CRIMES CIBERNÉTICOS, FALTA DE SEGURANÇA E LEGISLAÇÃO: UM ESTUDO DE CASO EM PERNAMBUCO

CYBER CRIMES, LACK OF SECURITY AND LEGISLATION: A CASE STUDY IN THE STATE OF PERNAMBUCO

Gustavo Boudoux de Melo[1]

RESUMO: O presente artigo pretende trazer uma reflexão e discussão com relação aos crimes cibernéticos, pois com o avanço das tecnologias e internet, todos os dispositivos passaram a estar conectados, porém não há uma segurança quando se refere a proteção dos dados, há uma carência de legislações específicas, que venha a penalizar os criminosos, estes que acabaram se multiplicando principalmente após a pandemia e a chegada da COVID-19, onde se teve um maior isolamento e *lockdown*. O principal objetivo é analisar os crimes cibernéticos em Pernambuco, verificar quais são os crimes de maior incidência e quais são os maiores desafios para a segurança e defesa cibernética. A metodologia utilizada foi através das pesquisas bibliográficas, estudo de caso e pesquisa de campo junto a Delegacia de Crimes Cibernéticos de Pernambuco, com a utilização da abordagem investigativa, métodos quantitativos e aplicação de questionários. Como resultados encontrados, acredita-se que se houvesse uma maior interação entre os órgãos públicos, as empresas privadas e as instituições de ensino, bem como estudos e investimentos públicos e privados, e uma maior interdisciplinaridade entre a área do direito penal e as tecnologias de informação e comunicação, poderia se ter uma maior esperança de um dia poder ter uma certa segurança, cobertura jurídica e justiça, num país praticamente sem leis, anonimato e impunidade cibernética.

Palavras-chaves: crimes cibernéticos; direito digital; legislação; segurança cibernética.

ABSTRACT: This article intends to bring a reflection and discussion regarding cyber crimes, because with the advancement of technologies and the internet, all devices are now connected, but there is no security when it comes to data protection, there is a lack of legislation specific, which will penalize criminals, who ended up multiplying mainly after the pandemic and the arrival of COVID-19, where there was greater isolation and lockdown. The main objective is to analyze cyber crimes in Pernambuco, to verify which

[1] Doutorando em Direito na Universidade Católica de Pernambuco (PPGD - UNICAP). MBA Executivo em Segurança Cibernética pela Faculdade INTERVALE. Especialização em Crimes Cibernéticos pela Faculdade INTERVALE. Especialização em Direito Trabalhista pela Faculdade INTERVALE. E-mail: dir.gustavomelo@gmail.com. Currículo Lattes: http://lattes.cnpq.br/9393295457857318.

are the crimes with the highest incidence and which are the biggest challenges for security and cyber defense. The methodology used was through bibliographic research, case study and field research with the Pernambuco Cyber Crimes Police Station, using an investigative approach, quantitative methods and questionnaires. As results found, it is believed that if there were greater interaction between public agencies, private companies and educational institutions, as well as studies and public and private investments, and greater interdisciplinarity between the area of criminal law and technologies of information and communication, there could be greater hope of one day being able to have a certain security, legal coverage and justice, in a country practically without laws, anonymity and cybernetic impunity.

Keywords: cyber crimes; cybersecurity; digital law; legislation.

1 INTRODUÇÃO

Com a chegada e comercialização da internet no Brasil, em meados de 1994, as pessoas, computadores e equipamentos passaram a se comunicar e trocar informações, quebrando assim as barreiras e distâncias geográficas. Em torno de 2001, já se tinha internet nos telefones celular, aumentando assim a acessibilidade e mobilidade maior com a comunicação e informação.

De acordo com Wendt e Jorge (2013) da mesma forma que houve uma evolução dos recursos tecnológicos, também surgiram, cresceram e se aprimoraram as ameaças praticadas principalmente com o uso dos computadores. Já no final da década de 50 começaram a aparecer os códigos maliciosos, onde depois evoluíram para os vírus (1982), cavalos de Tróia (1986), evoluindo assim diversas outras ameaças. Só em 1988 foi que surgiu o primeiro antivírus para tentar combater e imunizar os computadores. E em 2004 foi quando surgiram os primeiros vírus para celulares, através da internet e *bluetooth*, abrindo espaço para a evolução e conectividade para os diversos tipos de dispositivos.

Acredita-se que atualmente a maioria da população brasileira deve ter pelo menos um telefone celular ou dispositivo conectado à internet, com acesso a vários aplicativos de troca de mensagens, informações, e-mails, bancos, compras de produtos e serviços, redes socais, dentre outros. Porém, como todo mundo tem acesso a mesma rede de internet, provedores, operadoras de telefonia, *wi-fi*, sites, aplicativos, dentre outros, onde

nesse mesmo espaço cibernético é compartilhado com todo tipo de pessoas e grupos, vai ter gente que "acobertados pela distância e pelo anonimato, tentam burlar a segurança dos equipamentos e dos sistemas informatizados de qualquer empresa, governo ou indivíduo e extrair benefícios indevidos da exploração desse bem chamado informação" (MANDARINO JUNIOR, 2011, p. 40).

Jesus e Milagre (2016, p. 16) consideram que todo o cidadão está vulnerável e sujeito a riscos neste espaço cibernético, pois "constitui-se presa fácil nas mãos de especialistas em crimes cibernéticos, os *crackers*[2], que exploram as intimidades dos sistemas e também dos processos desenvolvidos sobre a tecnologia da informação para a prática de delitos".

Por conta disso, se faz necessário se preocupar com a segurança da cibernética, e buscar proteger todas as informações e infraestruturas, que suportam as soluções de tecnologia da informação, composta pelos hardwares, softwares, servidores, roteadores, computadores, dispositivos, sistemas e serviços, de forma a montar uma "Estratégia de Segurança Cibernética para a Nação brasileira".

Para Mandarino Junior (2011, p. 45):

> Uma Estratégia de Segurança Cibernética para a Nação brasileira deve projetar e dimensionar os esforços necessários para proteger seus ativos de informação, suas infraestruturas críticas de informação, suas informações críticas; avaliar riscos; desenhar planos de contingências, para recuperação, ou não, de informações diante de desastres naturais; capacitar recursos humanos para responder, pronta e competentemente, a incidentes nas redes; garantir a privacidade das pessoas e das empresas presentes na sociedade da informação; e, como grande diferencial, ter a capacidade de aprender a desenvolver ferramentas de defesa. E ainda que essa Estratégia de Defesa Cibernética esteja apta a utilizar essas ferramentas e a própria informação como recurso ou arma, para assegurar a preservação do Estado brasileiro.

Partindo do princípio que o espaço cibernético é um local virtual "composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais

[2] Cracker é um vândalo virtual, alguém que usa seus conhecimentos para invadir sistemas, quebrar travas e senhas, roubar dados etc. Alguns tentam ganhar dinheiro vendendo as informações roubadas, outros buscam apenas fama ou divertimento (MORIMOTO, 2005).

transitam, são processadas e armazenadas" (DEFESANET, 2014), onde um dos recursos mais utilizados, e que facilita bastante é a comunicação, que pode ser realizada através de vídeo conferência, redes sociais, bem como com o uso da inteligência artificial, hipertextos, multimídia interativa, simulações, mundos virtuais (metaverso), dispositivos de tele presença, realidade aumentada, internet das coisas, dentre outras ferramentas, porém se faz necessário ter segurança nesses espaços que são compartilhados com o uso da internet, de forma que os dados e as informações das empresas, bem como os dados pessoais não venham a cair em mãos erradas, e causar algum tipo de dano ou prejuízo.

O presente artigo aborda o tema "crimes cibernéticos: a falta de segurança e legislação no Brasil", tem como objetivo analisar a questão dos crimes cibernéticos em Pernambuco, o que se tem feito para contribuir com a segurança no ciberespaço e o que se tem de legislação na área de direito penal e digital. Como objetivos específicos: Analisar quais são os crimes cibernéticos de maior incidência em Pernambuco; descrever o que se tem feito para minimizar a carência de legislação e insegurança cibernética; e verificar quais são os maiores desafios para a segurança e defesa cibernética.

A pesquisa em campo foi realizada junto com os servidores da Delegacia de Repressão aos Crimes Cibernéticos (DPCRICI) de Pernambuco.

Como problema de pesquisa, com base no crescimento das ocorrências e deligências relacionadas aos crimes cibernéticos, buscou-se verificar quais são os maiores desafios da DPCRICI-PE, bem como contribuir com sugestões para soluções e melhorias no combate ao crime cibernético de Pernambuco.

Procurou-se apresentar a rotina atual com relação aos crimes cibernéticos ocorridos junto a DPCRICI-PE, onde foi verificado quais são as principais carências e desafios relacionados aos crimes cibernéticos.

Para trazer embasamento teórico para este artigo e atender ao tema proposto em questão foram abordados alguns assuntos relacionados aos crimes cibernéticos e algumas leis específicas da área; direito penal e o Código Penal (CP); carência da legislação na área de direito digital no Brasil; e os desafios estratégicos para a segurança e defesa cibernética.

2 CRIMES CIBERNÉTICOS

Para um melhor entendimento com relação aos crimes cibernéticos, como definição são os "delitos praticados contra ou por intermédio de computadores (dispositivos informáticos, em geral)" (WENDT; JORGE, 2012, p. 18).

> Os crimes tecnológicos são aqueles que envolvem o uso de tecnologias computador, internet, caixas eletrônicos), sendo, em regra, crimes meios — ou seja, apenas a orma em que são praticados é que é inovadora. Têm como subespécie os crimes virtuais, informáticos ou cibernéticos (praticados pela internet), onde, apesar de se concretizarem em ambientes virtuais, os delitos trazem efeitos no mundo real (BARRETO; BRASIL, 2016, p. 36).

Várias condutas são consideradas crimes cibernéticos, como: acesso ilegítimo, interceptação ilegítima, interferência de dados ou dano informático, interferência em sistemas, uso abusivo de dispositivos, falsidade ou fraude informática, burla informática, furto de dados ou vazamento de informações, pichação informática, envio de mensagens não solicitadas e uso indevido informático.

Para Barreto e Brasil (2016, p. 37) os crimes cibernéticos podem ser classificados como (1) puros ou próprios; (2) impuros ou impróprios. A primeira classificação é caracterizada quando os "sistemas informatizados, bancos de dados, arquivos ou terminais são atacados pelos criminosos, normalmente após a identificação de vulnerabilidades, seja por meio de programas maliciosos ou, ainda, por engenharia social (golpista engana a vítima)". Seguem alguns exemplos de crimes cibernéticos (1) acordo com o Código Penal (BRASIL, 1940):

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita.
> Art. 163 - (Dano) Destruir, inutilizar ou deteriorar coisa alheia.
> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento.
> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas

> informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente.

Os crimes cibernéticos classificados como impuros ou impróprios (2) "são aqueles onde o dispositivo tecnológico é utilizado como meio para a prática do delito, propiciando a sua execução ou o seu resultado (BARRETO; BRASIL, 2016, p. 39). São crimes comuns, que normalmente constam no Código Penal Brasileiro (BRASIL, 1940), onde o criminoso utiliza algum recurso tecnológico para cometer o delito, como nos exemplos a seguir:

> Art. 122 - Induzir ou instigar alguém a suicidar-se ou a praticar automutilação ou prestar-lhe auxílio material para que o faça.
> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime.
> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação.
> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro.
> Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave.
> Art. 147-A - Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.
> Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem.

Esses artigos citados do CP (BRASIL, 1940) exemplificam apenas alguns crimes comuns da área de Direito Penal, porém existem muito mais, que quando são praticados com o uso de dispositivo tecnológico, principalmente com a utilização da internet e as redes sociais, os mesmos são tipificados como crimes cibernéticos, onde não maioria das vezes não se tem uma legislação específica. Importante se repensar sobre isso, pois a repercurssão, influência, manipulação, divulgação, propagação e disseminação pela internet é muito maior, causando danos e imapctos mais significativos do que se fosse por exemplo pessoalmente, como são os casos das *fake news*, *deepfakes*, *cyberbullying*, *stalking*, dentre outros.

Quando se trata especificamente das "condutas indevidas praticadas por computador" há uma classificação que "podem ser divididas em 'crimes cibernéticos' e 'ações prejudiciais atípicas'. A espécie 'crimes cibernéticos' subdivide-se em 'crimes cibernéticos abertos' e 'crimes exclusivamente cibernéticos'" (WENDT; JORGE, 2013, p. 18).

A seguir, apresenta-se as condutas indevidas praticadas por computador, ligadas aos crimes cibernéticos abertos, crimes exclusivamente cibernéticos e ações prejudiciais atípicas.

Figura 1 – condutas indevidas praticadas por computador

Fonte: Wendt e Jorge (2012, p. 20)

Os crimes cibernéticos abertos são aqueles praticados de forma tradicional ou por intermédio de computadores, que são usados para a prática do crime, porém também

podem ser cometidos sem o uso do computador. Alguns crimes determinados como abertos, como os crimes contra a honra; ameaça; importunação ofensiva ao pudor; falsificação de documentos; estelionato; furto mediante fraude; concorrência desleal; espionagem industrial; violação de segredo; apologia de crime ou criminoso; racismo; tráfico de drogas; atentado a serviço de utilidade pública.

Já nos casos dos crimes exclusivamente cibernéticos, próprios, aqueles cometidos com a utilização do computador ou outros equipamentos tecnológicos que tenha acesso à internet, percebe-se que há pelo menos um artigo de lei que especifique e tipifique determinado crime, trazendo assim as suas respectivas penas e sanções, com base em cada tipo e gravidade do crime em questão. Como são os casos de crime de pornografia infantil por meio de sistema de informática (art. 241-B, Lei nº 8.069/90); corrupção de menores em salas de bate papo da internet (art. 244-B, § 1 º, Lei nº 8.069/90) violar os direitos de autor de programa de computador (art. 12, Lei nº 9.609/98); inserção de dados falsos em sistema de informações (art. 313-A, Decreto-Lei nº 2.848/40); e crimes contra equipamentos da votação (art. 72, Lei nº 9.504/97).

No caso das ações prejudiciais atípicas, por ainda não serem consideradas como crime no Brasil, e não ter uma legislação específica, esse assunto será abordado no próximo tópico, trazendo uma reflexão com relação a carência de legislação na área de direito digital e penal, bem como as consequências de sua impunidade, além dos transtornos e prejuízos que podem ser gerados com cada tipo de ação atípica citada.

O presente estudo não tem a pretensão de aprofundar, esgotar e nem tão pouco detalhar todos os crimes cibernéticos, pois quando se trata dos artefatos, técnicas ou métodos, Jesus e Milagre (2016) citam 22 (vinte e duas) possibilidades para a prática de crimes informáticos; e 11 (onze) condutas informáticas que podem caracterizar um crime cibernético. Sendo assim, coloca-se como sugestão para uma pesquisa futura esse aprofundamento e detalhamento técnico com relação a todas essas possibilidades citadas, visando trazer apenas uma maior contribuição para a área jurídica.

Mesmo com todos esses tipos de crimes cibernéticos, além dos outros que ainda não são tipificados e caracterizados como delitos ou crimes, no que se refere a legislação

brasileira, direito digital e penal, ainda há uma carência muito grande com relação as leis e justiça no país, principalmente com relação as questões de investigação, monitoramento e rastreamento desses criminosos que vivem no anonimato, onde na maioria das vezes vivem e navegam pelo mundo mais obscuro, como por exemplo na *deep web* e *dark web*.

2.1 A carência de legislação na área de direito digital e penal no Brasil

Uma das formas de provar que ainda há muito o que se evoluir e atualizar junto a legislação penal brasileira, pois não tem uma previsão penal para as "ações prejudiciais atípicas", conforme apresentado na figura 1, ou seja, quando se trata desses tipos de ações e condutas ilícitas, o indivíduo não é punido porque ainda não há uma legislação específica, deixando assim o cidadão, que neste caso é a vítima, no prejuízo e transtornos, e o criminoso vai ficar impune.

> As "ações prejudiciais atípicas" são aquelas condutas, praticadas na/através da rede mundial de computadores, que causam algum transtorno e/ou prejuízo para a vítima, porém não existe uma previsão penal, ou seja: o indivíduo causa algum problema para a vítima, mas não pode ser punido, no âmbito criminal, em razão da inexistência de norma penal com essa finalidade (WENDT; JORGE, 2013, p. 18).

Para a legislação brasileira, conforme apresentado na figura 1, ainda não são considerados crimes, segundo Wendt e Jorge (2012, p. 20):

> - Acesso não autorizado a redes de computadores;
> - Inserção ou difusão de código malicioso;
> - Obtenção ou transferência não autorizada de dado ou informação;
> - Divulgação de informações pessoais.

Acredita-se que alguns fatores contribuem muito com essa carência da falta de legislação, como o surgimento tardio das novas áreas ou ramo do direito, como o direito digital, direito cibernético, crimes cibernéticos, direito penal informático e talvez mais algumas áreas afins.

Outro fator relevante também é a falta de comunicação e interdisciplinaridade entre duas grandes áreas, como a do direito e a tecnologia da informação e comunicação (TICs). Como também afirmam Jesus e Milagre (2016, p. 28) onde a "falta de apoio técnico – especialistas em tecnologia e segurança da informação, em setores legislativos – leva o legislador brasileiro à criação de tipos penais incoerentes".

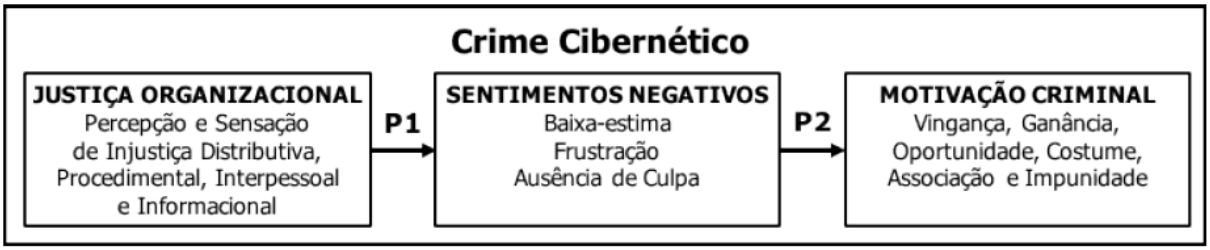
Como é de conhecimento comum, pode-se entender que se tratando de crimes cibernéticos no Brasil, o que vai servir como base de consulta legal é a Constituição Federal (BRASIL, 1988); Decreto-Lei nº 2.848, Código Penal (BRASIL, 1940); Decreto-Lei nº 3.689, Código de Processo Penal (BRASIL, 1941); Lei nº 12.735, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares (BRASIL, 2012a); Lei nº 12.737, dispõe sobre a tipificação criminal de delitos informáticos, conhecida como a Lei Carolina Dieckmann (BRASIL, 2012b); Lei nº 12.965, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, conhecido como o Marco Civil da Internet (BRASIL, 2014); Lei nº 13.772, para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado (BRASIL, 2018); e por fim, Lei nº 14.155, para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet (BRASIL, 2021).

Uma outra situação que merece atenção, e que também há uma carência de legislação, percepção de impunidade e falta de monitoramento, e tudo isso também pode acabar incentivando as pessoas a cometerem crimes cibernéticos na própria empresa que trabalham, conforme pesquisa realizada por Garcia, Macadar, Luciano (2018), onde trazem como contribuição e acrescentam que as pessoas também podem ser motivadas a praticar crimes cibernéticos pelos sentimentos negativos de injustiça organizacional, além dos outros pontos comentados em questão.

Para Garcia, Macadar, Luciano (2018) a percepção e a sensação de injustiça organizacional provocam sentimentos negativos de baixa-estima, frustração e ausência

de culpa, despertando a vingança, ganância, oportunismo, costume, associação ou impunidade na empresa, que acabam sendo motivadas a cometerem crimes cibernéticos, principalmente por ter o conhecimento tecnológico e mais fácil acesso dentro da organização, conforme apresentado na figura 2.

Figura 2 – Modelo conceitual de crime cibernético por funcionários nas organizações



Fonte: Garcia, Macadar, Luciano (2018, p. 15)

Sendo assim, percebe-se uma necessidade de legislação específica de monitoramento e rastreamento das informações nas empresas, de forma que a mesma possa se proteger e salvaguardar de várias possibilidades negativas que podem ser ocasionadas por funcionários insatisfeitos, desmotivados, mal intencionados, problemáticos ou desonestos.

Visando contribuir para minimizar essa carência com relação a legislação brasileira no combate aos crimes cibernéticos, Jesus e Milagre (2016, p. 26) relatam um equívoco no que se refere a forma de condenação das técnicas informáticas, pois "estas são mutantes, nascem e morrem a qualquer momento, de acordo com a evolução dos sistemas, novas vulnerabilidades e plataformas tecnológicas", onde defendem que 'não se legisla sobre técnica' ou 'vulnerabilidade', pois o correto seria condenar as 'condutas praticadas por diversas técnicas', conforme proposta da teoria do TCC (Técnica, Comportamento e Crime), apresentada a seguir.

> Para que se possa conceber uma legislação minimamente eficiente, eficaz e que não precise ser complementada com o tempo, bem como para que se possa compreender o crime digital, importante se faz sistematizá-lo da seguinte forma:

> • **Técnica**: método, procedimento, *software* ou processo informático utilizado e que pode caracterizar um comportamento. Uma técnica pode ser executada manualmente ou por meio de subtécnicas, métodos automatizados ou ferramentas. A exemplo, um agente que obtém acesso a dados de um repositório pode estar utilizando a técnica de *sql injection*.
> • **Comportamento**: uma ação realizada por meio de uma ou mais técnicas, cometida por um ou mais agentes, por ação ou omissão, em face de redes de computadores, dispositivos informáticos ou sistemas informatizados. No mesmo exemplo citado acima, por meio da técnica *sql injection*, o agente praticou o comportamento "invasão de sistema informático".
> • **Crime**: um ou vários comportamentos, que utiliza uma ou mais técnicas, que ofende um ou mais bens ou objetos jurídicos protegidos pelo Direito. Mantendo o mesmo exemplo, a "invasão de sistema informático" pode ser ou não considerada crime, dependendo do país em que é praticada (JESUS; MILAGRE, 2016, p. 26).

Essa carência com relação a falta de legislação brasileira, principalmente no que se refere ao direito penal e digital, gera mais um desafio para a segurança e defesa cibernética.

2.2 Desafios estratégicos para a segurança e defesa cibernética

As empresas e instituições públicas e privadas precisam ter mais atenção com relação a questão da segurança, integridade dos dados e informações, principalmente no tocante a precisão e consistência dos dados, visto que há várias possibilidades e meios que podem comprometer a integridade dos mesmos, como o erro humano, podendo ser não intencional ou até mesmo malicioso; erros de transferência; bugs, vírus, *malware*, *hackers*, dentre outras ameaças; *hardware* comprometido; e compromisso físico para dispositivos.

Uma das alternativas para se proteger contra os crimes cibernéticos é fazer a contratação de *cyber* seguro, sistemas de monitoramento e rastreamento para os riscos cibernéticos, como também investimento em Inteligência Cibernética, Inteligência Artificial, *Machine Learning*, *backups* de segurança, espelhamento, *firewall*, criptografia, antivírus, assinatura digital, gestão de riscos de TI, dentre outros.

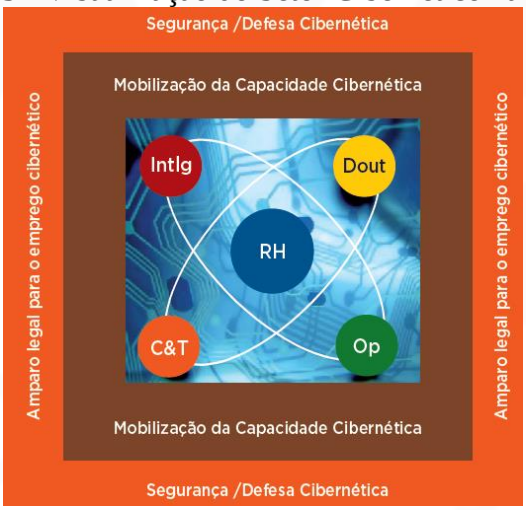
Segundo Barros, Gomes e Freitas (2011) a questão de capacitação dos recursos humanos deve ser uma atividade prioritária e indispensável, na qual a sua mobilização

deve ser integrada em quatro vetores, como: a inteligência; a doutrina; a ciência, tecnologia e inovação; e as operações.

Henriques (2021) afirma que um dos maiores desafios é com relação a capacitação de recursos humanos para a Defesa Cibernética, onde chama atenção de como deve ser trabalhada essa área, conforme apresentado a seguir.

> Para alcançar o objetivo de formar seus recursos humanos em cibernética o Exército precisou definir qual o universo a capacitar, bem como quais as capacidades necessárias para desempenhar as diversas atividades ligadas a Defesa Cibernética. Dentro desse contexto, definiu-se que o devemos entender que a capacitação em cibernética se desenvolve em 5 (cinco) níveis, quais sejam: USUÁRIO (Utiliza os sistemas de TI), TÉCNICO (Implementa sistemas de TI), ACADÊMICO (Programador, desenvolvedor de redes), PENTESTER (Aplica técnicas de defesa ativa), DESENVOLVEDOR 1 (Cria programas e técnicas de defesa), DESENVOLVEDOR 2 (Cria técnicas e programas contra sistemas operacionais) (HENRIQUES, 2021, p. 1).

Figura 3 - Visualização do Setor Cibernético na Defesa



Fonte: Barros, Gomes e Freitas (2011, p. 23)

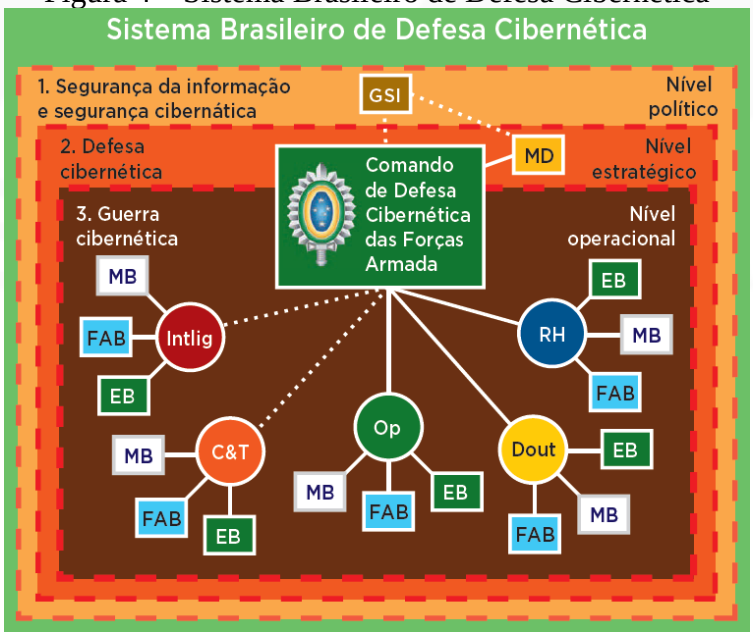
De acordo com Barros, Gomes e Freitas (2011) o Sistema Brasileiro de Defesa Cibernética deve ser implementado de forma integrada, como apresentas nas figuras 3 e 4.

Barros, Gomes e Freitas (2011, p. 27) destacam alguns desafios do setor cibernético no âmbito da defesa, como:

a. óbices de natureza cultural, associando as ações cibernéticas a atividades ilícitas de intrusão, quebra de privacidade das pessoas, roubo de dados etc.;
b. necessidade de conscientização de governantes e da sociedade como um todo em relação ao tema, decorrente do óbice anterior, que dificulta a obtenção da indispensável mobilização para a participação nas atividades de Segurança e Defesa Cibernéticas;
c. escassez de recursos financeiros ou não priorização do setor na alocação de recursos financeiros, também, em parte, decorrente dos óbices anteriores;
d. caráter sensível da atividade, dificultando a aquisição de conhecimento vindo do exterior; e
e. integração e atuação colaborativa incipientes dos diversos atores envolvidos.

Acredita-se que os principais desafios estratégicos seja manter o sistema brasileiro de defesa cibernética integrado e conectado, visto que o mesmo é composto por diversos órgãos, conforme apresentado na figura 4, que não haja uma rotatividade dos integrantes das equipes, que se desenvolvam e se qualifiquem continuamente na sua carreira e que se tenha recursos financeiros para os investimentos necessários como infraestrutura, equipamentos, tecnologias, sistemas e treinamentos específicos na área de segurança e defesa cibernética.

Figura 4 – Sistema Brasileiro de Defesa Cibernética



Fonte: Barros, Gomes e Freitas (2011, p. 26)

E por fim, Barros, Gomes e Freitas (2011, p. 28) destacam as ações estratégicas mais relevantes para que seja consolidado o Setor Cibernético na defesa, como:

> Assegurar o uso efetivo do espaço cibernético pelas Forças Armadas e impedir ou dificultar sua utilização contra interesses da defesa nacional;
> Capacitar e gerir talentos humanos para a condução das atividades do setor cibernético na defesa;
> Desenvolver e manter atualizada a doutrina de emprego do setor cibernético;
> Adequar as estruturas de CT&I das Forças Armadas e implementar atividades de pesquisa e desenvolvimento (P&D) para o setor cibernético;
> Cooperar com o esforço de mobilização militar e nacional para assegurar as capacidades operacional e dissuasória do setor cibernético.

Percebe-se que são muitos os desafios e que de fato se precisa ter estratégias para conseguir manter todo o sistema de segurança e defesa nacional funcionando, seguro e atualizado, além dos aspectos relacionados as doutrinas, legislações, ciência e tecnologia, pesquisa e desenvolvimento, e as relações internacionais, principalmente com o objetivo de troca de experiências, informações, expertises, dentre outros.

3 DESENVOLVIMENTO DA PESQUISA DE CAMPO

O objeto de estudo deste documento é formado pelos crimes cibernéticos e a falta de segurança e legislação no Brasil.

O objetivo foi analisar a questão dos crimes cibernéticos em Pernambuco, o que se tem feito para contribuir com a segurança no ciberespaço e o que se tem de legislação na área de direito penal e digital.

O universo e amostra da presente pesquisa foi com os servidores lotados na delegacia citada, onde contam atualmente com 8 (oito) servidores, porém um estava de férias e licença e o outro estava de licença médica, totalizando assim com 6 (seis) respondentes.

O desenvolvimento desta pesquisa teve um estudo bibliográfico, estudo de caso e pesquisa de campo junto a Delegacia de Crimes Cibernéticos (DPCRICI) de Pernambuco,

com a utilização da abordagem investigativa, métodos quantitativos, com aplicação de questionários com perguntas fechadas e objetivas, elaboradas de acordo com os assuntos e fundamentação teórica deste artigo em questão. Importante destacar que no estado de Pernambuco só tem apenas uma delegacia para atender os casos de crimes cibernéticos.

Para o desenvolvimento da pesquisa em campo foi aplicado um questionário fechado com 12 perguntas objetivas, visando analisar as ocorrências dos crimes cibernéticos na delegacia de repressão de Pernambuco, verificar quais são os seus maiores desafios, e quais são as sugestões para soluções e melhorias no combate ao crime cibernético.

4 ANÁLISES E RESULTADOS

Conforme questionário aplicado, o presente artigo teve as seguintes respostas.

1 - Com relação aos crimes cibernéticos abertos, qual desses tem o maior número de ocorrência na DPCRICI-PE? Os crimes mais comuns foram contra a honra, representando 66,7% e estelionato 33,3% das respostas.

2 - Com relação aos crimes exclusivamente cibernéticos, qual desses tem o maior número de ocorrência na DPCRICI-PE? Os que tiveram um maior número de ocorrências foram a pornografia infantil por meio de sistema de informática, com 66, 7%; e inserção de dados falsos em sistema de informações, com 33,3% das respostas.

3 – Com relação aos cibercrimes contra a pessoa, qual desses tem o maior número de ocorrência na DPCRICI-PE? As maiores ocorrências foram os crimes de difamação e injúria, ambos tiveram como 50% das respostas de cada.

4 - Com relação as condutas indevidas de ações prejudiciais atípicas, qual dessas tem o maior

número de ocorrência na DPCRICI-PE? O maior número de ocorrências com a inserção ou difusão de código malicioso, com 83,3%; e a obtenção ou transferência não autorizada de dados ou informação, com 16,7% das respostas.

5 - Na sua percepção, qual a principal motivação das pessoas que praticam um crime cibernético? A maior motivação para a prática dos crimes é a impunidade, com 83,34%; e a oportunidade, com 16,7% das respostas.

6 - Na sua percepção, qual das leis é a mais utilizada ou aplicada nesta Delegacia? As leis mais utilizadas são a Lei nº 12.965/2014 - Marco Civil da Internet, com 66,7%; e Lei nº 14.155/2021 - Violação de dispositivo informático, furto e estelionato, com 33,3% das respostas.

7 - Na sua percepção, qual o motivo que pode incentivar mais o cibercrime? Os motivos que mais podem incentivar os crimes são pela carência de legislação específica, com 50%; percepção de impunidade, com 33,3%; e falta de sistemas de rastreamentos, com 16,7% das respostas.

8 – Na sua percepção, o que mais contribui para essa carência de legislação específicas para o
cibercrime? O que mais contribui são a falta de qualificação e capacitação profissional, com 50%; falta de conhecimento do legislador, com 16,7%; e a falta de integração entre as forças de segurança pública, com 33,3% das respostas.

9 – A capacitação das pessoas em cibernética se desenvolve em cinco níveis, tais como: **Usuário** (Utiliza os sistemas de TI); **Técnico** (Implementa sistemas de TI); **Acadêmico** (Programador, desenvolvedor de redes); **Pentester** (Aplica técnicas de defesa ativa); e **Desenvolvedores** (Cria programas e técnicas de defesa ou programas contra sistemas operacionais). Qual capacitação em cibernética é a mais importante para o seu trabalho?

As capacitações mais importantes são no nível de desenvolvedores (Cria programas e técnicas de defesa ou programas contra sistemas operacionais) com 83,3%; e técnico (Implementa sistemas de TI), com 16,7% das respostas.

10 – Na sua percepção, qual o maior desafio do sistema brasileiro de defesa cibernética? Os maiores desafios são com a falta de investimento em segurança, com 83,3%; e falta de integração entre as forças de segurança pública, com 16,7% das respostas.

11 – Na sua percepção, o que mais poderia contribuir para uma maior segurança cibernética em Pernambuco? O mais poderia contribuir seria os investimentos em equipamentos e softwares, com 83,3%; e investimento em um sistema integrado de segurança cibernética, com 16,7% das respostas.

12 – Na sua percepção, o que poderia contribuir para agilizar o seu trabalho no combate ao cibercrime? O mais poderia contribuir para o combate ao cibercrime seria a integração entre as forças de segurança pública, representando 100% das respostas.

De acordo com as respostas apresentadas dos servidores da DPCRICI-PE, as maiores ocorrências em Pernambuco são os crimes contra a honra, estelionato, pornografia infantil por meio de sistema de informática, inserção de dados falsos em sistema de informações, difamação e injúria, inserção ou difusão de código malicioso, obtenção ou transferência não autorizada de dado ou informação.

A legislação mais utilizada foram a Lei nº 12.965/2014 - Marco Civil da Internet, e a Lei nº 14.155/2021 - Violação de dispositivo informático, furto e estelionato.

As principais motivações das pessoas e incentivos aos cibercrimes foram impunidade e a oportunidade; carência de legislação específica, percepção de impunidade, e a falta de sistemas de rastreamentos.

Ficaram evidentes as principais carências, como a falta de qualificação e capacitação profissional, a falta de integração entre as forças de segurança pública, e a falta de conhecimento do legislador.

E como principais desafios, que poderiam contribuir muito com o combate dos cibercrimes e trabalho da DPCRICI-PE, tiveram como maior destaque os pontos relacionados ao investimento na capacitação de desenvolvedores de soluções, programas e técnicas de defesa, investimento em segurança, equipamentos e softwares, bem como a integração entre as forças de segurança pública.

5 CONSIDERAÇÕES FINAIS

O tema escolhido é de extrema importância e urgência a ser debatido, bem como precisa de providências e soluções, principalmente pela possibilidade de trazer consequências negativas tanto para as pessoas e clientes, quanto para as empresas públicas e privadas, em função da vulnerabilidade, falta de segurança, monitoramento e rastreamento do espaço cibernético, principalmente das camadas que não tem nenhum tipo de regulação ou legislação, como na *deep web* e *dark web*, onde as pessoas navegam no anonimato.

De acordo com a Agência Senado (2021), a cada 11 segundos ocorre um ataque cibernético no mundo, e no último ano, provavelmente em razão da pandemia da covid-19, que levou mais pessoas a trabalhar em casa, houve um crescimento de 97% dos ataques cibernéticos, em relação a 2020.

Com base nas pesquisas e estudos, bem como em tudo o que foi apresentado nas análises e resultados, percebe-se que Pernambuco precisa investir e evoluir muito no combate aos crimes cibernéticos.

Acredita-se que se houvesse uma maior interação entre os órgãos públicos, as empresas privadas e as instituições de ensino, bem como estudos e investimentos públicos e privados, e uma maior interdisciplinaridade entre a área do direito penal e as áreas de sistemas e tecnologias de informação, poderia se ter uma maior esperança de um dia poder

ter uma certa segurança, cobertura jurídica e justiça, num país praticamente sem leis, anonimato e impunidade cibernética.

REFERÊNCIAS

AGENCIA SENADO**. Combate ao cibercrime é urgente, afirmam especialistas na CCT**. Publicado em: 15 dez. 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/12/15/combate-ao-cibercrime-e-urgente-afirmam-especialistas-na-cct. Acesso em: 31 maio 2022.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética**: à luz do marco civil da internet. Imprenta: Rio de Janeiro, Brasport, 2016.

BARROS, Otávio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS, Whitney Lacerda de (Orgs.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. Disponível em: http:/livroaberto.ibict.br/handle/1/612. Acesso em: 12 jan. 2022.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ ccivil_03/Constituicao/Constituicao.htm. Acesso em: 12 jan. 2022.

BRASIL. DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940. **Código Penal**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 12 jan. 2022.

BRASIL. DECRETO-LEI Nº 3.689, DE 3 DE OUTUBRO DE 1941. **Código de Processo Penal**. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/del3689.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 8.069, DE 13 DE JULHO DE 1990. **Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 9.504, DE 30 DE SETEMBRO DE 1997. **Estabelece normas para as eleições**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 9.609, DE 19 DE FEVEREIRO DE 1998. **Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, **para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências**. [2012a]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 12 jan. 2022.

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. [2012b]. Disponível em: http://www.planalto.gov.br/ ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 13.772, DE 19 DE DEZEMBRO DE 2018. Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), **para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13772.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), **para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet**; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 12 jan. 2022.

DEFESANET. Concepção Estratégica de Tecnologia da Informação. Portaria Nº 233, de 20 de Março de 2014. Aprova a Concepção Estratégica de Tecnologia da Informação. Disponível em http://www.defesanet.com.br/cyberwar/noticia/14799/EB---Concepcao-Estrategica-de-Tecnologia-da-Informacao/. Acesso em: 26 jan. 2022.

GARCIA, Plínio Silva de; MACADAR, Marie Anne; LUCIANO, Edimara Mezzomo. A influência da injustiça organizacional na motivação para a prática de crimes cibernéticos. **JISTEM - Journal of Information Systems and Technology Management [online]**. 2018, v. 15, e201815002. Disponível em: https://doi.org/10.4301/S1807-1775201815002. Acesso em: 24 jan. 2022.

HENRIQUES, Henrique de Queiroz. Os desafios da capacitação de recursos humanos para a Defesa Cibernética. **Observatório Militar da Praia Vermelha**. ECEME: Rio de Janeiro. 2021. Disponível em: http://ompv.eceme.eb.mil.br/defesa-cibernetica/guerra-cibernetica/392-des-c. Acesso em: 26 jan. 2022.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. 1. Ed. São Paulo: Saraiva, 2016.

MANDARINO JUNIOR, Raphael. **Reflexões sobre Segurança e defesa Cibernética**. In. BARROS, Otávio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS, Whitney Lacerda de (Orgs.). Desafios estratégicos para segurança e defesa cibernética. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. Disponível em: http:/livroaberto.ibict.br/handle/1/612. Acesso em: 12 jan. 2022.

MORIMOTO, Carlos E. **Dicionário Técnico de Informática.** 3ª Ed., 2005. Disponível em: http://www.dominiopublico.gov.br/download/texto/hd000001.pdf. Acesso em: 24 jan. 2022.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos:** Ameaças e Procedimentos de Investigação. 1. ed. Rio de Janeiro: Brasport, 2012.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos:** Ameaças e Procedimentos de Investigação. 2. ed. Rio de Janeiro: Brasport, 2013.