INTRODUÇÃO

A sociedade brasileira e mundial passou nas últimas décadas por diversas transformações nas mais variadas áreas e a conectividade via sistemas informatizados principalmente com o uso da internet é uma realidade irreversível. Esse novo modo de agir da sociedade, que sai do real para virtual trouxe inúmeras vantagens para a sociedade, mas também é inegável que tem pontos negativos e entre eles os crimes virtuais.

Os crimes virtuais têm características próprias e o direito como um todo deve se atualizar para enfrentá-los da melhor forma possível. Nessa esteira a legislação deve ser revista constantemente.

Ressalta-se que o enfrentamento aos crimes cibernéticos não deve ser visto apenas como uma questão do direito penal, o que seria resolvido com novas tipificações e uma política criminal especifica. Tal enfrentamento para trazer maior eficácia tem que ocorrer no âmbito de uma política pública, sendo assim um enfrentamento multissetorial, pois só assim será possível trazer segurança cibernética para os usuários de forma geral.

Desta sorte a primeira parte da pesquisa buscou-se apresentar os crimes virtuais no tocante ao seu surgimento, sua evolução, suas características que o diferem dos crimes comuns, exemplificando as novas tipificações penais e finalizando com a necessidade de um enfrentamento multissetorial via política pública.

Na segunda parte da pesquisa foi analisado o estado da arte das políticas públicas em relação a segurança cibernética com ênfase nos crimes virtuais, houve apresentação do conceito de política pública e foi verificado a existência de duas grandes normas afetas a este tema, quais sejam, o decreto nº 9.637 de 26 de dezembro de 2018, que instituiu a política nacional de segurança da informação-PNSI e o decreto nº 10.222 de 05 de fevereiro de 2020 que positivou a estratégia nacional de segurança cibernética, desta forma foi extraído os grandes nortes desses decretos no enfrentamento a insegurança cibernética e aos crimes virtuais. Ressaltou-se que existem outros diplomas legislativos que fortalecem o combate aos crimes virtuais, mas que a maioria são setoriais.

Na terceira parte desta obra se expôs a necessidade do contínuo aprimoramento das políticas publicas e da legislação penal e não penal. Houve a exposição do ciclo de políticas públicas, onde foi enfatizado a necessidade de percorrer todo esse ciclo para que se tenha melhores resultados.

A pesquisa foi prevalentemente do tipo teórica, com abordagem qualitativa de natureza básica, cuja lógica foi a dedutiva, com base teórica estruturalista, por meio de procedimento eminentemente bibliográfico.

1- CRIMES VIRTUAIS

As sociedades modernas tal qual são conhecidas hoje difere sobremaneira das sociedades antigas, onde a tecnologia é a principal marca dessa sociedade moderna, em que há uma conectividade jamais vista antes, seja entre pessoas, país ou empresas, tal conexão se dá por meio de rede de computadores, sobretudo pela internet.

Com o avanço dessa conectividade há atualmente uma estreita relação entre o mundo real e o mundo virtual, sendo praticamente impensável um mundo sem internet. Com esse avanço não houve apenas elementos positivos, mas também elementos negativos, e em especial o cibercrime ou crimes cibernéticos.

Os delitos passaram e passam por uma transformação, em que o ambiente virtual agora é o cenário, o espaço, onde eles ocorrem.

A denominação cibercrime (cybercrime, em inglês) surge pela primeira vez, no final dos anos 90, em reunião de um subgrupo envolvendo os sete países mais ricos do mundo e a Rússia. (D'URSO,2019).

Marcelo Crespo utiliza a denominação "Crimes Digitais" e cita algumas das diversas denominações dadas:

> Verificam-se, pois, várias denominações, dentre as quais "crimes de computador", "infrações por meio de computador", "crimes por meio de informática", "fraude informática", "delinquência informática", "crimes digitais", "computer-related crimes", "cybercrimes" ou "crimes cibernéticos". (CRESPO, 2011, p.47)

Elucidando o tema Vicente Greco Filho, diz:

> "Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes), e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é

> provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou.” (GRECO, 2000, p.85).

Destaca-se a escrita de Frabízio Rosa que conceitua os crimes virtuais da seguinte forma:

> “A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento dedados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; O ‘Crime de Informática’ é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; Assim, o ‘Crime de Informática’ pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável; Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública.”(ROSA, 2006, p. 55).

Tais crimes tem como características principais conforme labSEAD-UFSC (2020) a virtualidade; a interatividade; a ubiquidade; a pluriespacialidade, a anonimidade e; a velocidade, sendo que:

1. VIRTUALIDADE: Característica da imaterialidade que traz novas concepções humanas sobre as coisas. Aspecto dificultador na aplicação das normas jurídicas tradicionais.

2. INTERATIVIDADE: O ambiente é de total interação entre o usuário e o meio virtual, assim como entre os usuários da rede.

3. UBIQUIDADE: Possibilidade de um mesmo usuário estar em locais diferentes ao mesmo tempo.

4. PLURIESPACIALIDADE: O ciberespaço não tem lugar físico, fronteiras, limites territoriais ou dimensões mensuráveis.

5. ANONIMIDADE: Os usuários não possuem identificação civil aparente neste ambiente.

6. VELOCIDADE: A movimentação (criação, propagação etc.) dos elementos integrantes deste espaço ocorre em um dinamismo muito maior do que no mundo físico.

É cediço que o direito muda ao longo do tempo se adaptando as mudanças fáticas, desta forma acompanha a evolução da sociedade, por tanto em cada local, tempo, contexto

social, político ou moral da sociedade o direito se é diferente pois de adequa a necessidade daquele povo.

Desta forma é visto na sociedade moderna um avanço exponencial do modo como é praticado os delitos, e nesse avanço a legislação deve ser aprimorada para que haja um efetivo controle social sobre esses novos delitos.

Dentre os inúmeros crimes cometidos pela internet ou na internet tem-se os crimes contra a honra; o *cyberbuling* e o *cyberstalking;* crimes de ódio; pedofilia; *revenge-porn*; fraudes eletrônicas e outros.

O avanço do crime para o mundo virtual não é exclusividade do Brasil, sendo um problema mundial.

Nessa esteira não só o direito brasileiro como o direito fora do Brasil deve se aprimorar, uma vez que não há mais fronteiras para a consecução desses delitos.

E na busca desse aprimoramento legislativo surgiram no brasil algumas leis e algumas alterações legislativas, aprimorando a legislação para alcançar esses delitos, como por exemplo:

A) Invasão de dispositivo informativo, insculpido no artigo 154-A do CP, o qual diz:

> "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".

B) Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, previsto no artigo 266 do Código Penal.

C) Divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia, exposto no artigo 218-c do código penal, com causa de aumento se por motivo de humilhação ou vingança (*revenge porn*).

D) Furto mediante fraude por meio eletrônico ou informático, insculpido no artigo 155§4º-B e §4º- C do Código Penal, que dizem:

> "§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso: I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional; II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável."

E) Fraude eletrônica, prevista no artigo 171, §2-A e §2-B do código penal, os quais trazem a seguinte redação:

> "§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional."

Por tanto é visto que o direito penal tem tentado acompanhar o crescimento dos delitos virtuais com a tipificação de novos crimes com a finalidade de assim combater a ofensa a bens jurídicos penalmente tuteláveis.

Entretanto a proliferação de novos tipos penais por si só não é suficiente para o combate ao cibercrime, sendo necessária uma atuação mais ampla do Estado, e com base nessa constatação é que o Estado Brasileiro se debruçou para criar uma política pública par ao enfrentamento desses crimes e outros temas ligados a internet, o que será visto na próxima seção.

2- POLÍTICAS PÚBLICAS SOBRE SEGURANÇA CIBERNÉTICA – DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020 E O DECRETO Nº 9.637, DE 26 DE DEZEMBRO DE 2018.

O vocábulo "políticas públicas" possui diversas conotações, não existindo uma única definição única do que seja uma política pública, como ressalta Souza (2006).

Entre os diversos conceitos existentes na doutrina, destaca-se o de Heidemann (2009, pag.28) qual seja:

> "Em termos político-administrativos, o desenvolvimento de uma sociedade resulta de decisões formuladas e implementadas pelos governos dos Estados nacionais, subnacionais e supranacionais em conjunto com as demais forças vivas da sociedade, sobretudo as forças de mercado em seu sentido lato. Em seu conjunto, essas decisões e ações de governo e de outros atores sociais constituem o que se conhece com o nome genérico de políticas públicas."

Vale ressaltar que Romano (2009) diz que as políticas públicas também são entendidas como ações ou propostas promovidas pelo governo na tentativa do melhor uso dos recursos públicos, satisfazendo diferentes grupos sociais com interesses e anseios, que por vezes são divergentes e em outros momentos convergentes.

Nessa esteira, Saraiva (2006) ressalta que a política pública é feita de tomada de decisões com a finalidade de manter o equilíbrio social ou introduzir desequilíbrios com a finalidade de alterar a realidade diminuindo o problema social. Nessa linha, Secchi (2010) estabelece que uma política pública é uma ordem feita para enfrentar um óbice público, entretanto diz ser relevante apontar que não é pacífica a definição do que é política pública.

Ressalta-se que Souza (2006) concorda com as ideias de Secchi (2010) ao expor que inexiste uma definição uníssona para política pública, entretanto aduz que algumas características são relevantes, quais sejam: separar o que o governo planeja e o que, na realidade, faz; abrange diversos atores sociais e diversos níveis de decisão, mesmo sendo feita pelo governo; é vasto e não se restringe a leis e regras; absorve uma ação volitiva com objetivos definidos; pode trazer impactos de curto e longo prazo e engloba processos, em que é imprescindível planejar, implementar, acompanhar e avaliar.

Segundo Maria Paula Dallari Bucci: "As políticas públicas têm distintos suportes legais. Podem ser expressas em disposições constitucionais, ou em leis, ou ainda em normas infralegais, como decretos e portarias e até mesmo em instrumentos jurídicos de outra natureza, como contratos de concessão de serviço público, por exemplo." (BUCCI,2006). Por tanto inúmeras são as formas que uma política pública pode se apresentar.

A política pública sobre segurança cibernética adotou a forma de decreto, em que o decreto 10.222 de 5 de fevereiro de 2020, positivou a estratégia nacional sobre segurança cibernética o qual teve como fundamento também outro decreto, especificamente o inciso I do art. 6º do Decreto nº 9.637, de 26 de dezembro de 2018, sendo que este último instituiu a política nacional de segurança da informação.

Desta sorte o decreto 9.637/2018 institui a política nacional de segurança da informação, sendo dividido em 7(sete) capítulos, o primeiro capítulo traz as disposições gerais onde se destaca a finalidade da política nacional que é de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional.

No segundo capítulo é exposto os princípios da política nacional de segurança da informação. Já no terceiro capítulo é trazido os objetivos da política nacional, o qual destaca-se na presente pesquisa o insculpido no artigo 4º, III do referido decreto, o qual diz: "Art. 4º São objetivos da PNSI: III - aprimorar continuamente o arcabouço legal e normativo relacionado à segurança da informação". No quarto capítulo é exposto os instrumentos da PNSI, o qual salienta-se o positivado no inciso I do artigo 6, qual seja:

> "Art. 6º A Estratégia Nacional de Segurança da Informação conterá as ações estratégicas e os objetivos relacionados à segurança da

> informação, em consonância com as políticas públicas e os programas do Governo federal, e será dividida nos seguintes módulos, entre outros, a serem definidos no momento de sua publicação: I - segurança cibernética"

No quinto capítulo é constituído o comitê gestor da segurança da informação, trazendo sua atribuição, composição e forma de reunião. Já o sexto capítulo informa as competências de cada órgão do PNSI. Por derradeiro o sétimo capítulo expõem as disposições finais.

Desta forma o Decreto 9.637 de 2018 instituiu o plano nacional de segurança da informação – PNSI, sendo um instrumento primário de pouca concretização prática, mas de grande importância pois a partir dele que surgirá o aprimoramento das políticas públicas em relação a segurança da informação e ao combate aos crimes virtuais, escopo dessa pesquisa.

Com fundamento no decreto 9.637 de 2018 surgiu o decreto nº 10.222, de 5 de fevereiro de 2020

A Estratégia Nacional de Segurança Cibernética instituída no presente decreto tem caráter orientador, nela são expostas as principais ações do governo brasileiro tanto no âmbito interno quanto no âmbito internacional na área da segurança cibernética, e tal estratégia possui validade no período de 2020 a 2023.

O decreto é divido basicamente em 4(quatro) partes: a primeira com as considerações preliminares; a segunda com as linhas gerais da estratégia nacional de segurança; a terceira com o diagnóstico da situação atual e a quarta com a análise dos eixos temáticos. Os principais pontos do presente decreto no tocante aos crimes virtuais serão expostos a seguir.

As considerações preliminares esta dividia em 4(quatro) partes, a primeira diz respeito ao sumário, onde é exposto o porquê da existência da estratégia nacional e modo que ela foi elaborada, sendo fruto de diversas reuniões de trabalho de especialistas das mais variadas áreas.

Na segunda parte das considerações preliminares, chamada de introdução, há uma explicação do estágio atual da sociedade em relação ao uso da internet, com a denominada revolução industrial, a qual trouxe diversos benefícios sociais, econômicos, mas, por outro lado, surgem na mesma proporção ameaças virtuais que trazem riscos imensuráveis tanto a administração público com a sociedade em geral, nessa esteira é enfatizado o papel do Governo e de outros setores para que haja maior segurança cibernética, e é nesse espaço que a E-Ciber supre esta lacuna no arcabouço normativo brasileiro sobre segurança cibernética. É ressaltado que existem boas práticas nesta área, entretanto elas são fragmentadas e específicas, o que dificulta uma resolução mais apropriada e concentrada, ainda expõe que essa falta de um alinhamento normativo, estratégico e operacional, traz prejuízos ao aprendizado, inclusive com

retrabalhos, por fim afirma que a sociedade não é homogênea, tendo assim diferentes visões sobre o tema.

É trazido na terceira parte das considerações preliminares, a qual se refere a metodologia adotada para a consecução da estratégia nacional, onde foi adotada como metodologia reuniões com representantes de órgãos públicos, de entidades privadas, e do meio acadêmico, tais reuniões foram divididas em 3 subgrupos: o primeiro referente a governança cibernética, dimensão normativa, pesquisa, desenvolvimento e inovação, educação, dimensão internacional e parcerias estratégicas, o segundo em relação a confiança digital e prevenção e mitigação de ameaças cibernéticas e o terceiro tratou da proteção estratégica, proteção do Governo e proteção às infraestruturas. Trazendo melhor dinâmica aos debates o trabalho foi dividido em quatro etapas, quais sejam: a primeira referente ao diagnóstico com o levantamento e mapeamento de iniciativas, atores relacionados e ações existentes; a segunda com debates dos subgrupos em reuniões semanais com os atores relacionados e convidados de notório saber; a terceira com a consulta pública com disponibilização do documento na internet para contribuições e ampla participação da sociedade em geral; e a quarta com a aprovação e publicação levada para a finalização da proposta e submissão à aprovação presidencial.

Por fim na quarta e última parte das considerações preliminares é trazido a concepção estratégica, a qual é fruto da análise dos eixos temáticos, da visão e dos objetivos estratégicos.

Na segunda parte do decreto é consolidada a estratégia nacional de segurança cibernética, a qual se cinge em três compartimentos, o primeiro expõe a visão para que o Brasil se torne um país de excelência em segurança cibernética, o segundo positiva os objetivos da estratégia, que são três: 1. Tornar o Brasil mais próspero e confiável no ambiente digital; 2. Aumentar a resiliência brasileira às ameaças cibernéticas; e 3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional.

Por fim no terceiro compartimento é trazido as ações estratégicas, que são no total de 10(dez) ações estratégicas, quais sejam: 1. Fortalecer as ações de governança cibernética; 2. Estabelecer um modelo centralizado de governança no âmbito nacional; 3. Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade; 4. Elevar o nível de proteção do Governo; 5. Elevar o nível de proteção das Infraestruturas Críticas Nacionais; 6. Aprimorar o arcabouço legal sobre segurança cibernética; 7. Incentivar a concepção de soluções inovadoras em segurança cibernética; 8. Ampliar a cooperação internacional do Brasil em Segurança cibernética; 9. Ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade; 10. Elevar o nível de maturidade da sociedade em segurança cibernética.

Para a presente pesquisa deve-se analisar a estratégia referente ao aprimoramento do arcabouço legal, e nesse diapasão o decreto diz que deve ser revisado e atualizado os normativos existentes, abordando novas temáticas e elaborando novos instrumentos. O decreto exemplifica algumas ações que podem ser realizadas, tais como: identificar e abordar temas ausentes na legislação vigente; realizar esforços no sentido de incluir, no código penal, novas tipificações de crimes cibernéticos; elaborar normativos sobre tecnologias emergentes; criar políticas de incentivo para contratação de mão de obra especializada em segurança cibernética; definir requisitos de segurança cibernética nos programas de trabalho remoto; e elaborar, sob coordenação do Gabinete de Segurança Institucional da Presidência da República, um anteprojeto de lei sobre segurança cibernética, com diretrizes que proporcionarão alinhamento macro estratégico ao setor e contribuir de forma decisiva para elevar a segurança das organizações e dos cidadãos.

Desta forma é imprescindível para um combate eficiente aos crimes virtuais ações estratégicas em diversas frentes, sendo o aprimoramento do ordenamento jurídico primordial para o enfrentamento desses delitos.

Na terceira parte do decreto 10.222 de 2020 é exposto o diagnóstico do uso da internet no mundo e no Brasil, dos danos causados pelos ataques cibernéticos e do nível de segurança no mundo e no Brasil.

Segundo o diagnóstico em 2018, mais da metade da população mundial utilizou a internet (quatro bilhões e cem milhões de usuários, o que representa cinquenta e quatro por cento da população mundial), sendo noventa e três por cento dos acessos a redes sociais realizados via dispositivos móveis.

Portanto a conectividade das pessoas de forma simultânea através da internet ou redes particulares cresceu muito trazendo comodidade e agilidade para os usuários que podem realizar as mais diversas atividades pelos seus dispositivos.

Mas a referida conectividade não trouxe apenas aspectos positivos, pois daí adveio uma quantidade enorme de vulnerabilidades cibernéticas causando prejuízos de toda ordem para as pessoas, empresas e administração pública.

O decreto expõe que o dano financeiro é de grande monta e que os ataques cibernéticos causam perdas estimadas em US$ 600.000.000.000,00 (seiscentos bilhões de dólares) no mundo inteiro por ano. Nesse cenário as economias estão empenhadas em aumentar o seu grau de resiliência e o a sua segurança cibernética, onde os investimentos do setor privado e do Governo são altíssimos nessa área.

É destacado no diagnostico apresentado no decreto que o Brasil é um dos maiores mercados de telecomunicações do mundo e que a disseminação de códigos maliciosos perpetrados pelo crime organizado já é uma realidade.

Ainda é trazido no decreto 10.222 de 2020 diversos dados referentes à conectividade do Governo, do setor privado e dos cidadãos, aos índices globais e aos crimes cibernéticos, dentre os quais se destaca que em 2017, foram setenta milhões e quatrocentas mil vítimas de crimes cibernéticos.

Segundo o Relatório da "**Internet Organised Crime Threat Assessment** - IOCTA", de 2018, da Agência da União Europeia para a Cooperação Policial - Europol, "a falta de legislação adequada sobre crimes cibernéticos fez com que o Brasil fosse o alvo número um e a principal fonte de ataques **online** na América Latina; 54% dos ataques cibernéticos reportados no Brasil supostamente são originários de dentro do país".

O diagnostico alerta para a importância que as organizações sejam elas públicas ou privadas, criem políticas e procedimentos de segurança cibernética e que elas sejam atualizadas constantemente tendo em vista que a evolução tecnológica não para, e devem especializar seus processos com constante treinamento de todos os envolvidos.

Ressalta-se ainda que há diversas iniciativas do Governo para o uso da internet como a Política de Governança Digital positivada no Decreto nº 8.638, de 15 de janeiro de 2016, a Estratégia Brasileira para a Transformação Digital - E-Digital exposta no Decreto nº 9.319, de 21 de março de 2018 e a governança no compartilhamento de dados insculpida no Decreto nº 10.046, de 9 de outubro de 2019, diplomas esses que demonstram a inclusão do Governo na era digital.

É enfatizado que aperfeiçoar os instrumentos legais é primordial para o Brasil o que contribui para a proteção dos sistemas e redes governamentais protegendo-os contra interrupções, vazamento de dados ou outras ações danosas.

Foi observado que dados governamentais e sistemas de governo são alvos compensadores para ações criminosas, no intuito de provocar diferentes danos. Os ataques se mostram de grande monta quando atingem serviços estruturais do Estado.

Diante desse cenário o decreto traz na sua última parte a especificações dos eixos temáticos que auxiliam formulação das ações estratégicas, sendo dois os grandes eixos, o primeiro eixo temático se refere à área de proteção e de segurança, compostos das seguintes dimensões: a governança da segurança cibernética nacional, o universo subconectado e seguro, a prevenção e mitigação de ameaças cibernéticas, e a proteção estratégica. Já o segundo eixo é

chamado de transformadores, assim ditos pelo potencial que tem de transformar, de forma decisiva e estruturante, os temas por eles subjugados e possui as seguintes dimensões: a dimensão normativa, a pesquisa, desenvolvimento e inovação, a dimensão internacional e parcerias estratégicas, e a educação.

Na presente pesquisa será detalhado o a dimensão normativa do eixo transformador, pois ao falarmos do combate dos crimes virtuais via política pública tem-se como mais importante o arcabouço legal. Ressalta-se que os demais eixos têm grande relevância também para a diminuição de crimes cibernéticos.

A dimensão normativa do eixo transformador trazido pelo decreto relaciona explana inicialmente o crescente uso da internet e com o consequente aumento da criminalidade por essa via, surgindo assim os crimes cibernéticos ou crimes virtuais. Esses delitos conforme já exposto vão desde crimes que ofendem a honra da pessoa, como calúnia, difamação, injúria e **bullying**, até crimes que violam a privacidade do cidadão ou atentam contra seu patrimônio.

Ressalta-se que surgiram no período recente alguns diplomas legislativos no afã de combater esses delitos, dentre os quais destacam-se: a Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet e a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais - LGPD, mas segundo o exposto no decreto 10.222/2020: "o nível de articulação e de normatização das instituições brasileiras nos temas relacionados à segurança cibernética ainda é tímido, e exigem esforço adicional.".

Por tanto uma ação coordenada para normatizar os delitos virtuais e outros temas correlatos é de suma importância.

Frisa-se que no ano de 2012, foram criados dois diplomas legislativos importantes para combater os crimes virtuais, tais leis alteraram o Código Penal, tipificando condutas antes não alcançadas pela legislação penal.

Essas leis são: 1- Lei nº 12.737, de 30 de novembro de 2012, conhecida como "Lei Carolina Dieckmann", que tipificou condutas relacionadas a invasão de dispositivos; e a Lei nº 12.735, de 30 de novembro de 2012, que obriga a criação de delegacias especializadas em crimes virtuais.

Importante o alerta trazido pelo decreto para a ausência de segurança jurídica em relação a investimentos na economia digital, uma vez que falta de normatividade específica nessa área.

Importante instrumento normativo é a Lei nº 12.965, de 2014 - Marco Civil da Internet, que regula o uso da internet no Brasil por meio da previsão de princípios, de garantias, de direitos e de deveres para quem utiliza a rede mundial de computadores, e de diretrizes para a

atuação do Estado, protegendo os dados pessoais e a privacidade dos usuários da internet, o que é tratado, de modo mais direto e assertivo, pela LGPD.

A publicação, em agosto de 2018, da LGPD mencionada, reforçou a necessidade das organizações em realizar investimentos em sua estrutura e em adotar políticas internas que atendam às exigências de segurança voltadas ao tratamento dos dados pessoais.

Este é o arcabouço jurídico básico em relação a segurança cibernética e ao combate aos crimes virtuais.

3- (DES)NECESSIDADE DE APRIMORAMENTO DAS POLÍTICAS PÚBLICAS E DIPLOMAS NORMATIVOS

Conforme visto no tópico anterior existem diversas normas atuais e modernas em relação ao uso da internet e a tipificação de condutas, mas, segundo o decreto 10.222 de 2020, o intenso avanço da tecnologia e o consequente redesenho das relações humanas no espaço cibernético enseja análises periódicas desses valiosos instrumentos legais, no intuito de sempre preservar seus nobres pilares democráticos de liberdade de expressão e de livre trânsito de opiniões.

A outra frente de trabalho apontada pela Estratégia Nacional de Segurança Cibernética refere-se aos instrumentos normativos de competência do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, direcionados aos órgãos da Administração Pública federal, que visam ao aperfeiçoamento e à atualização das diretrizes operacionais e dos requisitos relativos ao tema. Após a criação do então Departamento de Segurança da Informação e Comunicações, em 2006, o Gabinete de Segurança Institucional da Presidência da República dedicou-se intensamente à temática. Como resultado, desde 2008, foram publicadas três Instruções Gerais e vinte e duas Normas Complementares, de forma a contemplar os assuntos relacionados à Segurança da Informação. Devido às características evolutivas do tema, tais instrumentos necessitam de apreciação e de revisão constantes.

Ainda o decreto 10.222 de 2020 expõe a necessidade de uma lei para disciplinar diversos aspectos da segurança cibernética, uma vez que todo o arcabouço normativo existente é insuficiente para o adequado enfrentamento do tema no Brasil. Essa insuficiência decorre da natureza infralegal dos instrumentos existentes, e faz com que se restrinjam à Administração Pública federal, de forma a não se aplicar, desse modo, aos demais entes do Poder Público, e a não contemplar, ainda, o setor produtivo, dentre os quais, os fornecedores de serviços essenciais, e a sociedade em geral.

Fora isso, frisa-se que a segurança cibernética apresenta novo paradigma em relação a segurança para o Estado, visto que todos os atores nacionais possuem vulnerabilidades que podem ser exploradas por uma ameaça cibernética que adquira grande repercussão, de forma a colocar em risco até mesmo a estabilidade das instituições nacionais, conforme enfatizado ao final do decreto sobre a estratégia nacional em segurança cibernética.

O decreto ressalta ainda que a segurança cibernética deve ser compreendida de uma forma holística e multissetorial, pois restringi-la apenas aos órgãos governamentais, com a ausência do setor privado e sem um ter em mente o usuário final de todas as tecnologias que usam o espaço cibernético é um grande equívoco.

Segundo o decreto 10.222 de 05 de fevereiro de 2020:

> "uma lei sobre segurança cibernética teria o condão de alinhar ações de governança e de conformidade nesse tema, a partir de um patamar único, ao vincular os diversos atores nacionais aos princípios e regramentos propostos. A economia digital, a inserção do Brasil na Indústria 4.0 e o alcance dos Objetivos de Desenvolvimento Sustentável elegidos pelas Organização das Nações Unidas, exigem que o País tenha condições de construir a confiança e a segurança necessárias para o desenvolvimento nacional na era da informação.
>
> Sob essa ótica, indicam-se ações que aprimorem o arcabouço legal da segurança cibernética nacional, por acreditar que essa iniciativa poderá proporcionar o necessário alinhamento estratégico e normativo às ações do País nessa área, de forma a ressaltar que deve ser atribuída especial atenção às políticas em segurança cibernética voltadas ao setor produtivo, as quais, pela natural força advinda do mercado, tendem a ser mais bem-sucedidas que aquelas dedicadas exclusivamente às ações do setor público e à fiscalização regulatória.
>
> Recomenda-se, ainda, no sentido de permitir a elaboração de instrumentos com a maior legitimidade possível, a criação de mecanismos que ensejem a participação da iniciativa privada e da academia para troca de experiências, para exploração de práticas internacionais, para discussão de padrões e de melhores práticas no tema e apoio às decisões da entidade central."

Desta forma a estratégia nacional de segurança cibernética é muito assertiva quando esclarece a importância do envolvimento de todos os atores na consecução das políticas públicas nesta área e ressalta que uma lei sobre segurança cibernética iria trazer mais segurança jurídica no Brasil.

Deve se salientar que não basta fazer a política pública ou ampliar o arcabouço legislativo para combater os crimes virtuais, é preciso também ter uma constante avaliação e atualização. Por isso seguir o ciclo de políticas públicas se faz necessário.

O ciclo de políticas nada mais é que um "esquema de visualização e interpretação que organiza a vida de uma política pública em fases sequenciais e interdependentes" (SECCHI, 2010). O número de fases e as fases variam na literatura, mas todos os doutrinadores apresentam as fases da formulação, implementação e avaliação (FREY, 2000).

Na política pública referente a segurança cibernética, que engloba o combate aos crimes virtuais, é importante que haja uma avaliação periódica e assim o aperfeiçoamento dessa política. Uma política publica dessa envergadura não se encerra com sua implementação, precisa ser constantemente avaliada e recriada para que seu objetivo seja alcançado.

CONSIDERAÇÕES FINAIS

A partir da análise do avanço da sociedade brasileira e mundial, verificou-se que a conectividade e a velocidade com que ocorrem as trocas de informações hodiernamente transformou a realidade fática. Essa transformação trouxe-se diversos pontos positivos para o mundo de forma geral, entretanto adveio daí também pontos negativos.

Entre os fatos adversos está a insegurança cibernética, e dentre os resultados dessa insegurança surgiu os crimes virtuais. Desta forma foi visto os principais conceitos e características desses novos delitos.

Foi examinado o modo como o direito brasileiro combateu os crimes cibernéticos, primordialmente com a proliferação de novos tipos penais acrescentados no Código Penal, com destaque para o artigo 154-A(invasão de dispositivo informático); art.266(Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública); artigo 218-c (Divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia); artigo 155§4º-B e §4º- C(Furto mediante fraude por meio eletrônico ou informático) e ; artigo 171, §2-A e §2-B(Fraude eletrônica).

Foi concluído que apenas a resposta penal por meio de novos tipos não é suficiente para combater os crimes cibernéticos, devendo existir uma resposta multissetorial através de uma política pública.

A pesquisa seguiu expondo o conceito de política público e suas características, bem como o tipo de diploma legislativo pelo qual uma política pública é feita.

Em seguida verificou-se a existência de dois grandes decretos referentes ao enfrentamento a insegurança cibernética e aos crimes cibernéticos. O primeiro decreto analisado foi o de número 9.637, de 26 de dezembro de 2018**,** o qual instituiu a Política Nacional de Segurança da Informação-PNSI, sendo detalhado seus objetivos, princípios, instrumentos e principais atores. O segundo decreto examinado foi o de número 10.222, de 5 de fevereiro de 2020 que institui a estratégia nacional de segurança cibernética, onde foi visto o estado atual da proteção à ataques virtuais do Brasil e de que forma o governo e demais atores devem atuar nesse enfrentamento. Nessa esteira foi enfatizado o estágio atual do arcabouço normativo nacional para o combate aos crimes virtuais.

Restou patente que ainda há muito o que se fazer no âmbito das políticas públicas e no aperfeiçoamento do ordenamento jurídico pois ainda há diversas lacunas legais bem como é necessário o constante aprimoramento das políticas públicas, nesse sentido foi exposto a importância da fase avaliativa do ciclo de políticas públicas.

A presente trabalho dessa forma concluiu que é insuficiente o aparato legal existente, mas já houve grande avanço normativo com o decreto 9.637, de 26 de dezembro de 2018 e o decreto 10.222, de 5 de fevereiro de 2020.

Também se considera que os atores responsáveis pelo enfrentamento a insegurança cibernética e aos crimes virtuais devem aprimorar os diplomas legais, uma vez que existem lacunas normativas. Igualmente é exigível que atualizem as políticas públicas existentes com base em avaliação periódica.

REFERÊNCIAS BIBLIOGRÁFICAS:

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2023]. Disponível em: planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 jul. 2023.

BRASIL. **Decreto-Lei n.º 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, [2023]. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/del2848compilado.htm. Acesso em: 11 jul. 2023.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014.

Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 jul. 2023.
BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em: 28 jul. 2023.
BUCCI, Maria Paula Dallari. O conceito de política pública em direito. In: BUCCI, Maria Paula Dallari (org.). **Políticas públicas: reflexões sobre o conceito jurídico**. São Paulo: Saraiva, 2006.
CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1ª Ed. São Paulo: Saraiva, 2011.
D'URSO,Filizzola Luiz. **Em Tempos de Cibercrimes.** 2019. Disponível em:https://www.migalhas.com.br/dePeso/16,MI310551,31047-Em+tempos+de+cibercrimes. Acesso em: 05 ago. 2023.
FREY, K. **Políticas públicas: um debate conceitual e reflexões referentes à prática da análise de políticas públicas no Brasil**. Planejamento e Políticas Públicas, Brasília, DF, n. 21, p. 211-259, jun. 2000. Disponível em: http://www.ipea.gov.br/ppp/index.php/PPP/article/view/89/158 Acesso em: 23 jul. 2023.
GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet.**Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.
HEIDEMANN, Francisco G. **Do sonho do progresso às políticas de desenvolvimento**. In:; HEIDEMANN, Francisco G.SALM, José F. (Org.). Políticas públicas e desenvolvimento: bases epistemológicas e modelos de análise. Brasília: EdUnB, 2009.
INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2018. EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION, EUROPOL. Disponível em: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018> Acesso em: 10 jul. 2023.
ROMANO, Jorge O. **Política nas políticas públicas: um olhar sobre a agricultura brasileira**. Seropédica: Mauad X, 2009.
ROSA, Fabrizio**. Crimes da Informática**. 1ª Ed. Campinas. Bookseller, 2006.
SARAIVA, Enrique. **Introdução à teoria da política pública**. In: SARAIVA, Enrique; FERRAREZI, Elisabete (Org.). Políticas públicas. Brasília: Enap, 2006, v. 1, p. 21-42.
SECCHI, Leonardo. **Políticas públicas: conceitos, esquemas de análise, casos práticos.** São Paulo: Cengage Learning, 2010.
SOUZA, Celina. **Políticas públicas: uma revisão da literatura**. Sociologias, Porto Alegre, v. 8, n. 16, p. 20-44, jul./dez. 2006.
UNIVERSIDADE FEDERAL DE SANTA CATARINA. **Laboratório da Secretaria de Educação a Distância (labSEAD-UFSC).** Florianópolis, 2020. Disponível em: http://lab.sead.ufsc.br/. Acesso em: 2 ago. 2023.