INSTITUTO ENSINAR BRASIL
FACULDADES UNIFICADAS DE TEÓFILO OTONI

DANILO DA SILVA GUEDES

CRIMES CIBERNÉTICOS E A NECESSIDADE DE ATUALIZAÇÃO DA LEGISLAÇÃO PENAL

TEÓFILO OTONI
2018

DANILO DA SILVA GUEDES

FACULDADES UNIFICADAS DE TEÓFILO OTONI

CRIMES CIBERNÉTICOS E A NECESSIDADE DE ATUALIZAÇÃO DA LEGISLAÇÃO PENAL

Trabalho de Conclusão de Curso apresentado ao Curso de Direito das Faculdades Unificadas de Teófilo Otoni, como requisito parcial à obtenção do título de Bacharel em Direito.

Área de Concentração: Direito Penal.

Orientador: Prof. Esp. Juvenal Martins de Souza Junior

TEÓFILO OTONI

2018

Rede de Ensino DOCTUM

FOLHA DE APROVAÇÃO

O Trabalho de Conclusão de Curso intitulado

CRIMES CIBERNÉTICOS E A NECESSIDADE DA TUTELA PENAL

elaborado pelo aluno Danilo da Silva Guedes foi aprovado por todos os membros da Banca Examinadora e aceita pelo Curso de Direito das Faculdades Unificadas de Teófilo Otoni, como requisito parcial da obtenção do título de

BACHAREL EM DIREITO

Teófilo Otoni, nas Minas Gerais,10 de julho de 2018.

Professor Esp. Juvenal Martins de Souza Júnior (orientador)

Professor MSc. Gylliard Matos Fantecelle

Professor Esp. César Cândido Neves Júnior

RESUMO

Pretende o presente estudo perquirir sobre a necessidade de atualização da legislação penal ante incidência dos delitos praticados através dos recursos tecnológicos como o computador e a internet. Busca-se trazer os diferentes conceitos doutrinários referentes ao chamado Direito Penal Informático. Citar exemplos de crimes informáticos, seus diferentes tipos, formas de incidência e se a legislação penal e processual se encontra apta a tutelar as possíveis condutas que utilizem os recursos tecnológicos como alvo ou meio para prática de delitos. Ainda, procura-se apresentar as diferentes interpretações atinentes às leis que foram recentemente aprovadas e que tem buscado alterar o ordenamento jurídico penal, demonstrando suas fragilidades e controvérsias. Elencar as propostas que estão em trâmite no Congresso Nacional e que procuram tutelar as condutas ilícitas praticadas através da internet, demonstrando seus pontos positivos quando de fato trazem inovações objetivando a modernização do direito face à demanda da sociedade, assim como suas deficiências e vulnerabilidades.

Palavras-Chave: Direito Penal Informático. Crimes Cibernéticos. Atualização da Lei Penal. Internet. Tecnologia.

ABSTRACT

The present study intends to investigate the need to update criminal legislation in the incidence of crimes practiced through technological resources such as the computer and the internet. It seeks to bring the different doctrinal concepts regarding the so-called Computer Criminal Law. To cite examples of computer crimes, their different types, forms of incidence, and whether criminal and procedural legislation is capable of protecting possible conduct that uses technological resources as a target or a means to commit crimes. In addition, it seeks to present the different interpretations related to the laws that were recently approved and that has sought to alter the criminal legal system, demonstrating its fragilities and controversies. List the proposals that are being processed in the National Congress and which seek to protect illicit practices practiced through the Internet, demonstrating their positive aspects when in fact they bring innovations aiming at the modernization of the law against society's demand, as well as its deficiencies and vulnerabilities.

Key Words: Computer Criminal Law. Cyber Crimes. Updating of the Penal Law. Internet. Technology.

SUMÁRIO

1 INTRODUÇÃO

É de notório conhecimento que o advento da tecnologia tem impactado em todos os setores da convivência humana. Várias interações e tarefas que antes só se davam de forma física ou mecânica passaram a ser feitas de maneira virtual e à distância. Surgiram novos tipos de comunicação e serviços, tornando a vida das pessoas mais simples, ágeis e menos onerosas. Consequentemente, houve um aumento exponencial na dependência com relação a esses recursos de forma que passaram a gerir quase em sua totalidade o estilo de vida de cada indivíduo.

Essa mutação social também foi percebida pelos criminosos, que passaram a se valer de citadas facilidades para praticar atos delituosos e auferir vantagens ilícitas de uma maneira mais ágil e com menos probabilidades de serem pegos. Nesse contexto, vários acontecimentos de grande proporção ocorreram e chamaram a atenção das autoridades em razão da falta de previsão legal de determinadas condutas e a necessidade de tutelar referidas práticas no intuito de coibir o fenômeno da impunidade.

Assim sendo, a doutrina tem discutido sobre a real necessidade de modificar ou criar novos dispositivos que busquem prever as especificidades de cada conduta delituosa. Nesse sentido, a presente pesquisa visa contribuir para o âmbito científico, mais especificadamente para o meio jurídico, trazendo informações atinentes às novas tipificações legais que surgiram como decorrência de situações fáticas ocorridas no cenário mundial e local, suas repercussões positivas e negativas, a mobilização e preocupação dos governos e seus respectivos ordenamentos jurídicos em tutelar bens jurídicos inexistentes ou pouco explorados, trazendo à tona a discussão acerca da efetividade dos Códigos Penal e Processual Penal em abarcar os delitos praticados através de recursos tecnológicos como o computador e a internet, abrangendo os pontos mais importantes e suas peculiaridades e se atualmente encontram-se aptos a oferecer uma resposta satisfatória à sociedade.

Observando essa realidade, vários países já adotaram uma série de mecanismos visando diminuir a prática dos atos criminosos em questão, editando leis e buscando medidas preventivas. Uma dessas medidas no âmbito internacional refere-se à denominada Convenção sobre o Cibercrime, também chamada de Convenção de Budapeste, que tem buscado uniformizar a legislação penal sobre o

tema e implantar uma espécie de cooperação internacional abrangendo os países signatários.

Atentos a essa questão, nossos legisladores já se mobilizaram, e apesar de não ter ratificado essa convenção internacional, tem buscado adequar nosso ordenamento jurídico penal ao tema objeto de preocupação. Com efeito, os últimos anos foram de grande importância para o assunto discutido, uma vez que foram editadas as leis nº 12.735 e 12.737 de 2012, que vieram tipificar e modificar algumas condutas não previstas ou incompletas no Código Penal. No entanto, conforme ressalta a doutrina, apesar de ser um passo importante na tutela dos bens jurídicos, tais previsões ainda podem se mostrar insuficientes ou deficitárias, tendo em vista que há certas particularidades que não foram suficientemente abrangidas, o que pode dificultar a análise do caso concreto pelos operadores do direito em determinadas ocasiões.

Destarte, após esses apontamentos iniciais, o desenvolvimento dessa pesquisa abordará todas as nuances que abrangem esse estudo, com o intento de oferecer uma análise contextualizada sobre a efetividade do nosso ordenamento jurídico penal e se há ou não necessidade de modificação de seu texto.

O trabalho será desenvolvido através da utilização de doutrinas, legislações e sítios eletrônicos relacionados ao tema proposto. Numa abordagem inicial serão estudados os aspectos gerais do chamado direito penal informático, logo após, a legislação existente sobre o tema. Finalizando com uma análise específica sobre o assunto, bem como os pontos peculiares, e a fixação dos pontos controversos e seus respectivos posicionamentos doutrinários.

2 DIREITO PENAL INFORMÁTICO - ASPECTOS GERAIS

Nas últimas décadas, a utilização do computador e da internet remodelou de modo espantoso a vida das pessoas, de maneira que a sociedade atual tem se encontrado absolutamente dependente das novas tecnologias da informação. Nesse sentido, Brito (2013, p.17) constata:

> Não há instituições financeiras sem computadores e internet; a maioria dos serviços públicos necessita de uma central informatizada; grande parte das grandes empresas – se não todas elas – possui bancos de dados para controle orçamentário, contábil, de estoques e de clientes. Os pequenos empreendimentos certamente estagnarão ou desaparecerão se não se adequarem à realidade que lhe é imposta.

Como consequência, surge na sociedade um novo ramo do Direito, o Direito Informático, que se direciona à tutela específica do relacionamento do Direito com a internet, trazendo novos regramentos em cada um dos ramos jurídicos. A título de exemplo temos os contratos eletrônicos no Direito Civil, a Tributação de Downloads no Direito Tributário, ou o pregão eletrônico no Direito Administrativo, e finalmente a criminalidade cibernética no Direito Penal, (JESUS, 2016).

Sendo assim, é de extrema relevância realizar um estudo sobre a evolução histórica desse cenário, apontando os principais fatos até a chegada do nosso estágio atual: a sociedade da informação.

2.1 Origem e evolução do Computador e da Internet

No início, uma das primeiras ferramentas usadas pelo homem para realizar cálculos remonta à Mesopotâmia de 5.500 anos atrás, que utilizavam o Ábaco. Nesse mesmo período, outros instrumentos com o mesmo objetivo podem ser identificados, como as Tábuas de Argila (1.700 a.C). Algum tempo depois passa-se pelos Bastões de Napier (1614), pela Máquina Aritmética de Pascal (1642) e pela Máquina de Recenseamento de Herman Holerith (1880), até chegar à contemporaneidade com os modernos microprocessadores, a inteligência artificial e a rede em nuvem (BRITO, 2013).

Não se pode deixar de citar um dos eventos mais importantes da história da humanidade, o qual foi imprescindível para evolução social no tocante aos recursos

tecnológicos: a Revolução Industrial. Esta modificou a visão de mundo moderno, alterando o modo de vida da população em geral, trazendo avanço significativo com o êxodo do homem do campo para os grandes centros.

Percebeu-se um impulso no desenvolvimento das cidades com o surgimento das máquinas em larga escala, os trabalhadores que antes exerciam toda a atividade de forma mecânica, passaram a controlá-las e as fábricas começaram a produzir cada vez mais. Ato contínuo, surgiram novos inventos como navios, locomotivas, carros, etc. Fazendo com que a produção e o crescimento da sociedade aumentassem de forma descomunal (SILVA, 2016).

Nesse contexto surgiram os computadores, destacando-se como um dos equipamentos mais importantes no desenvolvimento da sociedade como um todo. Sua evolução, como se pode observar, ficou dividida em cinco gerações, a saber: A 1º Geração (1940-1952) foi formada por computadores movidos por de válvulas a vácuo; na 2º Geração (1952-1964) houve a substituição das válvulas por transistores; na 3º Geração, a substituição dos transistores por circuitos integrados e a miniaturização dos grandes computadores; a 4º Geração foi marcada pela substituição dos circuitos pelos microprocessadores; e na 5º geração (1981) ocorreu um grande avanço da computação com a utilização da Inteligência Artificial, assim como a massificação do uso da internet (BRITO, 2013).

Por seu turno, a internet surgiu no decorrer da Guerra Fria, na década de 1960 em razão de uma necessidade militar. O Departamento de Defesa dos Estados Unidos financiou o projeto desenvolvido pela ARPA (*Advanced Research Projects Agency* – Agência de Projetos de Pesquisa Avançada) , através de um de seus departamentos, o IPTO (*Information Processing Techniques Office* – Escritório de Técnicas de Processamento de Informação), culminando na primeira forma de troca de comunicações através dos computadores. A chamada ARPANET (*Advanced Research Projects Administration* – Administração de Projetos e Pesquisas Avançados) conectando através da telecomunicação *online* (conectado) a Universidade da California em Los Angeles com a Universidade da California em Santa Barbara e a Universidade de Utah (CASTELLS, 2003).

Com o passar dos anos, outras fases de evolução se sucederam, criando-se conhecido protocolo de controle de transmissão TCP/IP[1] . Após a liberação da rede para domínio público, esta se desvinculou das relações militares, passando à privatização. Deste ponto em diante, empresas provedoras de acesso interessaram-se em direcionar investimentos para a comercialização da internet, desenvolvendo novos mecanismos de acesso à comunicação, ampliando sua utilização em escala global. (BRITO, 2013).

2.2 Conceito de Crimes Informáticos

Assim como aconteceu em todos os ciclos evolutivos da humanidade, a criminalidade também acompanhou o progresso tecnológico, desenvolvendo novas estratégias na busca de impunidade. Com o suporte da internet, o criminoso saiu da esfera local e regional para exercer suas atividades delituosas em âmbito mundial. (SILVA, 2017).

Delitos de natureza patrimonial como furto, extorsão e estelionato, fraudes tributárias e a lavagem de capitais advinda do tráfico de drogas, armas, órgãos e pessoas se tornaram muito mais frequentes, rápidos e lucrativos.

Assim sendo, Brito (2013, p.27) preconiza que:

> Os novos riscos passaram a causar conflitos até então desconhecidos pelo Direito, pelo que novas providências passaram a ser exigidas não mais para proteção de bens jurídicos clássicos e palpáveis, como a vida e o patrimônio dos cidadãos, mas de situações em que a vítima é a coletividade como um todo, de forma determinada, ou não, como é o caso das condutas atentatórias ao meio ambiente ou à ordem econômica, exemplos de bens jurídicos individuais, entendidos estes como os bens cuja titularidade pertence à coletividade, de forma determinável (coletivos) ou indeterminável (difusos).

Feitas tais considerações, cumpre esclarecer que a doutrina não chegou a um acordo no que diz respeito à nomenclatura dos crimes praticados através do meio computacional, nem quanto ao seu conceito.

[1] TCP significa *Transmission Control Protocol* (Protocolo de Controle de Transmissão) e o IP, *Internet Protocol* (Protocolo de Internet) (MARTINS, 2012).

Nesse ângulo, Lima (2006) aduz que a doutrina trata da temática denominando-a crimes de informática, crimes virtuais, crimes digitais, crimes eletrônicos, crimes informáticos, etc.

No entanto, Corrêa (2000, p. 43), tecendo comentários relacionados à questão, busca conceituar o que se entende por “crimes digitais”, entendidos como:

> Todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar.

Complementando o assunto, Pinheiro (2010) aduz que Crimes digitais podem ser conceituados como sendo condutas cujo acesso não teria sido autorizado em determinado sistema informático, resultando em atos danosos aos respectivos sistemas, como a interceptação ilegal de comunicações, alteração de dados, instigação ao ódio e preconceito, bullying, terrorismo, crimes contra o patrimônio, entre outros.

2.3 O princípio da legalidade e sua relação com os delitos informáticos

Conforme ensinamento de Greco (2016), o princípio da legalidade tem como base o artigo 5º, inciso XXXIX da Constituição Federal, texto que se assemelha ao artigo 1º do Código Penal. Complementando o assunto também ressalta que:

> É o princípio da legalidade, sem dúvida alguma, o mais importante do Direito Penal. Conforme se extrai do art. 1º do Código Penal, bem como do inciso XXXIX do art. 5º da Constituição Federal, não se fala na existência de crime se não houver uma lei definindo-o como tal. A lei é a única fonte do Direito Penal quando se quer proibir ou impor condutas sob a ameaça de sanção (Greco, 2016, p. 144).

Nesse sentido, há algum tempo vem sendo cobrado das autoridades competentes uma legislação penal que tutele a questão dos crimes informáticos, que por muito tempo se mostrou omissa aos novos fatos criminosos que vem surgindo como decorrência da evolução tecnológica. A atipicidade de determinadas condutas tem feito com que houvesse um aumento na sensação de impunidade quando diante de delitos praticados através do computador ou da internet (JESUS, 2016).

Com efeito, a discussão do assunto por diversos autores traz à tona a questão do “direito penal mínimo”, buscando justificar a desnecessidade de legislação quando diante de fatos não relevantes para o Direito Penal. No entanto, como adiante será explanado, a prática de delitos informáticos não tem se mostrado como fato que se enquadra na hipótese em apreço, em razão dos recorrentes crimes e os vultosos prejuízos financeiros ou pessoais constatados quando da consumação dos mesmos. Assim sendo, para melhor compreensão do assunto e da necessidade de abrangência legal de condutas reprováveis relacionadas ao meio informático, é de grande relevância apresentar a distinção feita pela doutrina acerca dos diferentes tipos de crimes, que podem ser classificados em próprios, impróprios ou mistos.

2.3.1 Crimes informáticos próprios

Nos crimes informáticos próprios os ataques são direcionados aos dados, equipamentos ou sistemas. Estes exigem, na maioria das vezes, a inclusão de novos dispositivos legais, dadas as suas particularidades técnicas (BRITO, 2013).

Fraudes eletrônicas, invasões de dispositivos computacionais, descaminho de DNS[2], inserção de vulnerabilidades em equipamentos eletrônicos, de maneira que confira ao invasor ingresso total e irrestrito ao dispositivo, apoderamento de senhas por Phishing[3], instalação de vírus para sabotagem eletrônica são alguns exemplos de condutas ilícitas que caracterizam os crimes informáticos próprios. Assim sendo, Ferreira (2000) preconiza que:

> Por outro lado, inúmeros problemas e grandes prejuízos podem e têm sido causados por ações praticadas diretamente contra o funcionamento da própria máquina, como é o caso da disseminação proposital do chamado ‘vírus do computador’ que destrói programas e fichários dos usuários, e cujos resultados ultrapassam as fronteiras nacionais, pelo uso da Internet,

[2] DNS significa Domain Name System, ou Sistema de Nomes de Domínios. É um computador com uma espécie de banco de dados que relaciona o endereço "nominal" de um site como www.uol.com.br com o endereço real onde está a página na rede, para poder acessá-la. Esse "endereço real" é dado pelo número de IP (Internet Protocol) (FERREIRA, 2008).

[3] “Phishing” em inglês corresponde a “pescaria”. Tem o objetivo de “pescar” informações e dados pessoais importantes através de mensagens falsas. Com isso, os criminosos podem conseguir nomes de usuários e senhas de um site qualquer, como também são capazes obter dados de contas bancárias e cartões de crédito (MÜLLER, 2012).

> adquirindo modernamente uma importância que não se ajusta aos estreitos limites do crime de dano conforme a tipificação feita no Código Penal.

No Brasil, foi aprovada a Lei 12.737 de 2012 que busca tipificar a conduta de invasão de dispositivo informático sendo, portanto, um importante passo na tutela dos crimes informáticos próprios.

2.3.2 Crimes informáticos impróprios

Conforme sabedoria de Jesus (2016), diz respeito à modalidade de crime em que os recursos tecnológicos são usados com ferramentas para prática de ilícitos já tipificados no Código Penal, como ameaça, estelionato, crimes contra a honra, etc. Para esses crimes a doutrina aponta que a legislação existente já se encontra apta a tutelar grande parte das condutas praticadas.

2.3.3 Crimes informáticos mistos

Compreende a violação a dois bens jurídicos distintos, caracterizando um crime complexo, ou seja, além da lesão ao bem jurídico informático fere outro bem tutelado pela legislação penal. A doutrina costuma citar como exemplo a transação ilícita de valores entre contas correntes (JESUS, 2016).

Como é notório quanto aos crimes informáticos próprios, onde o alvo da conduta delituosa direciona-se aos dispositivos ou programas, o Direito Penal mostra-se carente de regulamentação típica, fazendo-se necessário adequar-se de forma a diminuir ou extinguir as lacunas existentes no ordenamento jurídico penal. A diferenciação entre os crimes informáticos próprios, impróprios e mistos é imprescindível, haja vista que os delitos em que os dispositivos computacionais e a internet são utilizados como meio para a prática da atividade criminosa já estão presentes em sua grande maioria no Código Penal vigente, podendo o sujeito ativo ser devidamente processado e julgado conforme sua conduta. No entanto, quanto aos crimes onde o computador, seus arquivos ou programas são o alvo, seja para danificação do sistema, para subtração de informações, programas, ou qualquer outro objetivo danoso, os delitos e modos de atuação vão se traduzindo em tarefas

complexas para tipificação nos dispositivos previstos no Código Penal, deixando brechas na legislação e favorecendo a impunidade.

2.4 Condutas Informáticas que podem caracterizar crime

Examinar as condutas ilícitas que são praticadas através do meio informático é tarefa bastante complexa em razão da difícil constatação do local onde o criminoso que deu início à conduta se encontra, haja vista a falta de limitações fronteiriças proporcionada pela internet.

Grande parte dos crimes que são perpetrados através da internet são também verificados em nossa realidade física, no entanto, nota-se que há delitos com certas particularidades, fazendo-se necessário analisar se sua prática amolda-se ao nosso texto legal. A seguir, serão examinadas algumas condutas ilícitas praticadas através do meio informático e se nossa legislação tem condições de oferecer uma resposta diante de eventual prejuízo causado à vítima.

2.4.1 Acesso Ilegítimo

Refere-se à conduta de acessar sem permissão determinado sistema informático, não obrigatoriamente através de invasão de dispositivo de segurança. Nesse caso, o entendimento majoritário é que essa conduta tenha intenção ilegítima. Para a doutrina, o Brasil penaliza essa conduta através do artigo 154-A do Código Penal (JESUS, 2016).

2.4.2 Interceptação ilegítima

Está ligado à utilização de métodos técnicos em comunicações privadas para captação de informações comprometedoras das partes. Essa conduta é considerada pelo Código de Processo Penal como um meio para de obtenção de provas e deve ser utilizado de forma subsidiária, ou seja, como último recurso, tendo em vista o caráter invasivo na esfera particular do indivíduo. Atualmente é regulado pela Lei nº 9.296 de 1996 – Lei de Interceptação Telefônica, e depende de autorização judicial para que seja efetuada. A interceptação ilegal de comunicações telefônicas, de

informática ou telemática constitui crime, conforme o artigo 10 do referido diploma legal (HABIB, 2015).

2.4.3 Interferência de sistemas

Situação na qual o agente, dolosamente, provoca paralisação, perturbação ou dificuldade ao normal funcionamento de sistema de informações através de danificação, transmissão ou supressão de dados. Essa conduta encontra previsão no artigo 266 do Código Penal, na parte que relaciona os crimes contra a incolumidade pública. A lei 12.737 de 2012 acrescentou ao citado dispositivo o §1º, prevendo também incorrer na mesma pena prevista quando praticado tendo como alvo informação de utilidade pública ou dificultar o seu restabelecimento (SANCHES, 2015).

2.4.4 Uso abusivo de dispositivos

Relaciona-se ao comércio, a utilização ou distribuição de equipamento ou programa informático destinado para prática de condutas ilícitas, ou mesmo a captação de senhas ou códigos que possibilitem a entrada não permitida em determinado sistema. A lei 12.737 de 2012 no seu artigo 154-A, §1º tipifica citada atuação. Nesse sentido, o artigo 325, §1º, inciso I do Código Penal, na parte que se refere aos crimes contra a administração pública, prescreve a violação de sigilo funcional, punindo com seis meses a dois anos e multa o agente que fornece acesso a pessoas não autorizadas a sistema de informações ou banco de dados pertencentes à administração pública (SANCHES, 2015).

2.4.5 Falsidade ou fraude informática

Conforme entendimento de Sanches (2015), diz respeito à inserção, modificação ou supressão dolosa de dados informáticos, resultando em informações inverídicas com o intento de que sejam utilizados de forma lícita como se fossem verdadeiros. Atualmente, não há na legislação nacional um dispositivo específico que prescreva essa conduta no caso de banco de dados privados, no entanto, é possível

considerar o crime de falsidade ideológica, artigo 299 do Código Penal. Não obstante, nos crimes praticados por funcionário público contra a Administração Pública é possível observar o artigo 313-A do Código Penal, que prevê o seguinte, *in verbis:*

> 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: (Incluído pela Lei nº 9.983, de 2000)
> Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa. (Incluído pela Lei nº 9.983, de 2000)
> Modificação ou alteração não autorizada de sistema de informações (Incluído pela Lei nº 9.983, de 2000).

Nesse contexto, o artigo 313-B do mesmo diploma legal prevê punição para o funcionário que modifica ou altera sistema ou programa de informática sem autorização, conforme se observa no Código Penal *in verbis*:

> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: (Incluído pela Lei nº 9.983, de 2000)
> Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa. (Incluído pela Lei nº 9.983, de 2000)
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado. (Incluído pela Lei nº 9.983, de 2000).

2.4.5.1 Fraudes em certames públicos e o uso da cola eletrônica

A “cola” trata-se de determinada técnica utilizada por alunos que tem o objetivo de solucionar questões na hora da prova com o auxílio de discretas anotações não autorizadas pelos docentes. Referida conduta começou a ser vista com maior relevância e reprovabilidade quando utilizada diante de processos seletivos mais complexos, como os concursos públicos ou vestibulares. Com o advento das tecnologias da informação essa prática ganhou nova aparência, sendo denominada pela doutrina como “cola eletrônica”, permanecendo sua essência, mudando apenas o seu modo de prática que agora conta com o auxílio de ferramentas tecnológicas como smartphones, internet, pontos eletrônicos, entre outros (BRITO, 2013).

No ano de 2012 foi deflagrada a Operação Calouro pela Polícia Federal, que desmantelou uma quadrilha que cometia fraudes em vestibulares por todo país, conforme notícia do site G1:

> O delegado detalhou que o esquema funcionava de duas maneiras. Na mais simples, uma pessoa envolvida na quadrilha falsificava documentos e fazia a prova no lugar do verdadeiro candidato. Essa pessoa que realizava a prova quase sempre era um aluno de medicina com boas notas na faculdade.
> Na outra modalidade, um membro da quadrilha fazia a prova rapidamente e saia da sala. Esse falso candidato que resolvia a prova era chamado pelos integrantes das quadrilhas de "piloto", pois deveria ser rápido para resolver as questões, e também era aluno de medicina. De posse do gabarito, ele conferia o resultado e passava as informações por meio de uma escuta eletrônica ou por celular para o candidato. Antes da prova, os candidatos que contratavam os serviços das quadrilhas eram treinados para que soubessem como agir no momento de receber as respostas.
> O valor do serviço contratado por um candidato girava entre R$ 45 mil a R$ 80 mil. O dinheiro só era entregue após o cliente/candidato ter sido aprovado na faculdade. O líder repassava para o "piloto" valores entre R$ 5 mil e R$ 15 mil. Parte do pagamento também era entregue ao "corretor", responsável por aliciar candidatos para entrarem no esquema. Essas pessoas, geralmente, eram médicos. O líder também possuía um assistente que treinava os candidatos/clientes para receber a cola, escolhia os equipamentos tecnológicos e falsificava os documentos (G1, 2012).

Com efeito, Brito (2013), relembrando a intensa discussão nos tribunais acerca da tipificação da citada conduta, e os diversos projetos de lei que tramitaram na Câmara visando incluir o tema Fraudes em Concursos Públicos, ressalta que em 15 de dezembro de 2011, através da Lei nº 12.550, foi incluído o artigo 311-A ao Código Penal, que assim prescreve *in verbis*:

> Art. 311-A. Utilizar ou divulgar, indevidamente, com o fim de beneficiar a si ou a outrem, ou de comprometer a credibilidade do certame, conteúdo sigiloso de: (Incluído pela Lei 12.550. de 2011)
> I - concurso público; (Incluído pela Lei 12.550. de 2011)
> II - avaliação ou exame públicos; (Incluído pela Lei 12.550. de 2011)
> III - processo seletivo para ingresso no ensino superior; ou (Incluído pela Lei 12.550. de 2011)
> IV - exame ou processo seletivo previstos em lei: (Incluído pela Lei 12.550. de 2011)
> Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela Lei 12.550. de 2011)
> § 1º Nas mesmas penas incorre quem permite ou facilita, por qualquer meio, o acesso de pessoas não autorizadas às informações mencionadas no caput. (Incluído pela Lei 12.550. de 2011)
> § 2º Se da ação ou omissão resulta dano à administração pública: (Incluído pela Lei 12.550. de 2011)
> Pena - reclusão, de 2 (dois) a 6 (seis) anos, e multa. (Incluído pela Lei 12.550. de 2011)
> § 3º Aumenta-se a pena de 1/3 (um terço) se o fato é cometido por funcionário público.

Apesar das falhas na edição do supracitado dispositivo de lei, conforme aponta certos entendimentos doutrinários, é fato que a previsão legal da conduta criminosa

ajudou em parte no combate à incidência de fraudes em certames públicos, diminuindo o prejuízo causado àqueles que realmente se dedicam na esperança de conseguir uma vaga.

2.4.6 Burla Eletrônica

É o ato através do qual resulte em prejuízo, por meio de inserção, modificação, ou supressão de conteúdo informático ou alguma interferência com objetivo de auferir proveito econômico. A doutrina classifica essa atuação como sabotagem informática, e ressalta que atualmente não há nenhum dispositivo de lei que preveja de forma evidente a tipificação da citada conduta. No entanto, salienta que o projeto de reforma do Código Penal (Projeto de Lei do Senado nº 236 de 2012), traz em seu bojo a previsão do referido ato ilícito (JESUS, 2016).

2.4.6 Furto de dados ou vazamento de informações

Tem como objetivo copiar ou transferir de forma indevida, dados com determinado nível de segurança ou considerados confidenciais. Assim sendo, complementa Damásio de Jesus (2016, p. 45):

> Para punir a cópia indevida, muitas autoridades utilizaram da analogia in malam partem para classificar o ato como contrafração", "'furto de dados", outros partiram para a "interceptação telemática"", prevista na Lei nº 9.296/96. Outros autores ainda enquadravam a cópia indevida na concorrência desleal, crime previsto no art. 195 da Lei nº 9.279/96. Em verdade, não existe um tipo específico para esta conduta. Já para o vazamento de informações tem-se forçosamente utilizado o tipo do art. 153 do Código Penal (divulgação de segredo), sobretudo quando a divulgação se dá em relação a informações sigilosas, contidas ou não nos sistemas de bancos de dados da Administração Pública. A Lei nº 12.737/2012 trata essa circunstância como uma qualificadora do crime de "invasão de dispositivo informático", com pena de reclusão de seis meses a dois anos e multa se a conduta não constitui crime mais grave.

Nesse sentido, conforme salienta o citado autor, agora a conduta se encontra tipificada no Código Penal como uma qualificadora do crime previsto no artigo 154-A.

2.4.7 Envio de mensagens não solicitadas

Referida prática pode também ser conhecida como “spam”, que compreende o envio de mensagens que não teriam sido solicitadas e que de certa maneira podem vir a causar dano. É uma prática muito comum por empresas de marketing que utilizam programas de computador para enviar mensagens automáticas aos destinatários através da sua caixa de email cujo conteúdo trata da divulgação de marcas ou produtos. Apesar de ser uma conduta reprovável, ainda não existe legislação específica que regule o tema, no entanto, tramita no Senado o Projeto de Lei nº 283 de 2012 que busca atualizar o Código de Defesa do Consumidor e abarcar assim o envio de mensagens não solicitadas (JESUS, 2016).

2.5 Fixação da Competência

Em razão da ausência de limites territoriais, a fixação da competência no caso dos delitos informáticos pode apresentar algumas peculiaridades. No caso em que o local da infração seja de difícil constatação, deve-se recorrer às hipóteses previstas o artigo 69 do Código de Processo Penal *in verbis* :

> Art. 69. Determinará a competência jurisdicional: I - o lugar da infração; II - o domicílio ou residência do réu; III - a natureza da infração; IV - a distribuição; V - a conexão ou continência; VI - a prevenção; VII - a prerrogativa de função.

Nesse sentido, antes de analisar outras circunstâncias, é preciso que verifique se a competência abrange a esfera federal ou estadual. Com efeito, Brito (2013, p. 97) aponta o seguinte:

> O art. 109 da constituição Federal enumera o rol de objetos processuais que terão o condão de escalar um juiz federal para ser o responsável pelo julgamento da causa, e até agora não consta que é competência da Justiça Federal o processamento e julgamento de crimes praticados com o uso da internet. O caráter residual da competência estadual, portanto, ainda permanece da mesma forma, nos exatos limites do art. 109 da CF, não sofrendo qualquer alteração – até o presente momento – em razão da verificação de delitos praticados com o uso da internet.

Complementando o assunto, Jesus (2016) aponta que, conforme o artigo 109, incisos IV e V da Constituição Federal, caso o ilícito seja praticado em detrimento de bens da União, a competência passará para a esfera da Justiça Federal. Da mesma forma em situações em que por Convenção ou Tratado o Brasil se obrigou a reprimir.

Com efeito, no que se refere ao lugar do crime, de acordo com entendimento doutrinário, o Código Penal é adotante da teoria da ubiquidade, levando-se em conta que o lugar do crime, conforme artigo 6º é *in verbis*: “o local onde ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado”. Exemplificando:

> Deste modo, ao se considerar alguém no Estado do Rio de Janeiro, que invade o computador de outrem, localizado em São Paulo, teríamos o juízo onde está o dispositivo invadido como competente para processar e julgar o delito informático (JESUS, 2016, p. 60).

Dessa maneira, é importante lembrar no que se refere aos delitos praticados por nacionais no exterior, fazendo vítimas no Brasil, o fato deve ser considerado ilícito em ambos os países e o sujeito ativo deve adentrar em território nacional para que seja devidamente processado e punido, conforme art. 7º, II, §2º, a e b do Código Penal (SANCHES, 2016).

3 DA LEGISLAÇÃO ATUAL SOBRE OS DELITOS INFORMÁTICOS

Conforme os fatos supracitados, muitos delitos no campo da informática não vinham sendo apropriadamente reprimidos em razão da ausência de legislação específica que tipifique referidas condutas. Com efeito, mostrou-se necessária a criação ou modificação de dispositivos legais no intuito de suprir as lacunas existentes. Nesse sentido, conforme entendimento doutrinário, é importante lembrar no que se refere aos crimes informáticos impróprios, já previstos no Código Penal, não é necessário legislar, mas sim no tocante aos crimes informáticos próprios, ou seja, aqueles em que a internet, o computador ou seus equipamentos são o foco da conduta delituosa.

3.1 Da legislação nacional que regula os delitos informáticos

O ano de 2012 ficou marcado na história nacional do ramo jurídico denominado pela doutrina como Direito Informático. Nele surgiram as Leis nº 12.735 – “Lei Azeredo” e 12.737 – “Lei Carolina Dieckmann”, sancionadas pela presidente Dilma

Rousseff (2011-2016), com o objetivo de suprir as lacunas existentes no ordenamento jurídico penal até então (BRITO, 2013).

Dada a sucessão de fatos ilícitos praticados no ambiente virtual e a constante mutação das relações sociais, negociais e jurídicas proporcionados pela internet e a tecnologia, em 23 de abril de 2014, também foi promulgada a Lei nº 12.695 de 2014, conhecida como o Marco Civil da Internet Brasileira. Referida lei veio trazer regulamentação e solução às demandas jurídicas envolvendo a Internet quanto ao fornecimento de serviços e a necessidade de proteção específica de direitos, abordando assuntos como a responsabilidade civil e criminal dos provedores, proteção dos usuários da rede, uma vez configurada a relação de consumo, e a manutenção da internet como recurso que proporciona o exercício da liberdade de expressão, um dos direitos fundamentais previstos constitucionalmente (LEMOS, 2014).

3.1.1 Lei nº 12.737 de 2012 – “Lei Carolina Dieckmann”

Referida lei entrou em vigor no dia 3 de abril de 2013, modificando o Código Penal no intuito de tipificar os crimes informáticos próprios, ou seja, aqueles cujo alvo são dispositivos informáticos ou sistemas. Foi aprovada com certa urgência pelo Congresso Nacional, comovido com o clamor nacional em razão de determinada situação ocorrida com uma atriz de televisão, que teve arquivos de seu computador (fotos íntimas) amplamente divulgados na rede mundial de computadores sem o seu devido consentimento.

Com efeito, a citada lei cria o tipo penal “Invasão de Dispositivo Informático” no art. 154-A do Código Penal *in verbis*:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações

> sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Cria também o art. 154-B do Código Penal, apresentando a regra da ação penal no delito supramencionado *in verbis*:

> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos

Conforme destaca Brito (2013), além de novos tipos penais, a Lei nº 12.737 de 2012 – Lei Carolina Dieckmann, modifica o texto de dois crimes já existentes, previstos nos artigos 266 e 298 do Código Penal. Ao artigo 266 foi acrescentado parágrafo primeiro prevendo segundo o texto da lei que:

> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

Em paralelo, alterou o artigo 298, igualando como documento particular suscetível de falsificação os cartões de débito ou crédito *in verbis*:

> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

Dessa forma, trouxe mais uma proteção ao usuário desse tipo de serviço tão utilizado nos dias atuais.

3.1.2 Lei nº 12.735 de 2012 – “Lei Azeredo”

De acordo com Jesus (2016), o projeto de lei teve como relator o deputado Eduardo Azeredo e tinha como objetivo a criação de uma legislação criminal específica para a internet, tipificando uma série de condutas ilícitas perpetradas através rede mundial de computadores. Referida lei não foi tão abrangente como almejava, uma vez que dois dos quatro artigos foram vetados pela presidente Dilma Rousseff (2011-2016).

O diploma legal restringiu-se em dois tópicos, o primeiro prescrevendo que a polícia judiciária criasse setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivos de comunicação ou sistema informatizado, o segundo modifica a Lei nº 7.716 de 1989. Seu artigo 20, §3º, inciso II, foi atualizado de maneira a permitir que o juiz pudesse determinar a cessação de uma transmissão eletrônica, radiofônica , televisiva ou publicação (BRITO, 2013).

Foram vetados os artigos que tratavam de equiparação de cartões de crédito ou débito a documento particular em casos envolvendo falsificação de documento particular (art. 2º), e autorização para os militares controlarem os dados eletrônicos num eventual caso de guerra cibernética (JESUS, 2016).

A citada lei foi alvo de uma série de críticas pelos meios midiáticos em geral, vindo a ser comparada com uma espécie de AI-5[4] digital, em razão de atentar de forma desmesurada contra a privacidade e aos direitos dos usuários da rede mundial de computadores (BRITO, 2013).

3.1.3 Lei nº 12.695 de 2014 – “Marco Civil da Internet”

Sancionado pela presidente Dilma Rousseff (2011-2016) no dia 23 de abril de 2014, teve repercussões internacionais, fazendo com que o Brasil se tornasse referência na criação de uma espécie de “carta de direitos” direcionada aos usuários da internet. Ainda, serviu de fonte para discussão do tema em outras nações (LEMOS, 2014).

[4] O Ato Institucional nº 5, AI-5, baixado em 13 de dezembro de 1968, durante o governo do general Costa e Silva, foi a expressão mais acabada da ditadura militar brasileira (1964-1985). Vigorou até dezembro de 1978 e produziu um elenco de ações arbitrárias de efeitos duradouros. Definiu o momento mais duro do regime, dando poder de exceção aos governantes para punir arbitrariamente os que fossem inimigos do regime ou como tal considerados (D’Araújo, [200-?]).

Como era de se esperar, em razão da dinamicidade do Direito e a constante mutação das relações sociais, sua existência não foi capaz de exaurir todas as celeumas jurídicas presentes na rede mundial de computadores. De fato, referido diploma legal tem consistido num arcabouço normativo que choca-se diretamente com as relações virtuais, trazendo uma série de direitos e deveres direcionados aos usuários da internet (LEMOS, 2014).

3.2 Da legislação internacional que regula os delitos informáticos

Após o atentado terrorista perpetrado nos Estados Unidos contra as Torres Gêmeas, no dia 23 de novembro de 2001 foi elaborada a Convenção sobre o Cibercrime na cidade de Budapeste, Hungria. Tal documento trouxe à tona a necessidade de uniformização das leis penais no cenário mundial, criando mecanismos de fomento ao combate da criminalidade cibernética (SILVA, 2017).

Até o ano de 2010, constata-se que apenas quarenta e três países assinaram referida Convenção, mas somente vinte e dois a ratificaram. Apesar da pressão sofrida no âmbito internacional, o Brasil ainda não é signatário, contudo, os integrantes do Poder Legislativo têm envidado esforços no sentido de adequar os tipos legais de forma a atender às necessidades identificadas. (JESUS, 2016).

Ainda, de acordo com Brito, (2013, p.56), a citada convenção destina-se a três objetivos específicos, a saber:

> (a) Harmonizar a tipicidade penal no ambiente do ciberespaço pelos Estados signatários; (b) definir os elementos do sistema de informática promovendo a unidade na interpretação da legislação penal interna e possibilitar a credibilidade da prova eletrônica no ambiente virtual; (c) implementar um sistema rápido e eficaz de cooperação internacional no combate à criminalidade informática.

Dessa forma, em razão da complexidade e dimensão da rede mundial de computadores e seus equipamentos, constatou-se que a cooperação internacional poderia contribuir no combate aos ilícitos verificados no meio digital.

3.2.1 A Convenção de Budapeste e a legislação penal brasileira

Em razão da intenção de uniformização da legislação penal no tocante aos ilícitos praticados no cenário digital, é importante verificar se a citada Convenção trouxe impacto no ordenamento jurídico vigente, ou se este já tinha condições de apresentar soluções suficientes no combate a essa modalidade criminosa.

Uma primeira conduta a ser analisada é a criminalização do acesso ilegal a determinado sistema de computador sem o devido consentimento do seu proprietário ou administrador, desde que de maneira dolosa, uma vez que a Convenção não cuida de condutas consideradas culposas (JESUS, 2016).

Comentando a citada conduta, Brito (2013, p. 59) destaca que:

> Ao que se depreende, no Brasil a prática de acesso ilegal, com as elementares requeridas, já encontra um tipo penal abstrato recentemente criado para essa subsunção, sendo, portanto, típico nos termos do art. 154-A do Código Penal, ressalvada também a existência de um tipo específico para os pleitos eleitorais previsto no art. 72, I, da Lei nº 9.504/97.

Outro ponto a ser averiguado, conforme ensinamento de Brito (2013) refere-se ao artigo 3º da Convenção, que orienta os Estados signatários a criarem mecanismos legais no intento de considerar a prática de interceptação ilegal como crime. No entanto, assim como o tipo legal anterior, a conduta já se encontra prevista no artigo 10 da Lei nº 9.296/1996 – Lei de Interceptação Telefônica, que assim prescreve *in verbis*:

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa.

O artigo 4º prevê a criminalização da interferência de dados, contudo, esclarece que o delito refere-se à danificação, exclusão, deterioração, modificação ou supressão de dados sem permissão, uma vez verificado o dolo do agente e a não intenção de apropriação de arquivos privados, como previsto no artigo anterior. Porém, referido comportamento, a princípio, já se encontra previsto no artigo 163 do Código Penal, tipificando o delito de Dano. (PINHEIRO, 2010).

Logo em seguida o artigo 5º sugere a tipificação da interferência de sistema, que prescreve penalidade para o ato de causar retardo, sem autorização, de funcionamento de sistema de computador, por intermédio de inserção, transmissão,

danificação, deleção, deterioração, alteração ou supressão de dados de computador. No entanto, citadas elementares já possuem, em tese, previsão genérica nos artigos 256 e 26 do Código Penal. Nesse sentido Brito (2013, p. 60) observa que:

> O fato descrito, de acordo com as elementares apresentadas, em tese, já possuía um tipo penal genérico no Brasil. Trata-se do art. 265 e 266 do Código Penal, que considera crime contra a segurança do serviço de utilidade pública a conduta que "atentar contra a segurança ou o funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade pública"; ou do 266, em que " Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento" acarreta pena de detenção de um a três anos e multa. Porém, com a alteração promovida pela Lei nº 12.737/2012 no Código Penal, foi acrescentado ao artigo 266 o §1º com redação mais específica: Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

De acordo com sabedoria de Brito (2013), seu artigo 6º também trouxe caráter penal ao mau uso de equipamentos, orientando que os países adotantes da convenção criassem mecanismos legislativos para criminalizar a produção, venda, compra, importação, distribuição ou disponibilização de dispositivos, incluindo programas de computador, delineados para o cometimento dos ilícitos de acesso ilegal, interceptação ilegal, interferência de dados e a interferência de sistema, entre outros. Não obstante, a modificação consagrada pela Lei nº 12.737 de 2012 – Lei Carolina Dieckmann, no artigo 154-A, §1º trouxe justamente a conduta em questão.

Seu artigo 7º traz a previsão da falsificação computacional, objetivando estabelecer como lesivo a inserção, alteração, deleção ou supressão de dados, convertendo-os em falsos com o intento de utilizá-los para propósitos legais, se passando como verdadeiros. Atualmente, a falsificação documental, seja público ou particular, encontra previsão na lei penal, o que não se verifica com os dados eletrônicos ou computacionais. Importante destacar que a Convenção entende que esse é um delito formal, ou seja, basta que se realize a falsificação de dado eletrônico com a intenção de que se passe por verdadeiro para propósitos legais, mesmo que não haja dano efetivo. Não obstante, é importante de se observar que já tramitam no Congresso Nacional projetos de lei que pretendem criar essa modalidade criminosa ou a modificação dos artigos: 171, 297, 298 do Código Penal (PINHEIRO, 2010).

Como é de se notar, portanto, de um lado se tem os crimes informáticos impróprios, já previstos no ordenamento jurídico penal vigente, de outro, descrevendo uma pequena quantidade de condutas - mas com elevado grau de repercussão – se

tem os crimes informáticos próprios, que pela insuficiência legal mantinha inerte a atuação estatal. O legislador, dessa maneira, sintetizou em tipos penais a diretriz identificada na “Convenção de Budapeste” com relação à criminalidade cibernética. Todavia, fez isso de forma pouco técnica, criminalizando condutas já previstas em outros tipos legais, e utilizando condutas já abordadas em outras tipificações penais. (BRITO, 2013).

4. DA NECESSIDADE DE ATUALIZAÇÃO DA LEI PENAL

De todo apurado, constata-se que as ocorrências de delitos envolvendo o meio informático fizeram com que o estudo do Direito Penal abordasse novas condutas. Esses fatos impulsionaram de certa forma, uma nova abordagem dos princípios e normas penais para que alcançassem tais acontecimentos delitivos.

A população não pode ser impedida de usufruir das vantagens e benefícios proporcionados pela internet e os recursos tecnológicos em razão dos perigos que eventualmente podem correr. Por esse motivo é que a procura por aumentar a sensação de segurança no ambiente virtual tem se tornado um objeto de preocupação mundial. O Brasil, por seu turno, apesar da não assinatura da Convenção de Budapeste, necessita identificar o aparecimento de novos bens e buscar resguardá-los no meio jurídico, a exemplo do já esclarecido acerca dos crimes informáticos próprios e a decorrente criação das Leis nº 12.735 e 12.737 editadas no ano de 2012 que tem buscado tutelá-los.

Com efeito, em consonância com o entendimento de Brito (2013) a validade de normas penais que tem buscado reparar essa insuficiência legal poderia ser questionada com alegações relativas aos princípios do Direito Penal Mínimo e *ultima ratio*. Nesse contexto, Jesus (2016 apud Alexandre Jean Daoun 2011, p. 2) aduz que:

> a tônica principal é a seguinte: a desnecessidade de legislação penal nova, o direito penal para as relações virtuais é um direito penal mínimo. É isso que se recomenda. Minimamente usar o direito penal, sendo que se devem usar outros ramos do Direito para coibir as situações praticadas no ambiente eletrônico. Direito Penal deve ser guardado e resguardado para situações absolutamente extremas. Daí a crítica a essa compulsividade de legislar, de criar lei penal para isso, para aquilo, porque o Direito Penal é o instrumento mais drástico que se tem. Pagar uma indenização é uma coisa, perder a liberdade é outra. Então, para não se perder a credibilidade, é direito penal mínimo. E no ambiente virtual, 95% das relações que se tem já estão

> disciplinadas na legislação penal. Não há por que criar e falar tanto em legislação penal específica.

No entanto, não há como rejeitar a ideia de necessidade de pena no caso de condutas como as já estudadas, em razão do prejuízo sofrido por suas vítimas. Dessa forma, como é notório, a informática trouxe consigo uma série de novidades relativas à pratica de crimes já existentes. A ameaça, os crimes contra a honra, o furto, o estelionato, continuarão se caracterizando não importando se o modo de prática seja ou não através de recursos tecnológicos. Nesse sentido Brito (2013, p.152) destaca e alerta:

> Quanto aos denominados delitos impróprios, como o estelionato ou furto praticados pela internet, não se verifica a necessidade de alterações legislativas. Nova classificação do que já está definido e historicamente adaptado não somente ao meio jurídico, mas também à sociedade geral, gera desnecessária instabilidade jurídica e verdadeiro perigo à coletividade, notadamente em razão das inúmeras condenações fundamentadas nos tipos já existentes. Uma lei nova poderia causar o fenômeno que decidimos denominar atipicidade retroativa. Providência de bom alvitre seria a criação de uma agravante genérica ou mesmo de uma causa de aumento de pena nos casos de crimes comuns praticados com o uso da internet, pois, como já se afirmou acima, trata-se de instrumento facilitador de condutas indesejadas com inquestionável danosidade coletiva, situação que atualmente não se resolve tão somente com o aumento da pena-base pela intelecção do art. 59, caput, na primeira fase do cálculo da pena nos moldes do art. 68, ambos do Código Penal.

No que diz respeito à questão da fixação de competência, não foi constatada necessidade de alteração na lei. As disposições relativas aos ilícitos plurilocais ou transnacionais se encontram em conformidade com a Convenção de Budapeste, de forma que o trâmite processual pela justiça estadual continua sendo residual em relação à federal, conforme o artigo 109 da Constituição Federal (Brito, 2013).

Assim sendo, conforme explanação feita no corpo da pesquisa, o legislador nacional tem optado pela alteração ou inserção de novos tipos nos Códigos Penal e Processual Penal ao invés de se valer de legislação específica. Conforme sabedoria de Jesus (2016, p. 61):

> Tal premissa se justifica com o projeto de Lei nº 933/99 de autoria do Poder Executivo, que criou a Lei nº 9.983, de 14 de julho de 2000, nascida a princípio para proteger os sistemas da previdência social, e que posteriormente abrangeu toda a Administração Pública, alterando o Código penal para fazer prever as seguintes disposições envolvendo informática: a) no crime de divulgação de segredo, previsto no art. 153 do Código Penal, acrescentou o §1º A, punindo com detenção de um a quatro anos mais multa

> aquele que divulga, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou bancos de dados da Administração Pública; b) criação de novos tipos penais, a “”inserção de reclusão de dois a doze anos mais multa, e a “modificação não autorizada de sistema de informações, prevista no art 313-B, cominando pena de detenção de três meses a dois anos mais multa; c) a alteração do art. 325 do Código Penal, crime de violação de sigilo funcional, para acrescentar os §§1º e 2º, passando a punir com reclusão de dois a seis anos e multa quem permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública ou quem se utiliza indevidamente do acesso restrito.

Apesar de não ser um dos países signatários da Convenção de Budapeste, constata-se que o legislador pátrio tem buscado adaptar a legislação à realidade dos delitos informáticos, inserindo no ordenamento jurídico novos dispositivos que busquem tutelar as demandas ocasionadas pelos ilícitos praticados através ou contra os recursos tecnológicos.

4.1 Propostas Legislativas sobre os crimes cibernéticos

São muitos os projetos que existem em tramitação na Câmara buscando diminuir as brechas existentes na lei com relação às condutas ilícitas praticadas no meio informático, alguns trazem assuntos de grande repercussão e que não tem a devida regulamentação legal, outros trazem em seu bojo condutas já previstas sob outra nomenclatura em nosso Código Penal, mostrando-se ineficazes.

4.1.2 A reforma do Código Penal (Projeto de Lei do Senado nº 236 de 2012) e os crimes cibernéticos

Referido projeto que tem o intuito de reformar o Código Penal traz em seu corpo um título específico para os crimes cibernéticos, iniciando-se através de conceitos no artigo 208 para melhor entendimento do que trata seus artigos. Também tem o objetivo de tipificar os crimes de acesso Indevido, sabotagem informática, terrorismo, fraude informática, dano a dados informáticos, entre outros. Nesse sentido, Damásio de Jesus (2016, p. 186) explicita que:

> Em apertada síntese, estas são as principais propostas relacionadas à questão dos crimes informáticos trazidas por ocasião da apresentação do projeto de Lei de reforma do Código Penal, ainda em trâmite. Como se pode

> prever, certamente, muitos pontos mudarão e serão suprimidos, considerando que a fase de debates está se iniciando nas casas de Leis. Ainda assim, tal conteúdo é importante ao operador do Direito Penal Informático, na medida em que poderá se preparar de imediato para o futuro envolvendo a tipificação de novos delitos cibernéticos, bem como a adequação de velhos tipos para se fazer frente a situações delituosas envolvendo a tecnologia da informação.

No entanto, apesar dos intensos debates acerca do assunto, tem sido considerado um projeto carregado de falhas, sinalizando que está distante da aprovação (BRITO, 2013).

4.1.3 Projeto de Lei nº 7.758 de 2014

Se encontra em discussão na Câmara dos Deputados o referido projeto que tem o objetivo de tornar ilícito o uso de identidade falsa através da internet. De acordo com a proposta, sua finalidade baseia-se em criminalizar o indivíduo que usar da rede mundial de computadores com o intento de intimidar, prejudicar ou auferir vantagem ilícita, conforme artigo 307 *in verbis*:

> Art. 307. Atribuir-se ou atribuir a terceiro falsa identidade, inclusive por meio da rede mundial de computadores ou qualquer outro meio eletrônico, com o objetivo de prejudicar, intimidar, ameaçar, obter vantagem ou causar dano a outrem, em proveito próprio ou alheio:
> Pena – detenção de 3 (três) meses a 1 (um) ano, ou multa, se o fato não constitui elemento de crime mais grave.

Não obstante, de acordo com Jesus (2016) a referida proposta não se justifica uma vez que o delito do artigo 307 do Código Penal, do jeito que se encontra já é dotado de capacidade para abranger e punir a citada conduta ilícita. Nessa perspectiva aponta:

> Além disso, pela proposta não se alterou a pena para o delito e o interessante seria o agravamento da pena em casos de internet. Não bastasse, o projeto de Lei nº 7.758/2014 dispõe que o objetivo do perfil falso deve ser o de prejudicar, intimidar, ameaçar, obter vantagem ou causar dano a outrem. Aquele que criasse um perfil falso humorístico, por exemplo, seria punido. Ademais, “prejudicar” é expressão por demais vaga, podendo restar em interpretações forçosas” (JESUS, 2016, p.189).

Dessa maneira, a criação do referido artigo de lei demonstra mais uma vez a ineficiência na edição de dispositivos que procuram tutelar o tema.

5 CONCLUSÃO

O presente trabalho teve como objetivo expor a discussão atinente à necessidade de modificação dos Códigos Penal e Processual Penal nos delitos relacionados à criminalidade cibernética. Para tal fez-se necessário abordar sucintamente sobre os aspectos que norteiam o ordenamento jurídico penal quando aplicado aos delitos cujo alvo são os recursos tecnológicos.

A legislação penal vigente como vimos ao longo deste trabalho tem tutelado grande parte dos delitos praticados através do computador ou da internet. Os crimes informáticos impróprios, segundo entendimento de grande parte da doutrina, não têm necessitado de modificação legal, haja vista já se mostrarem eficazes e aptos a abarcar as condutas ilícitas em questão. No que tange aos delitos informáticos próprios ou mistos, há um consenso no sentido de que a modificação legal é necessária. Tal fato tem sido corroborado através da edição das Leis nº 12.735 e 12.737 de 2012, que vieram tutelar ilícitos praticados contra dados ou informações constantes em aparelhos eletrônicos.

Contudo, na prática, apesar de já ser um grande avanço na tutela dos bens jurídicos em questão, referidos dispositivos têm se mostrado insuficientes ou deficitários, uma vez que tem dado margem a interpretações dos mais variados tipos, necessitando de certa especificidade técnica. Nesse sentido, o legislador tem procurado adequar nossa legislação a já mencionada Convenção de Budapeste, procurando uniformizar os dispositivos de lei, apesar de não a ter ratificado.

Portanto, consideramos tratar de um tema que ainda merece amadurecimento doutrinário e jurisprudencial. Todos os fatos apontados no decorrer deste trabalho apontam para a necessitade de flexibilização da lei e sua adaptabilidade à constante mutação social. A evolução tecnológica é uma situação inevitável e se encontra em constante ascensão. Nosso ordenamento jurídico deve se adaptar a esse fato, devem os legisladores estarem atentos à realidade que os cercam e estarem aptos a sempre dar uma resposta satisfatória à sociedade, buscando garantir dos direitos fundamentais e o combate à impunidade.

REFERÊNCIAS

BRASIL. Câmara dos Deputados. *Projeto de Lei 7.758/2014*. Modifica o disposto no art. 307 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal. Disponível em: <http://www.praticadapesquisa.com.br/2011/06/como-apresento-referencia-de-um-projeto.html> Acesso em 05 de junho de 2018.

BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Disponível em: <http://www.senado.gov.br>. Brasil – Diário Oficial da União. Acesso em 01 de maio de 2018.

BRASIL. *Decreto-Lei nº 3.689, de 03 de outubro de 1941.* Código de Processo Penal. Brasil – Diário Oficial da União. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm>. Acesso em 05 de maio de 2018.

BRASIL. *Lei nº 9.296 de 24 de julho de 1996*. Lei de Interceptação Telefônica. Brasil – Diário Oficial da União. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/l9296.htm> Acesso em 10 de maio de 2018.

BRASIL. *Lei nº 12.735 de 30 de novembro de 2012*. Altera o Decreto-Lei nº 2848, 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 informados e similares e da outras providências. Brasil – Diário Oficial da União. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm> Acesso em: 12 de maio de 2018.

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 da outras providências. Brasil – Diário Oficial da União. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em 10 de maio de 2018.

BRITO, Auriney. *Direito Penal Informático.* 1ª ed. São Paulo: Saraiva, 2013, 189p.

CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e seus Aspectos Processuais*. 2ª ed. Rio de Janeiro: Lumen Juris, 2003, 219 p.

CASTELLS, Manuel. *A galaxia da internet: reflexões sobre a internet, os negócios e a sociedade*. Rio de Janeiro: Jorge Zahar, 2003, p.243

CORRÊA, Gustavo Testa. *A questão da tributação na internet*. In: ROVER, Aires José (Org.). *Direito, sociedade e informática: limites e perspectivas da vida digital.* Florianópolis: Boiteaux. 2000, 248p.

COSTA, Marco Aurélio Rodrigues da. *Crimes de Informática*. Publicado em outubro de 1995. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1826>. Acesso em 13 abril 2018.

CUNHA, Rogério Sanches. *Direito Penal – Parte Especial.* 8º ed. Salvador: Juspodvum, 2016, 941p.

CUNHA, Rogério Sanches. *Direito Penal – Parte Geral.* 4ª ed. Salvador: Juspodvum, 2016, 557 p

D'ARAUJO, Maria Celina. *O AI-5.* Disponível em: <http://cpdoc.fgv.br/producao/dossies/FatosImagens/AI5> Acesso em 18 de junho de 2018.

FERREIRA, Lilian. *O que é DNS e o que ele tem a ver com a minha conexão com a Internet?*. Publicado em 24 de julho de 2008. Disponível em: <https://tecnologia.uol.com.br/dicas/ultnot/2008/07/24/ult2665u363.jhtm> Acesso em 11 de junho de 2018.

FERREIRA, Ivette Senise. *A criminalidade informática*. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coord.) Direito & Internet: *Aspectos Jurídicos Relevantes*. Bauru: Edipro, 2000.

G1. *Operação da PF contra fraudes em vestibulares já prendeu 52*. Publicado em 18 de dezembro de 2012. Disponível em: <http://g1.globo.com/espirito-santo/noticia/2012/12/operacao-da-pf-contra-fraudes-em-vestibulares-ja-prendeu-52.html>. Acesso em: 15 maio de 2018.

GRECO, Rogério, *Curso de Direito Penal*, 18º ed. Rio de Janeiro: Impetus, 2016, 945 p.

HABIB, Gabriel, *Leis Penais Especiais*, 7º ed. Salvador: Juspdvum, 2015, 395 p.

JESUS, D.; MILAGRE, J.A.; *Manual de Crimes Informáticos*. 1º ed. São Paulo: Saraiva, 2016, 208 p.

LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional*. Campinas: Millennium, 2006, 192p.

LEMOS, Ronaldo. *O marco civil como símbolo do desejo por inovação no Brasil*. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). *Marco Civil da Internet*. São Paulo, Atlas, 2014, p. 04.

MARTINS, Elaine. *O que é TCP/IP?.* Publicado em 29 de maio de 2012. Disponível em: < https://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-.htm> Acesso em 22 de junho de 2018.

MÜLLER, Leonardo. *O que é Phishing?.* Publicado em 05 de julho de 2012. Disponível em: <https://www.tecmundo.com.br/phishing/205-o-que-e-phishing-.htm> Acesso em: 05 de maio de 2018.

PINHEIRO, Patrícia Peck. *Direito Digital*. 4. ed. São Paulo: Saraiva, 2010, 272 p.

SILVA, Ângelo Roberto Ilha, *Crimes Cibernéticos*, 2º ed. Porto Alegre: Livraria do Advogado, 2018, 270 p.