CRIMES CIBERNÉTICOS: O ESTELIONATO VIRTUAL E A INSUFICIÊNCIA INVESTIGATIVA E JUDICIÁRIA

Cyber crimes: the virtual establishment and the investigative and judicial insufficiency

Hebert Josiel Gonçalves de Freitas[1]
Camila Soares Gonçalves[2]

Resumo: O cibercrime pode ser caracterizado como um tipo de violência que se pratica contra vítimas inocentes com o objetivo de promover alguma causa ou percepção do mundo. A definição de cibercrime é diferente em cada país, visto que o Direito Internacional, não o conceitua de forma unificada. O cibercrime é considerado hodiernamente um dos principais males que assolam a humanidade, ameaçando a democracia, a paz e a segurança mundial. De todo modo, percebe-se que são várias as razões para não ser possível conceituar unanimemente o conceito, bastando às definições acima apresentadas para que seja iniciada a abordagem da presente pesquisa. Não é de se assustar e fácil de acreditar que grupos terroristas como a Al-Qaeda utilizam a rede para comunicação, estratégias e recrutamento, como uma empresa recrutando funcionários para suas empresas. O cibercrime não está previsto legalmente em diplomas legais pátrios, portanto é necessário, partir dele, para tentar elaborar um conceito válido de cibercrime.
Palavras-chave: Cibercrime – Era Tecnológica – Estelionato Virtual

Abstract: Cybercrime can be characterized as a type of violence that is practiced against innocent victims in order to promote some cause or perception of the world. The definition of cybercrime is different in each country, since international law does not conceptualize it in a unified way. Cybercrime is today considered one of the main evils that plague humanity, threatening democracy, peace and world security. In any

[1] Aluno do curso de Bacharel em direito ela Faculdade Minas Gerais - FAMIG
[2] Mestre em Direito Privado pela FUMEC.
Especialista em advocacia cível pela ESA OAB/MG e em Direito Tributário pela PUC Minas.
Professora da pós-graduação da Escola Superior de Advocacia da OAB MG, PUC Minas, Portal IED (Instituto Elpídio Donizetti), CEDIN e FEAMIG.
Também das graduações na Faculdade Minas Gerais (FAMIG), COTEMIG e Alis.
Membro da Comissão de Educação Jurídica e Gestão, Empreendedorismo e Inovação da OAB/MG.
Palestrante.

case, it is clear that there are several reasons for not being able to unanimously conceptualize the concept, just the definitions presented above are enough to start the approach of this research. It is not frightening and easy to believe that terrorist groups like Al-Qaeda use the network for communication, strategies and recruitment, like a company recruiting employees for its companies. Cybercrime is not legally provided for in national legal acts, so it is necessary, starting from it, to try to elaborate a valid concept of cybercrime.
Keywords: Cybercrime - Technological Era - Estelionato Virtual

1. Introdução

Este trabalho foi desenvolvido com o viés de demonstrar a eficácia da lei no combate aos crimes cibernéticos. Essa modalidade de crime que para muitos é vista como uma novidade, já vem atingindo a população cibernética há tempos.

O mundo inteiro passou a ouvir falar de terrorismo e crimes cibernéticos a partir do famoso “BUG DO MILÊNIO”, evento ocorrido na virada do século e no qual a maior ameaça foi justamente aos serviços de informática e as redes de computadores.

Não que nessa época não existiam tais crimes, mas após esse episódio não só o mundo teve conhecimento, mas as grandes empresas iniciaram uma força tarefa na intenção de preservar seus sistemas de informática e informação, sendo esse o cerne do presente trabalho.

No primeiro capítulo fora aborado o conceito de crime cibernético e a Lei 12.737/2012, criada na intenção de legislar sobre os crimes que afetam as redes mundiais, além de apresentar as peculiaridades entre os conceitos de terrorismo e ciberterrorismo, e crimes cibernéticos

O crime cibernético de estelionato virtual é abordado no capítulo 2, onde se aprofunda sobreo Código Penal e a dificuldade em legislar sobre crimes cibernéticos.

No terceiro capítulo fora feita uma abordagem sobre os procedimentos de investigação, suas caracteristicas e peculiaridades, além de apresentar as vulnerabilidades cibernéticas.

No quarto e último capítulo a abordagem é feita sobre as consequências jurídicas no mundo virtual.

Utilizou-se o método hipotético dedutivo no presente trabalho,

pretendendo uma reflexão sobre como esses crimes são atuais, mas que já estão presentes mundialmente há algumas decadas.

2. Crimes cibernéticos e a lei 12.737/2012: aspectos gerais

O crime de terrorismo está atrelado aos crimes cibernéticos.Porém, quanto ao seu objetivo, não restam dúvidas de que são atos praticados com fim de ameaçar, amedrontar e, até mesmo, lesar a vida ou patrimônio de outrem, em nome da defesa ou para a consecução de um ideal, normalmente fruto de intolerância política, religiosa ou social, é o que discorre Fabiani Borges (2015).

Vive-se em uma era tecnológica, mais conhecida e denominada como “Era Digital” e se hoje tudo gira em torno dessa era, e se tudo evolui rapidamente, infelizmente os crimes também passam por mudanças e apresentam suas novidades.

Atualmente surgiu a modalidade do Terrorismo Cibernético ou o ciberterrorismo, que é conceituado por Rodrigo Santos (2020) como sendo diferente de tudo o que foi apresentado até então, já que ele envolve uma ação pontual, mas devastadora para as vítimas, pode afetar diversas vítimas de maneira inesperada e ágil, algo como o que aconteceria em um ato de terrorismo tradicional.

Santos (2020) discorre ainda que nos casos de guerra cibernética, existem pessoas que não acreditam ser possível equiparar o termo digital com o originário, mas neste caso, a associação é ainda mais fácil.

Não é de se assustar e fácil de acreditar que grupos terroristas como a Al-Qaeda utilizam a rede para comunicação, estratégias e recrutamento, como uma empresa recrutando funcionários para suas empresas.

Nesse sentido, Fabiani Borges (2015), explana que o surgimento das redes sociais, por exemplo, trouxe a possibilidade de captação de novos membros extremistas, e a mera postagem de fotos nas mesmas redes permite, através dos sistemas de georreferenciamento, a localização de tais membros e sua capacitação para a organizada facção do terror.

Assim, como fruto do ciberterrorismo nasceu o ciberterror, que é o trauma e medo constante de um possível novo ataque, uma consequência real e que faz muitas vítimas a todo instante, afetando inclusive países que não sofreram com o

ato, mas por estarem em conflitos internacionais estão mais suscetíveis a crer em falsas ameaças (SANTOS, 2020).

Essa cultura do medo foi rapidamente adotada em diversos cibercrimes e ciberguerras ao longo da história, pois o medo do improvável é fortificado com o desconhecimento sobre tecnologia e as possibilidades no uso de redes ao redor do mundo.

Os praticantes desses ataques, os ciberterroristas, querem chamar a atenção e, para isso, podem preferir atacar sistemas públicos como governo, hospitais, programas de segurança pública e qualquer outro alvo que possa fazer com que a população duvide da supremacia do próprio governo e com isso cause conflitos internos e o país também sofra com as pressões externas (BORGES, 2015).

As motivações de um ato de terrorismo cibernético pode envolver política, como no caso de uma guerra cibernética, mas também pode girar em torno de razões ideológicas, uma discordância nada amigável contra um grupo de pessoas.

2.1 Características e peculiaridades

A associação entre terrorismo e ciberterrorismo, ou crimes cibernéticos, dá-se pelo fato de que as 2 (duas) atividades estão ligadas a uma forma de trazer medo a um lugar e a sua população.

Nesse sentido Rodrigo Santos (2020) dispõe que:

> A partir do ciberterrorismo também **nasceu o ciberterror**, considerado um trauma e um medo constante de um possível ataque, uma consequência real e que faz muitas vítimas a todo instante, afetando inclusive países que não sofreram com o ato, mas por estarem em conflitos internacionais estão mais suscetíveis a crer em falsas ameaças (SANTOS 2020).

Além disso, existe o terrorismo cibernético, que envolve uma ação pontual, mas devastadora para as vítimas. Esse tipo de terrorismo pode afetar diversas vítimas de maneira inesperada e ágil, algo como o que aconteceria em um ato de terrorismo tradicional (TANGERINO, 2020).

Para a prática do ciberterrorismo são utilizadas algumas formas como, por exemplo: vírus, cavalo de troia, *worms*[3], *spywares*[4] e *SPAM*[5]. Matheus Souza Costa (2017) dispõe que essas formas são meios iniciais de ciberataque que são utilizados por possuírem uma grande capacidade de difusão no meio tecnológico. Assim, a característica do ciberterrorismo é difundir o pânico, terror ou medo a fim de atingir grande quantidade de pessoas.

Dessa forma, fica evidente que os vírus, cavalo de troia, worms, spywares e SPAM, sozinhos, não podem provocar pânico na sociedade, uma vez que é necessário que o ciberterrorismo, ao realizar um ataque, tenha o dolo de causar medo, terror ou pânico nos sujeitos e que tenha um sujeito que pratique esses atos (COSTA, 2017).

Nesse seguimento, somente se os vírus e demais formas forem utilizados para causarem pânico em massa é que eles poderão ser considerados como armas do ciberterrorismo. Dessa forma, as armas utilizadas pelo ciberterrorismo são diferentes do terrorismo convencional, sendo a principal delas a internet.

A Constituição Federal de 1988, em seu artigo 5º, XLIII, indica ao legislador brasileiro que realize uma previsão ao crime de terrorismo. Com isso, foi editada pelo Legislativo, a referida Lei 13.260/2016, que dispõe no artigo 2º, parágrafo 1º, o que são atos de terrorismo:

> O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública (BRASIL, 1988).

Além disso, a Constituição elencou esses atos considerados como ciberterrorismo, como demonstrou Dayane Tangerino, sendo eles:

> – usar ou ameaçar usar, transportar, guardar, portar ou trazer consigo explosivos, gases tóxicos, venenos, conteúdos biológicos, químicos,

[3] Programa semelhante aos vírus, com a diferença de este ser auto-replicante, ou seja, ele cria cópias funcionais de si mesmo e infecta outros computadores. Tal infecção pode ocorrer através de conexões de rede locais, Internet ou anexos de emails.

[4] Software espião que costuma ser instalado no celular ou no computador sem o consentimento do usuário. Uma vez no computador, o programa monitora as atividades online, o histórico e os dados pessoais, para repassar as informações para terceiros.

[5] Termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE (do inglês Unsolicited Commercial E-mail).

> nucleares ou outros meios capazes de causar danos ou promover destruição em massa;
> – sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou servindo-se de mecanismos cibernéticos, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento.
> – atentar contra a vida ou a integridade física de pessoa (TANGERINO 2020).

Destarte, após apresentar de forma clara um conceito de ciberterrorismo é necessário aduzir sobre a (in)eficácia da lei no combate ao crime.

3. Estelionato virtual: o desafio o código penal na atualidade

O fator criminógeno virtual cresce de forma a fazer surgirem crimes novos, além de potencializar alguns dos já existentes. Muitos desses crimes são cometidos através da internet ou com o uso do computador.

Desse modo, é criada uma nova esfera de atuação delituosa, a saber, os chamados crimes virtuais ou cibercrimes (como são chamados os crimes praticados com o uso do computador ou crimes praticados pela internet) (LIMA, 2014).

> O marco inicial do desenvolvimento tecnológico propriamente dito, e considerado assim por muitos autores, teria se dado em 1957, quando, o então presidente dos Estados Unidos, John Kennedy, em contrapartida ao lançamento do primeiro satélite artificial pela antiga União Soviética, prometeu enviar um americano para a lua e criar um sistema de defesa à prova de destruição. Dessa forma, tendo em vista tal objetivo, foi criada a Agência de Investigação de Projetos Avançados (LIMA, 2014).

Os usuários da internet que não têm a devida cautela com os dados pessoais inseridos na rede têm mais chances de serem vítimas de crimes cometidos no ambiente virtual, uma vez que, ao inserir as informações em sites que não possuem uma segurança adequada, os dados ficam suscetíveis de utilização pelos criminosos.

Dentre as diversas classificações doutrinárias para estes tipos de crime, os crimes virtuais aponta-se Ivette Senise Ferreira que os classifica como:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e

> dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial (FERREIRA, 2017).

Os crimes informáticos são basicamente os mesmos que ocorrem fora do mundo virtual. A internet pode sim facilitar a vida de todos, porém, alguns criminosos se aproveitam da falta de cuidado dos internautas para coletar informações pessoais capazes de, por exemplo, permitir o acesso à conta bancária do usuário. Abaixo, analisam-se alguns dos crimes praticados virtualmente.

Nesse sentido, Maria Helena Junqueira Reis lembra:

> A gama de delitos que podem ser perpetrados pela Internet é quase infinita. A lista inclui o mau uso dos cartões de crédito, ofensas contra a honra, apologia de crimes, como racismo, ou incentivo ao uso de drogas, ameaças e extorsão, acesso não autorizado a arquivos confidenciais, destruição e falsificação de arquivos, programas copiados ilegalmente e até crime eleitoral (propaganda não autorizada, por exemplo) dentre outros (REIS, 2017)

Como nos casos praticados no mundo real, de acordo com o art. 171 do Código Penal, há o estelionato quando o criminoso induz a vítima a erro com o objetivo de obter vantagem ilícita para si ou para outrem (BRASIL, 2015).

> Artigo 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa (BRASIL,1940).

Abaixo, temos um exemplo de um crime desta natureza, veja-se a decisão do Tribunal de Justiça do Estado de São Paulo:

> EMENTA – Art. 171, caput, do Código Penal – Autoria e materialidade demonstradas – Réu que obteve vantagem ilícita, em prejuízo da vítima, que depositou numerário na conta bancária dele, pela compra de um notebook, pela internet, e não recebeu o produto. Penas e regime prisional corretamente fixados. Recurso não provido (TJSP, 2015).

Quando praticado de maneira ordinária, ou seja, em sua forma típica, o crime de estelionato sintetiza-se essencialmente na possibilidade em que o autor delituoso encontra para obter proveito de modo ilícito, para si, ou para outrem, utilizando-se de meios fraudulentos para tanto (FEITOZA, 2012).

O ordenamento jurídico brasileiro versa que somente a pessoa física pode ser sujeito ativo do crime de estelionato, cometendo-o de forma dolosa, com livre e consciente vontade, embora possa agir de modo diverso para alcançar seus fins. Em

contrapartida, o sujeito passivo desta modalidade será a vítima que sofreu o prejuízo patrimonial, devendo ser pessoa certa e determinada, embora muitas vezes exista mais de um indivíduo envolvido na relação (FEITOZA, 2012).

Trata-se de um dos crimes mais comuns praticados pelo computador ou fora dele. É necessário que a vítima seja enganada pelo criminoso. Os casos que acontecem com mais frequência ocorrem quando os infratores criam sites de vendas (ou oferecem produtos em sites de vendas já existentes), e anunciam mercadorias que não estão realmente à venda (MALHEIRO, 2017).

O falso vendedor espera as vítimas entrarem em contato, informa dados para depósito bancário, ou emitem boleto, e após o pagamento ser reconhecido, congelam o domínio de seus sites, de forma que estes não sejam mais localizados, deixam de atender aos telefonemas e não respondem mais às mensagens dos consumidores, praticando, dessa forma, um crime virtual.

4. Procedimentos de investigação: caracteristicas e peculiaridades

A globalização e a consequente difusão da internet e dos dispositivos eletrônicos de comunicação, tais como smartphones, computadores e tablets, ao mesmo tempo que favoreceram a instantânea troca de informações, otimizando os mecanismos de comunicação e negociação, também propiciaram o surgimento de condutas criminosas ocorridas no cyberespaço (FERREIRA, 2017).

Assim, destaca-se o dever que o Direito possui de acompanhar essa evolução, regendo e limitando situações advindas das relações cibernéticas.

Em detrimento das dificuldades de rastrear e identificar os criminosos, a internet é comumente taxada como uma “terra sem lei”, o que torna ainda mais imprescindível um regramento específico para tratar do assunto com a devida atenção, protegendo a sociedade e punindo os responsáveis pela prática de ilícitos no cyberespaço.

4.1 Vulnerabilidades Cibernéticas

Não existe um portal digital conectado à internet que seja 100% seguro e sem vulnerabilidades. Lei Geral de Proteção de Dados (LGPD) e E-Ciber[6] são fatores importantes para motivar o aumento a prevenção contra incidentes cibernéticos, mas ainda é preciso assimilar culturalmente as estratégias.

A segurança cibernética tem evoluído bastante no Brasil ao longo dos últimos anos, e a entrada em vigor da Lei 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD), após alguns adiamentos, colocou a segurança cibernética em pauta para empresas que têm grandes bases de dados pessoais. Mesmo empresas pequenas e médias passaram a ter alguma preocupação com o assunto afinal, hoje todos têm dados armazenados em algum meio digital conectados ao espaço cibernético (MALHEIRO, 2017).

Entretanto, no Brasil, a cultura não é da prevenção. Somos mais focados em reagir aos incidentes do que em preveni-los, e essa cultura precisa mudar tanto no cenário público quanto no privado.

No Brasil, especificamente no âmbito público, em 6 de fevereiro de 2020, através do Decreto no. 10.222/2020 surgiu a Estratégia Brasileira de Segurança Cibernética (E-Ciber), que é um começo da retomada das iniciativas anteriores na área de cibersegurança, com menção expressa à Política Nacional de Segurança da Informação. Une-se à ela a recente LGPD, mas ambas ainda precisam ser desdobradas em diretrizes e ações práticas (FEITOZA, 2012).

De forma atual, hoje o mundo inteiro houve falar em Terrorismo Cibernético. Sobre essa modalidade de terrorismo, o terrorismo cibernético ou o ciberterrorismo é conceituado por Rodrigo Santos (2020) que menciona dizer ser esse diferente de tudo o que foi apresentado até então, já que ele envolve uma ação pontual, mas devastadora para as vítimas, pode afetar diversas vítimas de maneira inesperada e ágil, algo como o que aconteceria em um ato de terrorismo tradicional

Santos (2020) discorre ainda que nos casos de guerra cibernética, existem pessoas que não acreditam ser possível equiparar o termo digital com o originário, mas neste caso, a associação é ainda mais fácil.

Não é de se assustar e fácil de acreditar que grupos terroristas como a Al-Qaeda utilizam a rede para comunicação, estratégias e recrutamento, como uma empresa recrutando funcionários para suas empresas.

[6] A **E-Ciber** é um texto cujo conteúdo abrange tanto o diagnóstico da situação brasileira a respeito da segurança virtual, como um compilado de orientações visando a melhoria do cenário verificado, com validade para o quadriênio 2020-2023.

Essa cultura do medo foi rapidamente adotada em diversos cibercrimes e ciberguerras ao longo da história, pois o medo do improvável é fortificado com o desconhecimento sobre tecnologia e as possibilidades no uso de redes ao redor do mundo.

As motivações de um ato de terrorismo cibernético pode envolver política, como no caso de uma guerra cibernética, mas também pode girar em torno de razões ideológicas, uma discordância nada amigável contra um grupo de pessoas.

4.2 Desafios na Investigação

Devido ao dinamismo da tecnologia de informações, muitas são as dificuldades enfrentadas pelos investigadores no processo de verificação dos crimes cibernéticos. Todavia, em que pesem os desafios enfrentados pela polícia investigativa, muitas soluções estão sendo procuradas, como a criação de leis específicas e uma melhor capacitação dos agentes responsáveis pela persecução penal, a fim de acompanhar o crescente desenvolvimento da tecnologia e o consequente surgimento de novas ameaças virtuais (FEITOZA, 2012).

Assim, passar-se-á a analisar algumas das principais dificuldades enfrentadas pela polícia investigativa na seara dos crimes cibernéticos.

4.3 Os limites materiais de infiltração virtual dos agentes policiais e responsabilidade penal

A Lei 13.441, de 08 de maio de 2017, previu expressamente a possibilidade de “infiltração de agentes de polícia na internet, com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente” (BRASIL, 2017).

A novel legislação acrescentou os arts. 190-A, 190-B, 190-C, 190-D e 190-E à Lei 8.069/1990 (Estatuto da Criança e do Adolescente), que traz, de forma expressa, a possibilidade de que um policial oculte sua real identidade e ingresse em ambientes virtuais com o escopo de investigar delitos contra a dignidade sexual de criança e adolescente, obtendo provas de materialidade e autoria.

Cleber Masson e Vinícius Marçal já admitiam, antes da edição da nova Lei, a possibilidade de que a infiltração de agentes policiais em organizações criminosas ocorresse de forma física ou virtual.

A infiltração virtual de agentes policiais na internet, como em sites de relacionamento, tem como fundamento de validade uma conjugação da Lei 9.296/1996 (que permite a captação de dados telemáticos no seu art. 1º, § 1º) com a Lei 12.850/2013 (que trata da infiltração de agentes em seus arts. 10 e seguintes), desde que a medida investigativa – que permite o acesso a dados privados, como, por exemplo, conversas em ambientes fechados na web – seja autorizada judicialmente. *In verbis*:

> Concebemos que o uso do fake pelos órgãos de persecução equivale à modalidade de infiltração de agente, a qual consiste em meio extraordinário de obtenção de prova. Na criação de perfil falso de usuário (fake) pelo investigador, há de ser respeitada a proporcionalidade, a subsidiariedade, o controle judicial e a legalidade. O agente policial pode criar perfil falso de usuário (fake) visando incursão investigativa na web, desde que 'calçado' pelo competente mandado judicial. A Lei 9.296/1996 (que regulamenta as interceptações), conjugada com a Lei 12.850/2013 (Lei das Organizações Criminosas), outorgam validade processual às ações infiltradas no plano cibernético, desde que observada a cláusula de reserva de jurisdição (FERREIRA, 2017).

Os crimes que ensejam a infiltração virtual no âmbito da Lei 13.441/2017 são aqueles cujo bem jurídico tutelado é a dignidade sexual de crianças e adolescentes, abrangendo a produção e a distribuição de material contendo pornografia infanto juvenil, a aquisição e o armazenamento de tal material, a simulação da participação em cenas de sexo explícito e o aliciamento para a prática libidinosa com criança ou adolescente (BRASIL, 2017).

Nesse seguimento, Antonio Roberto de Oliveira Filho, assevera que:

> Além disso, o instituto também se aplica na investigação dos crimes de invasão de dispositivo informático, estupro de vulnerável, corrupção de menores, satisfação da lascívia mediante presença de criança ou adolescente e favorecimento a prostituição ou de outra forma de exploração sexual de criança ou adolescente ou de vulnerável, tipificados no Código Penal (FILHO, 2020).

Na hipótese referente ao armazenamento e a posse de material pornográfico no âmbito da investigação, apesar da omissão da Lei 13.441/2017, o próprio Estatuto da Criança e do Adolescente afasta a existência dos crimes ligados ao armazenamento e a posse de tal material com a finalidade específica de comunicar as autoridades competentes sobre a ocorrência de tais crimes, como dispõe o art.241- B, §2º, I, do ECA.

Conclui-se que o legislador optou por deixar em aberto o tratamento jurídico a respeito da responsabilidade penal do agente que, no curso da investigação devida autorizada pelo poder judiciário, sem exceder os limites impostos pela mesma, cometer crimes inerentes a infiltração virtual de agentes. Caberá à doutrina especializada tratar disso nos casos concretos.

5. Consequencias jurídicas dos crimes virtuais

O Direito, por ser instrumento regulador dos fatos juridicamente relevantes, deve acompanhar as mudanças tecnológicas, buscando se adaptar as transformações de modo direto, a fim de trazer adequação efetiva e gradual perante a mudança na realidade, no esforço de promover novas soluções para os novos problemas se propondo a estudar aspectos jurídicos do uso do computador devido ao grande desenvolvimento da Internet.

Com o surgimento da informática e a popularização de seu uso, a sociedade se encontra diante de uma tecnologia revolucionária que tomou conta de suas vidas nos mais diversos aspectos como nenhuma outra invenção foi capaz de fazer.

As consequências diretas dessa criação, o uso generalizado dos computadores pessoais e acesso a grande rede da internet fez com que esse meio de integração e comunicação se consolidasse em nossa sociedade (CARNEIRO, 2012).

6. Conclusão

Após a confecção desse trabalho pode-se concluir que falar sobre cibercrime, é falar sobre algo novo. Essa modalidade de crime é diferente e um assunto sem muitas fontes de pesquisas.

Isso se dá porque o cibercrime é uma novidade, assim como a lei que regula sobre esse assunto. É muito interessante falar sobre um assunto que é inovador e apresentar suas perspectivas diante dele, apesar de não se ter uma fonte de pesquisa abrangente.

A conclusão há que se chega é que a lei de cibercrime é eficaz na medida que lida com os cometedores desse tipo de crime, funciona como modo de coibir o

crime, funciona como forma de punir aqueles que o cometem.

Como se observa do presente trabalho, falar sobre crimes cibernéticos é falar sobre algo ainda novo no ordenamento jurídico brasileiro. Essa modalidade de crime é diferente e um assunto sem muitas fontes de pesquisas acadêmicas e científicas.

A conclusão há que se chega é que a lei de crimes cibernéticos é eficaz na medida que lida com os cometedores desse tipo de crime, funcionando tanto para coibir o crime, como forma de punir aqueles que o cometem.

Referências

BEZERRA, Juliana. **Terrorismo: definição, atentados e grupos terroristas.** Disponível em: <https://www.todamateria.com.br/terrorismo/>. Acesso em 07 de set. de 20.

BRASIL. **Constituição da República Federativa do Brasil.** Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em 01 de out. de 20.

BRASIL. **Lei nº 13.441, de 8 de maio de 2017.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13441.htm. Acesso em 23 de abril de 2017.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em: 23 de abril de 2021.

FEITOZA, Luiz Guilherme de Matos. **Crimes Cibernéticos: O Estelionato Virtual.** Disponível em: https://egov.ufsc.br/portal/sites/default/files/crimes_ciberneticos_o_estelionato_virtual.pdf. Acesso em 20 de março de 2021.

FILHO, Antonio Roberto de Oliveira. **Os limites materiais da infiltração virtual de agentes policiais: a responsabilidade penal do agente infiltrado virtual.** Disponível em: http://www.repositorio.ufc.br/bitstream/riufc/55202/1/2020_tcc_aroliveirafilho.pdf. Acesso em 23 de abril de 2021.

JOSÉ, Maria Jamile. **Os limites materiais de infiltração virtual dos agentes policiais e responsabilidade penal.** Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2137/tde-01122010-144008/publico/Infiltracao_policial_Maria_Jamile_Jose.pdf. Acesso em 23 de abril de 2021.

LIMA, Simão Prado. **Crimes virtuais: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade.** Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/crimes-virtuais-uma-analise-da-eficacia-da-legislacao-brasileira-e-o-desafio-do-direito-penal-na-atualidade/. Acesso em 20 de março de 2021.

MALHEIRO, Emerson Penha. **Delitos virtuais praticados na sociedade da informação. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:artigo.revista:2017;1001107175. Acesso em 04 de março de 2021.**

SANTOS, Rodrigo. **Guerra Cibernética, Cibercrime e Ciberterrorismo: Qual a diferença?** Disponível em: <https://www.compugraf.com.br/guerra-cibernetica-cibercrime-e-ciberterrorismo-qual-a-diferenca/>. Acesso em 20 de março de 2021.

TJ-SP. **Tribunal de Justiça do Estado de São Paulo** – APL: 00016278920118260572 SP 0001627-89.2011.8.26.0572, Relator: Machado de Andrade. Data de Julgamento: 13.08.2015, 6ª Câmara de Direito Criminal, Data de Publicação: 18.08.2015. Disponível em: https://tj-sp.jusbrasil.com.br/jurisprudencia/220964870/apelacao-apl-16278920118260572-sp-0001627-8920118260572/inteiro-teor-220964948. Acesso em 04 de março de 2021.