ao repassar, o número de WhatsApp dela foi sequestrado. (PINHEIROS, 2020, p.1).

Depois de conseguir o número de celular da professora, os criminosos passaram a dar golpes utilizando o nome da professora, ou seja, se passaram por ela com o objetivo de pedir dinheiro as pessoas que faziam parte do ciclo de amizades da professora.

A professora ainda afirmou que “é uma dor de cabeça. Pois tive que bloquear meu chip de celular e pedir o bloqueio do aplicativo, que só terei acesso daqui a no mínimo sete dias. Tudo por falta de atenção”.

Um dos principais fatores que impulsionam as ações criminosas na pandemia é justamente a falta de atenção dos internautas ao fazer comprar em lojas virtuais e não tomar cuidados simples, como por exemplo, manter atualizado o antivírus do computador.

Uma outra forma de aplicar golpes, usado também durante a pandemia do coronavírus, foi justamente a falsificação de boletos bancários enviados por e-mail, sendo assim, a vítima pensa que está pagando um boleto da empresa a qual contraiu uma dívida ou comprou algo nesta modalidade, quando na verdade, está sendo mais uma vítima de golpes cibernéticos.

Diante disso, se faz necessário alguns cuidados com os boletos bancário, ou seja, verificar alguns dados das empresas emissora e do titular do boleto (logotipo, códigos e etc), como mostra a figura abaixo.

Figura 04: Dados importantes à serem analisados no boleto

Fonte: EXTRA (2019).

Se faz necessário analisar esses dados para reconhecer uma possível fraude e evitar transtornos, ao analisar esses dados será possível verificar que os golpistas cometem alguns pequenos erros na hora de adulterar o boleto. Assim, poderá haver

um logotipo diferente da utilizada pela instituição financeira responsável, além disso, verificar se os três primeiros números do código de barra é igual ao código do banco.

Recentemente, foi noticiado pela mídia que o STJ passou a fazer parte das estatísticas de crimes cibernéticos, ou seja, a primeira impressão que se tinha era que os telefones e a internet estariam com problemas técnicos. Contudo, a Polícia Federal foi acionada para abriu um inquéritos para averiguar a situação, tendo em vista que tratava-se precauções, no entanto, a Polícia Federal e o Comando de Defesa Cibernética do Exército, acabaram constatando que tratava-se de ataque de um hacker.

Neste ataque, o hacker conseguiu bloqueou e criptografar dados guardados nos computadores do STJ.

> Um ministro da corte ouvido pela ConJur contou que o hacker não teve acesso aos arquivos e processos que estão guardados em nuvem. Com isso, o hacker conseguiu bloquear e criptografar apenas os dados que estão guardados nos computadores. Informações preliminares indicam que o ataque foi localizado vindo de uma empresa particular estrangeira e estava sendo programado havia três meses. (VALENTE, 2020, p. 2).

Além deste, a também a grande possibilidade do Tribunal Regional Federal 1ª Região (TRF-1) ter cedo atacado por um hacker, onde semelhantemente ao caso do STF, o sistema ficou fora do ar no dia 27 de novembro de 2020, contudo, ainda a Polícia Federal não confirmou se tratava-se de ataques ao sistema do TRF-1, pois as investigações estão em andamento.

Portanto, esses e outros casos de crimes virtuais são vistos diariamente na mídia e que, foi intensificado com a pandemia do COVID-19, assim, se faz necessária uma atenção das autoridades governamentais e também mais cuidado por parte da população para evitar transtornos gerando pelo coronavírus.

CONSIDERAÇÕES FINAIS

Tendo em vista as discussões desta pesquisa acadêmica, verificou-se a confirmação de algumas premissas e que serão abordadas a seguir. Desta maneira, verificou-se que as diversas facilidades do acessar à internet atrelados aos valores acessíveis dos computadores e smartphones, fizeram surgir um crescente significativos de usuários do mundo virtual e também as facilidades para se relacionar, trabalhar e estudar.

Porém, essas facilitações proporcionadas pelo mundo virtual veio repletos de incidências de crimes cibernéticos, ou seja, a utilização de meios eletrônicos e tecnológicos para praticar crimes no mundo virtual.

Desta forma, observou-se que as condutas criminosas no mundo virtual são diversas, a saber, incidências de crimes contra a honra, pedofilia, divulgação indesejadas de fotos e vídeos, furto de dados pessoais e tantos outros. Inclusive, há uma grande dificuldades de identificação e punição, onde as vítimas são prejudicadas ou constrangidas.

Contudo, é possível observar que a maioria deste crimes que são praticado encontra-se respaldo no Código Penal brasileiro, ou seja, mesmo uma tipicidade ocorra no meio cibernético, porém, há ainda dificuldade de combater os crimes praticas no mundo virtual.

Diante disso, verificou-se que há uma grande necessidade de legislações ou normas específicas de combate aos crimes praticados ambiente virtual, inclusive, a edição de lei temporária para punir crimes cibernéticos nos períodos de crises, onde torna-se um ambiente mais propício às práticas de crimes virtuais.

Tal realidade, pode ser comprovada na atual crise sanitária (COVID 19), desta forma, o Brasil viu-se obrigado a paralisar as maioria das atividades econômicas e sociais, restando apenas o funcionamentos das atividades essências, assim, as empresas tiveram que fechar as postas e esperar a pandemia passar.

No entanto, algumas atividades tiveram condições de continuar de forma virtual, assim, empresas da área de educação e varejo continuam suas atividades através de plataformas online e seus funcionários passaram a trabalhar em home office durante a quarentena da pandemia.

Porém, as empresas não tiveram tempo e nem condições rápidas de pensar sobre possíveis ataques de criminosos no mundo virtual, desta forma, houve uma crescimento significativo de ataques durante a pandemia, assim, os criminosos se aproveitaram da conjuntura atual (pandemia no novo coronavírus - COVID 19).

REFERÊNCIAS

BARRETO, Clara. **Coronavírus: tudo o que você precisa saber sobre a nova pandemia.** 2020. Disponível em: https://pebmed.com.br/coronavirus-tudo-o-que-voce-precisa-saber-sobre-a-nova-pandemia/#:~:text=O%20primeiro%20caso%20da%20pandemia,e%20depois%20por%20outros%20pa%C3%ADses. Acesso em: 05 de novembro de 2020.

BRAIDA, Fernando Henrique Menezes da Silva. **Crimes cibernéticos: tipificação e legislação brasileira.** 2020. Disponível em: http://www.conteudojuridico.com.br/consulta/Artigos/54506/crimes-cibernticos-tipificao-e-legislao-brasileira. Acesso em: 03 de novembro de 2020.

BORGES, Beatriz. **Curva de gráfico de casos de coronavírus em SP cresce abaixo da média do Brasil, diz governo.** Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2020/04/17/curva-de-grafico-de-casos-de-coronavirus-em-sao-paulo-cresce-abaixo-da-media-do-brasil-diz-governo.ghtml. Acesso em: 05 de novembro de 2020.

CORREA, Flavia Cristina Jeronimo. **Crimes contra a honra nas redes sociais.** 2015. Disponível em: https://flaviacristinajcorrea.jusbrasil.com.br/artigos/206759390/crimes-contra-a-honra-nas-redes-sociais. Acesso em: 02 de novembro de 2020.

CNJ. Crimes digitais: **o que são, como denunciar e quais leis tipificam como crime?.** 2018. Disponível em: https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/. Acesso em: 21 de outubro de 2020.

Christou, Edmond. **Ataques cibernéticos e a ameaça à economia global.** Disponível em: https://www.bloomberg.com.br/blog/ataques-ciberneticos-e-ameaca-economia-global/. Acesso em: 01 de novembro de 2020.

DA SILVA, Patrícia Santos. **Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais.** Brasília: Vestnik, 2015.

DIAS, Roger. **Brasil completa 100 dias de covid-19 com maior curva ascendente no mundo.** 2020. Disponível em: https://www.correiobraziliense.com.br/app/noticia/brasil/2020/06/04/interna-

brasil,861191/brasil-completa-100-dias-de-covid-19-com-maior-curva-ascendente-no-mun.shtml. Acesso em: 05 de novembro de 2020.

DIÁRIO DA REGIÃO. **Explosão de crimes cibernéticos.** 2019. Disponível em: https://www.diariodaregiao.com.br/_conteudo/2019/02/cidades/rio_preto/1141695-explosao-de-crimes-ciberneticos.html. Acesso em: 01 de novembro de 2020.

DUARTE, Adrienne. Crimes virtuais: **conceito e formas de investigação.** 2018. Disponível em: https://www.boletimjuridico.com.br/artigos/direito-penal/10382/crimes-virtuais-conceito-formas-investigacao#:~:text=55)%2C%20que%20conceitua%20os%20crimes%20virtuais%20da%20seguinte%20forma%3A&text=Profusas%20s%C3%A3o%20as%20denomina%C3%A7%C3%B5es%20para,bem%20simples%20de%20ser%20compreendido. Acesso em: 20 de outubro de 2020.

ESTADÃO DE MINAS. **Crimes cibernéticos disparam e expõem fragilidade tecnológica no Brasil.** 2020. Disponível em: https://www.em.com.br/app/noticia/politica/2019/08/04/interna_politica,1074689/crimes-ciberneticos-disparam-expoem-fragilidade-tecnologica-no-brasil.shtml. Acesso em: 21 de outubro de 2020.

EXTRA. **Golpe do falso boleto: veja como reconhecer.** 2019. Disponível em: https://extra.globo.com/noticias/economia/golpe-do-falso-boleto-veja-como-reconhecer-24151074.html. Acesso em: 06 de novembro de 2020.

FIORATTI, Caroline. **Wuhan, cidade onde o novo coronavírus surgiu, registra apenas 1 novo caso.** Disponível em: https://super.abril.com.br/saude/wuhan-cidade-onde-o-novo-coronavirus-surgiu-registra-apenas-1-novo-caso/. Acesso em: 05 de novembro de 2020.

FONSECA, Jaqueline**. Registros de golpes na internet crescem 310% no DF durante a pandemia.** Disponível em: https://www.correiobraziliense.com.br/cidades-df/2020/08/4868977-mais-golpes-na-pandemia.html. Acesso em: 05 de novembro de 2020.

GOMES, João. **A substituição do Homem pela Máquina.** 2020. Disponível em: http://mundoplanotp2uminho.pbworks.com/w/page/4857864/A%20substitui%C3%A7%C3%A3o%20do%20Homem%20pela%20M%C3%A1quina. Acesso em: 19 de outubro de 2020.

GRECO, Rogério. **Direito Penal do Equilíbrio – Uma Visão minimalista do direito penal**. Rio de Janeiro: Impetus, 2005.

JORNAL OUVIDOR. **Pandemia freou crimes, mas não converteu homicídios.** 2020. Disponível em: http://jornalouvidor.com.br/noticia/pandemia-freou-crimes-mas-nao-conteve-homicidios--/17446. Acesso em: 06 de novembro de 2020.

MACHADO, Jacqueline. **Crimes digitais: o que são, como denunciar e quais leis tipificam como crime?.** 2018. Disponível em: https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/. Acesso em: 19 de outubro de 2020**.**

MARTINS, Humberto. **Na epidemia, crime virtual tomou lugar de subtrações físicas.** 2020. Disponível em: https://www.conjur.com.br/2020-jun-18/epidemia-crime-virtual-tomou-lugar-subtracoes-fisicas. Acesso em: 06 de novembro de 2020.

MARTINS, Geiza. **O que é o Marco Civil da Internet?.** 2018. Disponível em: https://super.abril.com.br/mundo-estranho/o-que-e-o-marco-civil-da-internet/. Acesso em: 03 de novembro de 2020.

MACHADO, Lucyana A. **Crimes cibernéticos.** 2014. Disponível em: https://www.direitonet.com.br/artigos/exibir/8772/Crimes-ciberneticos. Acesso em: 02 de novembro de 2020.

MEORIN, Caio Badran Kalil. **Ransomware, extorsão digital.** Disponível em: https://monografias.brasilescola.uol.com.br/direito/ransomware-extorsao-digital.htm. Acesso em: 01 de novembro de 2020.

MUNDO ADVOGADOS. **Crimes cometidos nas redes sociais: conheça seus direitos.** Disponível em: https://www.mundoadvogados.com.br/artigos/crimes-cometidos-nas-redes-sociais-conheca-seus-direitos. Acesso em: 02 de novembro de 2020.

NOGUEIRA, Luiz. **Dados mostram o crescimento impressionante da internet em 10 anos**. Disponível em: https://olhardigital.com.br/noticia/dados-mostram-o-crescimento-impressionante-da-internet-em-10-anos/85914. Acesso em: 01 de novembro de 2020.

PINHEIROS, Eduardo. **Crimes cibernéticos prosperam durante pandemia de Covid-19.** Disponível em: https://www.jornalopcao.com.br/ultimas-noticias/crimes-ciberneticos-prosperam-durante-pandemia-de-covid-19-254215/. Acesso em: 06 de novembro de 2020.

VEIGA, Renato. **Crimes cibernéticos disparam e expõem fragilidade tecnológica no Brasil.** 2020. Disponível em: https://www.em.com.br/app/noticia/politica/2019/08/04/interna_politica,1074689/crimes-ciberneticos-disparam-expoem-fragilidade-tecnologica-no-brasil.shtml. Acesso em: 21 de outubro de 2020.

VITTA, Lucas de. **Interpol alerta para crescimento de crimes virtuais durante a pandemia.** 2020. Disponível em: https://valor.globo.com/mundo/noticia/2020/08/04/interpol-alerta-para-crescimento-de-crimes-virtuais-durante-a-pandemia.ghtml. Acesso em: 21 de outubro de 2020.

VITORIANO, Larissa. **A lei tipifica crimes virtuais e altera artigos do código penal.** 2018. Disponível em: https://cpjur.com.br/lei-carolina-dieckmann/#:~:text=A%20Lei%2012.737%2F2012%20de,Brasileiro%20que%20trouxe%20muitas%20pol%C3%AAmicas.&text=O%20texto%20foi%20o%20primeiro,sem%20permiss%C3%A3o%20do%20seu%20dono. Acesso em: 03 de novembro de 2020.

REVISTA APÓLICE. **Roubo e furto de veículos cresceram 21,74% em julho.** 2020. Disponível em: https://www.revistaapolice.com.br/2020/08/roubo-e-furto-de-veiculos-cresceram-2174-em-julho/. Acesso em: 06 de novembro de 2020.

RIZZO, Carolina. **Crimes cibernéticos crescem durante a pandemia da COVID-19.** 2020. Disponível em: https://www.daquibh.com.br/crimes-ciberneticos-crescem-durante-a-pandemia-da-covid-19/. Acesso em: 05 de novembro de 2020.

RIBEIRO, Valéria Lopes. **A China e a pandemia do Covid-19 - das medidas de contenção à estratégia global.** Disponível em: https://www.cartamaior.com.br/?/Editoria/Pelo-Mundo/A-China-e-a-pandemia-do-Covid-19-das-medidas-de-contencao-a-estrategia-global/6/46992. Acesso em: 05 de novembro de 2020.

RIBEIRO, Caroline. **O aumento dos crimes cibernéticos e a pandemia da Covid-19.** Disponível em: https://www.conjur.com.br/2020-abr-29/caroline-ribeiro-aumento-crimes-ciberneticos-pandemia. Acesso em: 05 de novembro de 2020.

ROSSINI, Augusto Eduardo de Souza. **Informática Telemática e Direito Penal**. São Paulo: Memória Jurídica 2004.

RODIRGUES, Fernando. **Denúncias de crimes cibernéticos aumentaram 109,9% em 2018, diz associação.** Disponível em: https://www.poder360.com.br/justica/denuncias-de-crimes-ciberneticos-aumentaram-1099-em-2018-diz-associacao/. Acesso em: 01 de novembro de 2020.

SANCHES, Ademir Gasques. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** 2018. Disponível em: https://jus.com.br/1756990-ademir-gasques-sanches/publicacoes. Acesso em: 21 de outubro de 2020.

SANTOS, Gabriel dos. **Saiba como hackers podem invadir dispositivos móveis com ataques remotos.** Disponível em: https://blogbrasil.westcon.com/saiba-como-hackers-podem-invadir-dispositivos-moveis-com-ataques-remotos#:~:text=Saiba%20como%20hackers%20podem%20invadir%20dispositivos%20m%C3%B3veis%20com%20ataques%20remotos,-Compartilhar&text=Cibercriminosos%20descobriram%20como%20invadir%20smartphones,para%20a%20seguran%C3%A7a%20de%20dados. Acesso em: 03 de novembro de 2020.

SCHMIDT, Guilherme. **Crimes Cibernéticos.** 2015. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. Acesso em: 20 de outubro de 2020.

SHINCARIL, Fernando. **Liberdade de Expressão e Anonimato na Internet.** Disponível em: https://schincariolfernando.jusbrasil.com.br/artigos/251634616/liberdade-de-expressao-e-anonimato-na-internet. Acesso em: 03 de novembro de 2020.

TEFFÉ, Chiara Spadaccini. **Responsabilidade dos provedores por conteúdos de terceiros na internet.** 2017. Disponível em: https://www.conjur.com.br/2017-jan-23/responsabilidade-provedor-conteudo-terceiro-internet. Acesso em: 04 de novembro de 2020.