Pró-Reitoria Acadêmica
Curso de Direito
Trabalho de Conclusão de Curso

CRIMES CIBERNÉTICOS

Autor: Iago Felipe de Souza Santos
Orientador: Dr. Nefi Cordeiro

Brasília - DF
ano 2021

IAGO FELIPE DE SOUZA SANTOS

CRIMES CIBERNÉTICOS: EFICIÊNCIA PENAL NOS CRIMES CIBERNÉTICOS

Artigo apresentado ao curso de Graduação em Direito da Universidade Católica de Brasília, como requisito parcial para obtenção do Título de Bacharel em Direito

Orientador: Dr. Nefi Cordeiro

Coorientador: Profª Analicia Ortega Hartz

Brasília
ano 2021

Artigo de autoria de Iago Felipe de Souza Santos, intitulada “EFICIÊNCIA PENAL NOS CRIMES CIBERNÉTICOS, apresentada como requisito parcial para obtenção do grau de Bacharelado em Direito da Universidade Católica de Brasília, em 2021, defendida e aprovada pela banca examinadora abaixo assinada:

_____

Prof. Dr. Nefi Cordeiro
Orientador
Direito– UCB

_____

Prof. Dr. José Eduardo Sabo Paes
Direito– UCB

Brasília
ano 2021

AGRADECIMENTOS

Primeiramente devo agradecimentos ao criador por permitir que acordemos todos os dias com vida e saúde em um momento de instabilidade global. Depois, agradeço à minha mãe por sempre estar presente e sempre ajudando para minha satisfação acadêmica. Da mesma forma, agradeço a todos os meus familiares que puderam me ajudar nessa jornada acadêmica, e por fim, meus professores que me guiaram nessa jornada, assim como meu orientador e coorientadora.

Qualquer um pode julgar um crime tão bem quanto eu, mas o que eu quero é corrigir os motivos que levaram esse crime a ser cometido.

Confúcio

EFICIÊNCIA PENAL NOS CRIMES CIBERNÉTICOS

CRIMINAL EFFICIENCY IN CYBER CRIMES

IAGO FELIPE DE SOUZA SANTOS[1]

Resumo:
Trata-se de um estudo que tem como objeto um dos crimes que está em ascensão atualmente, os crimes cibernéticos. O estudo visa compilar a atual legislação sobre crime digital, apontar suas características, peculiaridades, crimes tipificados e suas possíveis falhas na eficiência do combate aos crimes cibernéticos. Apontará também estatísticas atualizadas sobre os diversos crimes cibernéticos no Brasil e no mundo. Também visa apontar os fatores e motivos que levam ao aumento desse tipo de crime, bem como, apresentar ferramentas, soluções e dificuldades na investigação do crime digital.

Palavras-chave: Trabalho acadêmico. Referência. Estrutura. Artigo científico. Direito Digital. Lei Digital. Crime Digital. Crime cibernético. Criptomoedas. Eficiência penal. Logs. Deep Web. Investigação de Crime digital.

Abstract:
This is a study that has as its object one of the crimes that is on the rise today, cyber crimes. The study aims to compile the current legislation on digital crime, to point out its characteristics, peculiarities, typified crimes and its possible flaws in the efficiency of the fight against cyber crimes. It will also point out updated statistics on the various cyber crimes in Brazil and in the world. It also aims to point out the factors and reasons that lead to the increase of this type of crime, as well as to present tools, solutions and difficulties in the investigation of digital crime.

Key words: Academic work. Reference. Structure. Scientific article. Right Digital. Digital Law. Digital Crime. Cyber crime. Cryptocurrencies. Penal efficiency. Logs. Deep Web. Digital Crime Investigation.

1 TRATAMENTO PENAL NOS CRIMES CIBERNÉTICOS

1

No Brasil, são tímidas as leis que tratam sobre crime cibernéticos. Há pouco tempo que o legislador virou sua atenção aos crimes digitais aqui no Brasil. Dessa forma, a falta de resposta legislativa traz vários problemas e riscos para o mundo digital, gerando, na maioria das vezes, impunidade para esse tipo de crime.

Sendo assim, existem apenas três leis que procuram tipificar os crimes digitais no Brasil que são: LEI Nº 12.737/12 - lei Carolina Dieckmann; LEI Nº 12.965/14 - Marco civil da internet; e LEI Nº 13.709 – lei geral de proteção de dados (LGPD).

Com o crescimento exponencial da internet, cada vez mais ambientes domésticos tendo acesso ao ambiente digital. Conforme De oliveira (2020, p. 13), o crime cibernético também cresceu a passos largos.

Dessa forma, nota-se que a lei brasileira sobre o crime digital ainda é muito rasa. Muitas condutas criminosas ainda faltam regulamentação, tipificação penal e proporcionalidade da pena. É preciso um debate sério e técnico para que a legislação consiga acompanhar a dinamização do crime digital.

1.1 LEI CAROLINA DIECKMANN

Famosa aqui no Brasil, Carolina Dieckmann teve suas fotos íntimas e dados indevidamente expostos na internet, concomitante no tempo que em o projeto da lei Nº 12.737/12 tramitava na câmara dos deputados, rapidamente, a lei ficou conhecida pelo nome da atriz.

Com a publicação da lei em 2012, foi inserido no código penal brasileiro o crime de invasão a dispositivo informático no artigo 154-A do código penal. Dessa forma, tornou crime a conduta de invadir dispositivo informático com o dolo específico de obter, adulterar ou destruir os dados ali contidos, vale lembrar que é parte essencial do tipo a quebra de dispositivo de segurança.

A lei também alterou os artigos 266 e 298 do código penal, trazendo mais condutas para o crime de interrupção de serviço e para o crime de falsificação de documento particular.

Apesar de prever algumas qualificadoras e aumentos de pena, essa lei sofreu fortes críticas devido a pena ser muito branda, possuir um texto ambíguo, e faltar alguns tipos penais que estavam previstos no projeto. Porém, foi uma lei pioneira no Brasil quanto a esse tipo de crime. Precisa ser lapidada para que acompanhe a dinamização do crime digital, pois a quantidade de pontos negativos está superando a quantidade de pontos positivos da lei. (PAULINO, 2018, p.37).

1.2 MARCO CIVIL DA INTERNET

A lei 12.965/14, de acordo com sua própria ementa no site do planalto, traz princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Dessa forma, essa lei diz sobre várias diretrizes a serem seguidas pelo mundo digital brasileiro, sendo de grande importância para o estudo dos crimes digitais.

Segundo César e Junior (2017), um dos princípios mais importantes que esta lei regularizou no Brasil foi o da neutralidade de rede, onde podemos ver seu conceito claramente descrito em seu artigo 9º a seguir:

> O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação. (BRASIL, 2014)

Na leitura do artigo supra, percebe-se que o marco civil da internet trouxe o princípio da neutralidade de rede, que proíbe provedores de restringir parte da rede, seja velocidade, seja entrega de pacotes.

1.3 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei geral de proteção de dados (LGPD), aprovada em 2018, visa criar um cenário de segurança jurídica para os documentos digitais. Ela identifica como dados pessoais qualquer informação que possa identificar direta ou indiretamente um indivíduo vivo, seja RG, CPF, IP, cookies, entre outros. (BARBOSA, 2020, p.20)

Dessa forma, a lei trouxe mais segurança sobre o tratamento a ser feito pelos dados das pessoas no mundo digital. Deve haver um consentimento mútuo entre cliente e servidor para que seja coletado dados pessoais na internet. Embora tardio, somente em 2018, foi um avanço muito importante para o cenário jurídico digital no Brasil.

É importante ressaltar que a lei também trouxe a figura do órgão responsável pela proteção de dados pessoais, que é Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

Destarte, fica claro a importância dessa lei para o combate aos crimes digitais. Dessa forma, é preciso lapidar as lacunas e otimizar o órgão responsável pelos dados digitais, pois, com os recentes e comuns mega vazamentos de dados no Brasil, é preciso mais do que nunca fortalecer essas instituições.

1.3 OUTRAS LEIS QUE PODEM TRATAR DE CRIMES DIGITAIS

De acordo com Adeneele (2012), o crime digital é classificado como próprio quando é essencialmente digital, ou pode ser classificado como impróprio quando o digital é apenas um meio para a consumação do crime. Dessa forma, há várias condutas que podem ser consideradas crimes cibernéticos, a seguir um rol exemplificativo de artigos penais que podem ser considerados crimes cibernéticos e suas respectivas penas:

1.3.1 Crimes digitais próprios:

Comentar, em chats, e-mails e outros, de forma negativa, sobre religiões e etnias (Art. 20, da Lei n. 7.716 /89) – Ocorre muito em redes sociais, e aplicativos de mensagens - Pena: reclusão de um a três anos e multa;

Inserção de dados falsos em sistema de informações (Art. 313-A, do Código Penal) é causado pelo próprio agente público responsável - Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa;

Modificação ou alteração não autorizada de sistema de informações - Art. 313-B, do Código Penal - Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.

1.3.2 Crimes digitais próprios:

Falsa identidade (art. 307, do Código Penal) – Quando o agente utiliza a internet para se atribuir falsa identidade, perfis falsos, etc - Pena - detenção, de três meses a um ano, ou multa;

Falsificação de cartão de crédito ou débito (Art. 298, §único, do Código Penal) – Quando o agente utiliza da internet para conseguir as informações do cartão da vítima – Pena - reclusão, de um a cinco anos, e multa.

Ameaça (art. 147, do Código Penal) – Quando o agente usa da internet para ameaçar a vítima, geralmente ocorre em redes sociais, fóruns de internet e aplicativos de mensagens – Pena - detenção, de um a seis meses, ou multa;

Divulgação de segredo (Art. 153, do Código Penal) - O agente divulga segredos da vítima por meio da internet para causar danos, ocorre muito em redes sociais Pena - detenção, de um a seis meses, ou multa, de trezentos mil réis a dois contos de réis;

Incitação ao crime (Art. 286, do Código Penal) – se consuma quando o agente utiliza da internet para incitar o crime - Pena - detenção, de três a seis meses, ou multa

Furto (Art. 155, do Código Penal) – pode se configurar quando o agente utiliza dos dados da vítima para retirar saldo bancário por meio da internet, dados esses que podem ser obtidos utilizando um keylogger (programa de computador que grava as teclas digitadas pelo usuário), por exemplo – Pena - reclusão, de um a quatro anos, e multa;

Estelionato (Art. 171, do Código Penal) pode acontecer quando o agente utiliza da internet para aplicar golpes - Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.

É de consenso que o meio digital é um reflexo do mundo físico. Portanto, o arcabouço jurídico já existente de crimes pode ajudar no combate aos crimes digitais impróprios. Porém é necessário adequar e complementar as leis já existentes para que possam dar eficiência jurídica proporcional aos crimes digitais.

2 DIFICULDADES ENFRENTADAS NO COMBATE AO CRIME CIBERNÉTICO E ESTATÍSTICAS

2.1 DO ATUAL CENÁRIO DIGITAL BRASILEIRO

Em 2019, de acordo com a pesquisa do comitê gestor da internet (CGI.br), o Brasil contava com 74% das pessoas com acesso à internet, ou seja, 134 milhões de pessoas possuem acesso, número esse que, nos dias atuais em 2021, deve ter aumentado significativamente. Dessa forma, tornou-se uma terra fértil para o crescimento exponencial de crimes digitais em todo o ciberespaço. O número de tentativa de fraudes, roubos de senhas, sites, contas, e dinheiro por meios digitais chegou a um número absurdo, tornando o Brasil o segundo país que mais sofre com esse tipo de crime:

> De acordo com um relatório da Norton Cyber Security, em 2017 o Brasil passou a ser o segundo país com maior número de casos de crimes

> cibernéticos, afetando cerca de 62 milhões de pessoas e causando um prejuízo de US$ 22 bilhões (De BRASIL, em São Paulo, 2018, p.1)

As penas brandas já evidenciadas em legislação supra, a dificuldade intrínseca de investigar crimes digitais, e a sensação de impunidade ainda existente torna o crime digital um dos tipos de crimes que mais crescem no Brasil (BORTOT, 2017). Até mesmo sites e bancos de dados governamentais sofrem com a falta de infraestrutura digital do governo e constantemente são alvos fáceis, atualmente, notícias deste tipo são corriqueiras no Brasil:

> Os recentes megavazamentos de dados
> Um deles tinha 223 milhões de números de CPF, acompanhado de informações como nome, sexo e data de nascimento, além de uma tabela com dados de veículos e uma lista com CNPJs (Cadastro Nacional de Pessoas Jurídicas). Essas informações circulam na internet de forma gratuita. (Do MEGAVAZAMENTO, 2021, p.1)
>
> O outro incluía, além dos 223 milhões de CPFs, informações sobre escolaridade, benefícios do INSS e programas sociais (como o Bolsa Família), renda, entre outras informações. Esse está sendo vendido por criminosos. (Do MEGAVAZAMENTO, 2021, p.1)

E o cidadão brasileiro que teve seu dado exposto não possui muito o que fazer, além de ficar atento a possíveis fraudes envolvendo seus dados.

2.1 DAS DIFICULDADES DE INVESTIGAÇÃO DO CRIME DIGITAL

O crime cibernético é intrinsecamente difícil de combater. Se não houver um gasto e esforço público em todas as esferas governamentais, esse cenário pode piorar muito mais.

Há várias formas de se praticar um crime cibernético, pode ser por meio de programas maliciosos, e-mails, grupos de debate, etc. O primeiro passo para o sucesso da persecução penal é procurar delimitar o crime cometido e a ferramenta utilizada pelo criminoso. (CAVALCANTE, 2015, p.6)

Diferentemente dos crimes comuns, os vestígios dos crimes digitais, segundo Cavalcante (2015), são difíceis de encontrar, de entender e são muito complexos, podem ser facilmente manipulados, apagados e modificados, todos esses fatores em conjunto com a anonimidade intrínseca da internet e a possibilidade de o sujeito do crime estar em qualquer lugar do mundo tornam o crime digital, muitas das vezes, um crime quase impossível de ser apurado. Geralmente, as vítimas sequer têm conhecimento de que foram vítimas desse tipo de crime.

2.2 FERRAMENTAS DISPONÍVEIS PARA COMBATER OS CRIMES CIBERNÉTICOS E SUAS FRAGILIDADES

O endereço de protocolo da internet (IP – internet protocol) é um dos principais vestígios que os investigadores procuram para encontrar o autor de um crime digital. O IP é uma sequência de números no qual é possível ter a localização física da máquina do usuário. (CAVALCANTE, 2015, p.8)

Porém, conforme diz Barreto e dos Santos (2019), existem várias ferramentas capazes de esconder o IP do usuário entre elas tem o serviço de VPN (o usuário terceiriza seu acesso ao site, o servidor acessa o site por ele e depois envia para ele os dados de forma criptografada). Um criminoso que utiliza um serviço que mascara o IP de sua máquina dificulta muito a investigação de um crime digital.

Os logs são arquivos onde são armazenados históricos de usos, data, hora, local de acesso, número de IP, etc. Vários sites que são acessados na internet comum utilizam vários tipos de logs. Ao possuir acesso aos logs, um investigador consegue ter acesso a várias informações que podem terminar no sucesso da investigação. (CAVALCANTE, 2015, p.7)

Entretanto, assim como o endereço de IP há ferramentas, segundo Barreto e dos Santos (2019), que são utilizadas para que os logs e os registros de acesso não sejam guardados. Um exemplo é a utilização do navegador TOR – ONION, neste navegador o usuário tem acesso a páginas totalmente criptografadas, e não passaram pelo processo de indexação feito por motores de busca comuns como o google (indexar é o ato de classificar o assunto da página para fácil acesso). Desse modo, o usuário tem acesso à deep web (conhecida como a internet do anonimato) e pode se tornar totalmente anônimo para realizar vários tipos de crimes.

O rastreamento de valor monetário é uma ferramenta importante para investigação de qualquer crime. Mediante uma quebra de sigilo bancário, o investigador tem acesso a valores e transações que podem ajudar na investigação de vários tipos de crimes, por exemplo, vantagens obtidas por meio de um estelionato digital. Porém, se esses valores forem transacionados por meio de moedas digitais, o investigador não consegue ter acesso ao dono da carteira digital utilizada na transação, motivo esse que muitos crimes digitais são consumados utilizando de moedas digitais – as famosas criptomoedas. (EGEWARTH, 2020, p. 28)

Portanto, pode-se observar que várias ferramentas que o investigador possui para procurar a autoria de um crime digital possuem vários modos de burlar, o que dificulta a investigação e a eficiência no combate ao crime digital.

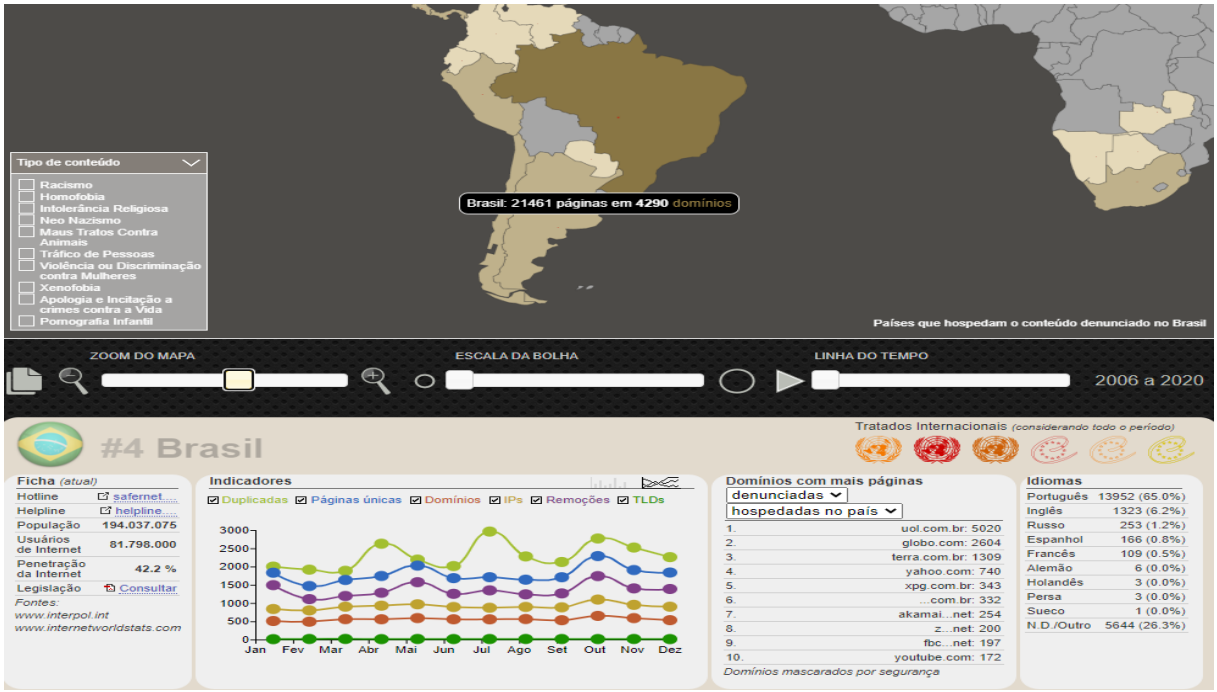
2.3 ESTATISTICAS E INDICADORES DE CRIMES DIGITAIS NO BRASIL

No mundo inteiro, o crime digital tem crescido de forma exponencial. Dados apontam que, hoje, o Brasil está entre os países que mais sofrem com os crimes digitais. No meio desse cenário caótico, o Brasil também está entre os primeiros quando se fala em prejuízos econômicos envolvendo crimes digitais.

2.3.1 Das páginas denunciadas por crimes digitais

Como não poderia ser diferente, o Brasil também está entre os primeiros países que hospedam páginas denunciadas por cometerem crimes cibernéticos, conforme dados a seguir:

Figura 1 – Número de páginas denunciadas por crimes digitais nos indicadores da central de denúncias de crimes cibernéticos



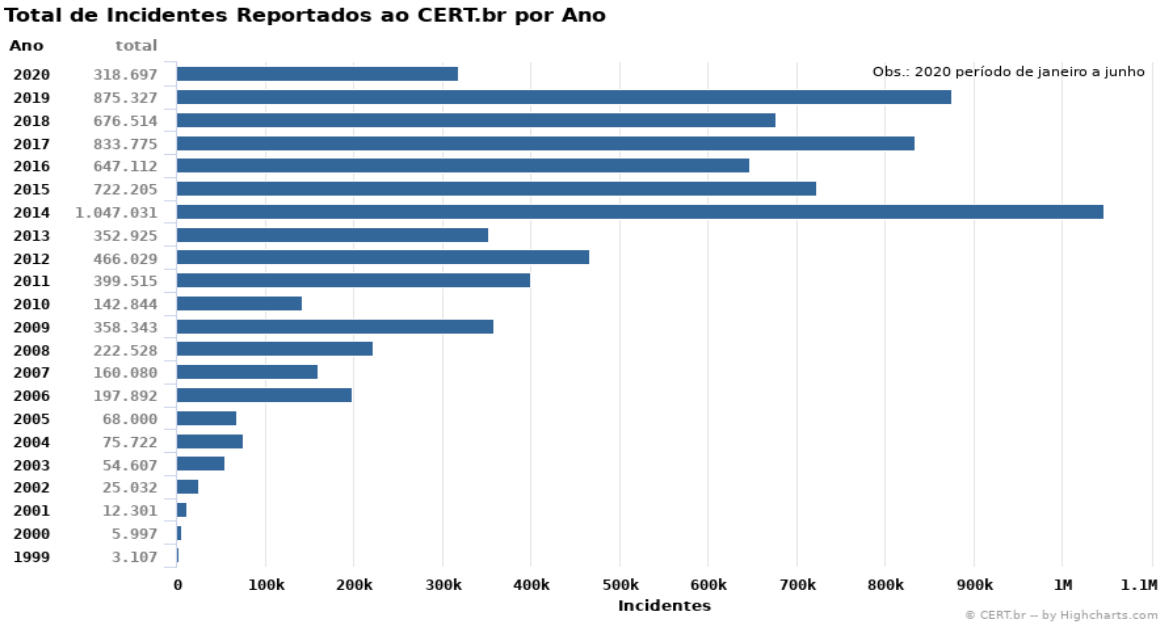
Fonte: https://indicadores.safernet.org.br/ , em parceria com safernet, ministério público federal, polícia federal, secretaria dos direitos humanos, senado federal e câmara dos deputados.

De acordo com os indicadores na figura 1, é possível perceber que o Brasil, no período entre 2006 a 2020, ostentou o quarto lugar de denúncias a páginas digitais que foram acusadas de praticar no meio digital um dos crimes a seguir: racismo; homofobia; intolerância religiosa; neonazismo; maus tratos contra animais; tráfico de pessoas; violência e discriminação contra as mulheres; xenofobia; apologia e incitação a crimes contra a vida; pornografia infantil.

Destarte, nota-se que o brasil ostenta o quarto lugar com 21.461 (vinte e um mil e quatrocentas e sessenta e um) páginas denunciadas a fazer esse rol de crimes no meio digital. O número é de se assustar. É preciso uma forte coordenação das forças de inteligência não só nacionais, mas também, internacionais, para coibir esse tipo de conduta criminosa.

2.3.2 Incidentes reportados

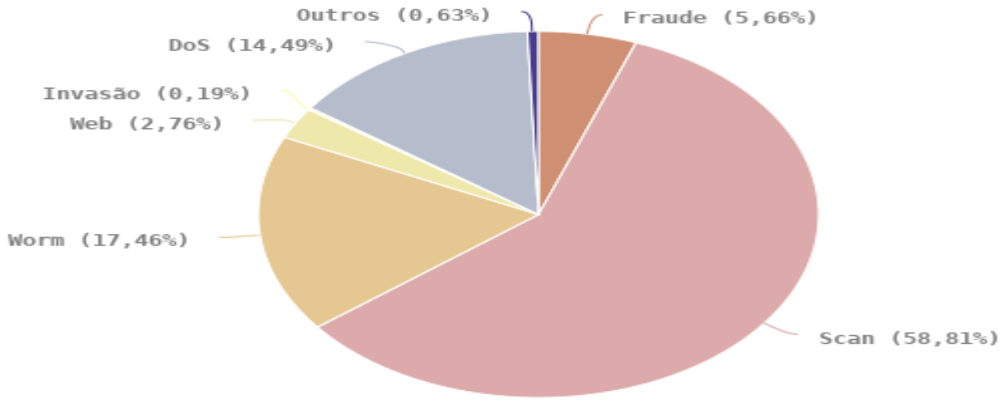
Figura 2 – total de incidentes de crimes digitais reportados ao CERT.br por ano



Fonte: https://www.cert.br/ Centro de Estudos, resposta e tratamento de incidentes de segurança no Brasil

Pode-se observar que os números não seguem uma relação linear perfeita, porém, a tendência é de crescimento, o ano de 2014 foi o ano em que mais teve incidentes de acordo com a figura 2.

Figura 3– tipos de incidentes reportados ao CERT.br de janeiro a junho de 2020



Fonte: https://www.cert.br/ Centro de Estudos, resposta e tratamento de incidentes de segurança no Brasil.

As estatísticas da figura 3 mostram que o ataque de scam é o que mais ocorre no Brasil com 58,81%. De acordo com o Cert.br (2020), Scam é o ato em que o criminoso faz varreduras na rede para procurar possíveis vítimas.

O ataque de Worm, em segundo lugar com 17,46%, é o ataque em que consiste numa invasão de ameaças replicantes automaticamente pela rede. (figura 3)

Em terceiro lugar, com 14,49%, está o ataque de negação de serviço (DoS) – esse ataque opera tirando do ar determinada página, serviço ou rede com muitos acessos simultâneos. (figura 3)

Portanto, ao ver os indicadores, nota-se que é preciso estudar os tipos mais comuns de crimes digitais no Brasil para que o investigador possa aumentar a eficiência penal desse tipo de crime.

2.3.2 Dos prejuízos econômicos relacionados a crimes digitais

O mundo inteiro assiste um crescente e exponencial aumento de prejuízos econômicos relacionados aos crimes digitais, conforme notícias a seguir:

> [...] o estudo conjunto da McAfee e do Centro de Estudos Estratégicos e Internacionais (CSIS) indica o tamanho do desafio. O levantamento diz que a cibercriminalidade terá um impacto de US$ 1 trilhão na economia global em 2020, 50% mais do que o atingido em 2018 (EMBRATEL, 2020)

O Brasil é um dos principais alvos desse tipo de crime, de acordo com notícias de relatórios mais recentes:

> Outro relatório Kaspersky indica que aconteceram na América Latina 1,3 milhão de tentativas de ransomware entre janeiro e setembro, média de cinco mil por dia, sendo 46,7% contra alvos apenas no Brasil. Ataques no trimestre final de 2020 a importantes órgãos da Administração Pública e grandes empresas no país reforçam o alerta (EMBRATEL,2020)

Destarte, é inegável que os crimes digitais, atualmente, são responsáveis por grande parcela dos prejuízos. Gastos em estrutura e capacitação de profissionais não devem ser considerados como despesas, mas sim como investimento capaz de contornar todos esses prejuízos causados pelos crimes digitais.

3 PROPOSTAS DE MELHORIA E CRÍTICAS EXISTENTES

A centralização do poder na união em relação ao direito penal, a demora demasiada do legislativo em fazer leis específicas, e o sistema de leis penais arcaico acabam dificultando que o Brasil acompanhe a velocidade que o meio digital proporciona. Dessa forma, já é de se esperar que tenham várias críticas e propostas de melhoria dos modelos de legislação atuais. É preciso debatê-las para melhorar a eficiência no combate aos crimes digitais.

3.1 REGULAÇÃO DOS LOGS

Como já dito anteriormente, segundo Cavalcante (2015), os Logs são uma importante ferramenta que o legislador pode utilizar para investigar os crimes

cibernéticos. Neles ficam armazenadas várias informações do usuário como data, local, IP, horário, facilita bastante a investigação.
“É uma legislação ainda tímida, em verdade, a internet é muito pouco ordenada, exemplo é a falta de regulamentação da guarda de logs, o que facilita a atividade criminosa e prejudica ou inviabiliza a investigação” (CAVALCANTE, 2015.p.19)

Dessa forma, a falta de regulação dos Logs torna a internet uma terra sem lei. Uma importante ferramenta de investigação de crimes digitais não pode carecer de regulação.

Portanto, pode-se perceber que a falta de regulação dificulta ou inviabiliza totalmente a investigação. É um assunto que deve ser amadurecido pelos legisladores e regulado com rapidez que o mundo digital necessita.

3.2 REGULAÇÃO DA CRIPTOMOEDAS

As criptomoedas, moedas digitais ou criptografia do dinheiro dão às operações virtuais os benefícios de integridade, velocidade, liberdade de pagamento, taxas baixas, anonimato e baixos riscos para comerciantes (ANDRADE, 2018, p.10).

Hoje, a capitalização de mercado das criptomoedas atinge números absurdos, o dinheiro digital se tornou mais atrativo que o físico, tendo em vista que se torna uma reserva de valor por ser deflacionário, ao contrário das moedas de cunho forçado, como o Dólar e o Real. A seguir estimativa da quantidade de capitalização de mercado das criptomoedas no mercado:

> De acordo com dados do CoinGecko e do CoinMarketCap, a capitalização de mercado das criptomoedas existentes ultrapassou o valor de US$ 1,9 trilhão (pouco mais de R$ 10,8 trilhões), chegando a uma máxima histórica de US$ 1,99 trilhão (mais de R$ 11,3 trilhões) (GUSSON, 2021, p.1).

Pode-se perceber que, devido ao caráter descentralizado da maioria das criptomoedas, seu importante papel, e a alta capitalização de mercado, uma proibição das criptomoedas não é tecnicamente impossível para os dias atuais. Não há como proibir as transações criptografadas, seria como tentar proibir a própria internet.

Antes da popularidade das criptomoedas, o Brasil já tinha criado o órgão Conselho de Controle de Atividades Financeiras – COAF. Esse órgão é responsável pelo controle de atividades financeiras e aponta certas fragilidades em seus relatórios. uma dessas fragilidades, é a demora de obtenção de mandado judicial para que o investigador possa combater crimes como lavagem de dinheiro envolvendo crimes cibernéticos e criptomoedas. (DE OLIVEIRA, 2020, p.20).

Em abril de 2014, a receita federal tratou as criptomoedas como ativos digitais e estabeleceu imposto de 15% em cima das transações com valores maiores que 35 mil reais. Em maio de 2017 a Receita Federal incluiu a bitcoin (principal criptomoeda no mercado) na declaração de imposto de renda. (ANDRADE, 2018, p.54).

Conforme afirmado por De Lucena (2019, p.99), os criminosos digitais geralmente utilizam criptomoedas (especialmente bitcoin) para a obtenção de lucros provenientes dos ataques de *ransonware* (extorsão virtual de dados da vítima). A

utilização de criptomoedas para a satisfação de crimes digitais dificulta a investigação do crime, pois falta uma regulação eficiente desses ativos.

Segundo De oliveira (2020, p. 17- 18), se for comparar com os meios monetários oficiais, as criptomoedas possuem um vácuo enorme de regulamentação, facilitando a lavagem de capital.

Dessa forma, pode-se perceber que não há uma regulação eficiente que vise combater crimes para as criptomoedas. É preciso, por exemplo, que as transações em sites de troca e venda sejam reguladas para que os investigadores possam ter acesso a informações de autores, data e hora de cada transação envolvendo dinheiro digital

3.3 DAS PENAS ATUAIS

Segundo Dornelas (2020), uma das maiores críticas sobre a atual legislação que trata de crimes digitais é a falta de proporcionalidade da pena, as penas são muito brandas, basta ler a lei Nº 12.737/12 que podemos ver que as penas impostas não passam de 2 (dois) anos, mesmo em sua forma qualificada. Penas muito baixas aliadas ao atual sistema de execução penal brasileiro acabam deixando o infrator de crime digital impune. Outra crítica, conforme Dornelas (2020), é a falta de legislação específica para tratar sobre os crimes digitais. O aplicador do direito, geralmente, precisa utilizar de analogias para conseguir dar uma resposta punitiva aos delitos digitais. Portanto é preciso um enfrentamento por parte do legislativo para trazer proporcionalidade aos crimes digitais. É preciso enfrentar o aumento desenfreado de crimes digitais.

4 CONSIDERAÇÕES FINAIS

É fácil perceber que a lei brasileira não se ocupou muito legislando sobre crime digital. As leis são fracas, deixam muitas lacunas, e acabam não regulando pontos de suma importância que ajudam na investigação do crime cibernético. Fazendo uma analogia comparativa, para fácil elucidação, é como se a lei deixasse de regular sobre autópsia e necrópsia nos crimes de homicídio.

Um ponto em comum em crimes cibernéticos é que geralmente todos eles buscam o anonimato. Dessa forma, é importante que ferramentas do anonimato sejam reguladas, como os logs e as criptomoedas.

Os logs, ao apagá-los, é como se fosse o assassino apagando os rastros de sangue de seu crime. No caso do homicídio, há a regulação e a proibição no sentido de proibir alterações no local do crime, assim deveria caminhar o tratamento dos logs no direito brasileiro.

É inegável que as criptomoedas são o futuro do dinheiro atual. Porém, é preciso que haja uma regulação para impedir o anonimato completo do dinheiro digital. Não é difícil prever que valores monetários totalmente anônimos são alvos de lavagem de dinheiro, comércio ilegal e sonegação de imposto. Portanto, a falta de regulação das criptomoedas acaba tornando o mundo digital um paraíso fiscal anônimo para todos os tipos de criminosos.

As penas atuais são outro ponto que a legislação brasileira deve procurar mudar. Ora, em tantos outros crimes do direito penal foi dado um tratamento penal

mais áspero devido à alta ocorrência, porém o congresso brasileiro não segue o mesmo raciocínio em relação aos crimes digitais. As penas continuam irrelevantes, contribuindo para a impunidade e o crescimento dos crimes cibernéticos.

Portanto, percebe-se que a legislação brasileira deve caminhar muito para conseguir uma eficácia penal que o mundo digital necessita. O direito brasileiro demora muito para acompanhar a dinamicidade dos crimes digitais. Dessa forma, é preciso agir o quanto antes, procurar ferramentas, debates no congresso, melhorias na lei, para que a sociedade se sinta mais segura no meio digital. Lembre-se, o mundo digital é apenas um espelho do mundo físico. Logo, é preciso um tratamento legal equivalente.

REFERÊNCIAS

BARBOSA, MATEUS ISRAEL ALVES CRUVINEL**. Crimes virtuais: a evolução dos crimes cibernéticos e os desafios no combate**. 2020. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/105. Acesso em: 7 abr. 2021.

BARRETO, Alesandro; DOS SANTOS, Hericson. **Deep Web: Investigação no submundo da internet**. Brasport, 2019. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=0PafDwAAQBAJ&oi=fnd&pg=PA72&dq=Deep+Web:+investiga%C3%A7%C3%A3o+no+submundo+da+internet&ots=mVeq8foDQE&sig=yz9ZrtdrLCk2LKhe9Q0Et2jq7PA#v=onepage&q=Deep%20Web%3A%20investiga%C3%A7%C3%A3o%20no%20submundo%20da%20internet&f=false . Acesso em: 7 abr. 2021.

BORTOT, Jessica Fagundes. Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional. **Virtuajus,** v. 2, n. 2, p. 338-362, 2017.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União**: seção 1, Brasília, DF, p. 2391, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 7 abr. 2021.

BRASIL. Lei nº 7.716, de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor. **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 5 jan. 1989. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 7 abr. 2021.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, 3 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em: 6 abr. 2021.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 6 abr. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 6 abr. 2021.

BRASIL é o segundo país no mundo com maior número de crimes cibernéticos. **UOL,** 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm. Acesso em: 8 mar. 2021.

CARNEIRO, ADENEELE GARCIA. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. 2012**. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/#:~:text=Os%20crimes%20virtuais%20denominados%20impr%C3%B3prios,agora%20com%20a%20utiliza%C3%A7%C3%A3o%20do. Acesso em: 7 de abr. 2021.

CAVALCANTE, Waldek Fachinelli. **Crimes cibernéticos: noções básicas de investigação e ameaças na internet. 2015.** Disponível em: http://www.conteudojuridico.com.br/artigo,crimes-ciberneticos-nocoes-basicas-de-investigacaoeameacas-na-internet,54548.html. Acesso em: 4 abr. 2021.

CÉSAR, Daniel; JUNIOR, Irineu Francisco Barreto. Marco civil da internet e neutralidade da rede: aspectos jurídicos e tecnológicos. **Revista Eletrônica do Curso de Direito da UFSM**, v. 12, n. 1, p. 65-88, 2017.

COMITÊ GESTOR DA INTERNET. (Cetic) **Indicador domicílios brasileiros com acesso à internet**., 2019. Disponível em: https://cetic.br/pt/pesquisa/domicilios/indicadores/. Acesso em: 2 abr. 2021.

DE ANDRADE, Mariana Dionísio. Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, p. 43-59, 2018.

DE ARAUJO, Fábio Lucena. Aspectos jurídicos no combate e prevenção ao ransomware. **Revista do Ministério Público do Estado do Rio de Janeiro nº**, v. 71, p. 93, 2019.

DE OLIVEIRA MONTENEGRO, Guilherme Augusto. AS CRIPTOMOEDAS E A INVESTIGAÇÃO POLICIAL: Desafios e Soluções. **Revista Brasileira de Ciências Policiais**, v. 11, n. 3, p. 183-230, 2020.

DORNELAS, Natália Alves. A RESPOSTA ESTATAL QUANTO AOS CRIMES CIBERNÉTICOS: UMA ANÁLISE DIRECIONADA ÀS LEIS Nº 12.735/2012 E 12.737/2012. **Repositório de Trabalhos de Conclusão de Curso**, 2020.

EGEWARTH, Arthur Bernardo. **Os crimes cibernéticos e a ineficácia da lei "Carolina Dieckmann"**. 2020. . Disponível em: http://bibliodigital.unijui.edu.br:8080/xmlui/handle/123456789/6497. Acesso em: 7 abr. 2021.

EMBRATEL. Brasil é alvo global de ciberatagues. **Valor.globo**, 30, nov, 2020. Disponível em : https://valor.globo.com/patrocinado/embratel/juntos-no-proximo-nivel/noticia/2020/11/30/video-especialistas-apontam-como-vencer-desafios-da-ciberseguranca.ghtml. Acesso em: 3 de abr. 2021.

GUSSON, João. **Capitalização de mercado de criptomoedas chega a US$ 1,9 tri**. 2, abr, 2021. Disponível em: https://www.dci.com.br/investimentos/criptomoedas/capitalizacao-de-mercado-de-criptomoedas-chega-a-us-19-tri/113913/. Acesso em: 4 abr. 2021.

MEGAVAZAMENTO de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. **G1**, 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 8 mar. 2021.

PAULINO, Fabiana. **A ineficácia da legislação nos crimes virtuais**. 2018. Disponível em: http://45.4.96.19/handle/aee/1200 . Acesso em: 04/05/2021

Campus I - QS 07 – Lote 01 – EPCT – Águas Claras – Brasília – DF CEP: 71966-700 - (61) 3356-9000
Campus Avançado Asa Norte - SGAN 916 Módulo B Avenida W5 - CEP: 70790-160 - Brasília/DF - Telefone: (61) 3448-7134
Campus Avançado Asa Sul - SHIGS 702 Conjunto 2 Bloco A - CEP: 70330-710 - Brasília/DF - Telefone: (61) 3226-8210