CENTRO UNIVERSITÁRIO FACULDADE GUANAMBI

BACHARELADO EM DIREITO

AYUME DA SILVA ASSUNÇÃO

A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da Lei nº 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos

GUANAMBI-BA

2021

AYUME DA SILVA ASSUNÇÃO

A tipicidade dos crimes cibernéticos no direito penal brasileiro: Um estudo sobre o impacto da Lei nº 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos

Artigo científico apresentado ao Curso Superior de Direito do Centro Universitário Faculdade Guanambi como requisito de avaliação da disciplina Trabalho de Conclusão de Curso 2.

Orientador: Prof. Eujécio Cotrim

GUANAMBI-BA

2021

SUMÁRIO

A tipicidade dos crimes cibernéticos no direito penal brasileiro: Um estudo sobre o impacto da Lei nº 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos

Ayume da Silva Assunção[1], Eujécio Cotrim[2]

[1] Graduanda do curso de Bacharelado em Direito do Centro Universitário de Guanambi – UniFG.
[2] Docente do curso de Direito do Centro Universitário de Guanambi – UniFG.

RESUMO: O presente artigo trata sobre a tipicidade dos Crimes Cibernéticos no Direito Penal Brasileiro, consistindo em um estudo a respeito do impacto da Lei nº 12.737/2012, a dogmática penal dos crimes realizados através da internet. A priori, foi realizado um breve apanhado de conceitos relacionados aos crimes cibernéticos, bem como, a respeito da lacuna legislativa presente no ordenamento jurídico brasileiro a respeito desta temática. Posteriormente é desenvolvida uma análise acerca da interpretação da lei penal à luz do princípio da Legalidade e da eficiência da Lei n°12.015 de 2009, bem como da Convenção de Budapeste. A metodologia utilizada para a construção do estudo foi em formato de pesquisa bibliográfica, respaldada por grandes doutrinadores do Direito Penal, jurisprudência e legislação, além de artigos renomados sobre o tema. Ao final, verificou-se que diante dos Crimes Cibernéticos, é notável evidenciar que a falta de tipificação adequada para os delitos praticados no ambiente cibernético, promove insegurança tanto para a sociedade quanto para o âmbito jurídico brasileiro. É necessária a adoção de uma legislação específica que trate a respeito da presente temática, com normas claras e eficientes, de modo que promova segurança à sociedade e punição àqueles que se utilizam de meios escusos para provocar danos matérias e morais a terceiros.

PALAVRAS-CHAVE: Crimes Cibernéticos. Tipicidade. Princípio da Legalidade.

ABSTRACT: This article deals with the typicality of Cyber Crimes in Brazilian Criminal Law, consisting of a study about the impact of Law No. 12,737/2012, the penal dogmatics of crimes

Endereço para correspondência: Rua Milão, n° 117, B.: São Sebastião, Condomínio Park Boulevard
Endereço eletrônico: AyumeSilva98@gmail.com

carried out through the internet. A priori, a brief overview of concepts related to cyber crimes was carried out, as well as the legislative gap present in the Brazilian legal system regarding this theme. Subsequently, an analysis of the interpretation of criminal law is carried out in light of the principle of Legality and the efficiency of Law No. 12,015 of 2009, as well as the Budapest Convention. The methodology used for the construction of the study was in the form of a bibliographic research, supported by great scholars of Criminal Law, jurisprudence and legislation, in addition to renowned articles on the subject. In the end, it was found that in the face of Cyber Crimes, it is remarkable to show that the lack of adequate classification for crimes committed in the cyber environment, promotes insecurity both for society and for the Brazilian legal sphere. It is necessary to adopt specific legislation dealing with this subject, with clear and efficient rules, in order to promote security to society and punishment to those who use shady means to cause material and moral damages to third parties.

KEYWORDS: Cyber Crimes. Typicality. Principle of Legality.

1. INTRODUÇÃO

O presente artigo tem por desígnio abordar a importância em torno da positivação dos crimes cibernéticos, contextualizando sobre o déficit em torno do sistema jurídico brasileiro e principalmente do Código Penal envolvendo a culpabilidade das condutas ilícitas praticadas no ambiente virtual, além de mencionar acerca da ineficiência da Lei nº 12.737/12, promovendo insegurança social e jurídica.

Para produção do presente estudo, houve um levantamento bibliográfico, com o uso de doutrinas renomadas pelo Direito Penal Brasileiro, como Guilherme de Souza Nucci, Cleber Masson, Rogério Grecco, Damásio de Jesus, José Antônio Milagre, entre outros. Também foram utilizadas jurisprudências, além de legislações nacionais e internacionais que regulamentem acerca da relação entre os Crimes Cibernéticos e a lacuna em torno da codificação dos referidos ilícitos virtuais dentro do ordenamento jurídico brasileiro.

Em seu aspecto metodológico, o método de pesquisa empregado no presente projeto é o qualitativo, apoiando-se em técnicas de coleta de dados e materiais que levam à análises e reflexões.

A inexistência da culpabilidade pelos crimes cibernéticos é preocupante, pois a mesma consiste na condição regular necessária para fundamentar juridicamente uma responsabilidade, sendo constituída por livre arbítrio e juízos sobre a realidade, criando um sistema de subjetividade individual de aferição da culpabilidade do agente. Não é apenas a percepção cultural, mas a percepção da realidade em si, o que alteraria a capacidade de entender o caráter ilícito da conduta e de se adequar perante tal entendimento.

Assim, na ausência de uma legislação específica, aquele que praticou algum ato ilícito cibernético, deverá ser julgado dentro do próprio Código Penal, mantendo-se as devidas diferenças. No Direito Brasileiro existe o instituto da analogia, consistindo na integração do ordenamento jurídico com a intenção de suprir lacunas na lei, de forma que se torna aplicável ao caso omisso, uma lei que prejudique o réu e que regulamente a prática de um ato ilícito semelhante.

A princípio, seria uma ótima alternativa para tipificar ações ilícitas praticadas no âmbito virtual, porém, a maioria da doutrina do Direito Penal Brasileiro, como Rogério Sanches Cunha, Guilherme de Souza Nucci e Cleber Masson, em outras áreas do Direito esse instituto pode ser aplicado com eficiência, mas no ordenamento penal, a sua aplicação necessita ser cuidadosamente avaliada, pelo fato desta possibilidade poder ferir o princípio constitucional da legalidade.

Sendo assim, o epicentro da discussão sobre os crimes cibernéticos está assentado no princípio da legalidade, caracterizado como princípio basilar do Direito Penal. Diante dessa temática, surgem os seguintes questionamentos: Como punir possíveis infratores desses crimes diante da ausência de lei descrevendo tal conduta como criminosa? O Estado-Juiz pode aplicar sanções para comportamentos não tipificados em lei? É nesse diapasão que se discute a atipicidade dessas condutas e a consequente isenção de punição desses indivíduos.

2. MATERIAIS E MÉTODOS

A Metodologia descreve os procedimentos de coleta e análise dos dados e os materiais que levam à obtenção dos resultados (MOTA-ROTH; HENDGES; 2010)[2]. O método de pesquisa utilizado é o qualitativo, apoiando-se em técnicas de coleta de dados. De acordo com Neves (1996, p.01)[3], a pesquisa qualitativa não busca enumerar ou medir eventos. Ela serve para obter dados descritivos que expressam os sentidos dos fenômenos. A referida pesquisa se classifica como sendo exploratória proporcionando maiores informações sobre o referido tema, além de ser qualificada como sendo uma cadeia de raciocínio pelo método dedutivo, que a partir de teorias e leis gerais pode-se chegar à determinação ou previsão de fenômenos particulares. (MARCONI e LAKATOS, 2017)[4]

Para que o estudo seja possível, houve um levantamento bibliográfico, com o uso de doutrinas renomadas pelo Direito Brasileiro, jurisprudências e demais legislações que regulamentem acerca da relação entre os Crimes Cibernéticos, a lacuna em torno da codificação dos referidos ilícitos dentro do ordenamento jurídico brasileiro e seus possíveis problemas para a segurança jurídica e para a sociedade.

3. CRIMES CIBERNÉTICOS

[2] MOTTA-ROTH, Désirée; HENDGES, Graciela H. Produção textual na universidade. São Paulo: Parábola Editorial, 2010.
[3] NEVES, J. L. Pesquisa qualitativa: características, usos e possibilidades. Caderno de pesquisa em administração, v. 1., n. 3., 1996.
[4] MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Fundamentos de Metodologia Científica, 8ª Ed. Atlas, 2017.

Os crimes cibernéticos consistem no cometimento de atividades ilícitas por meio do computador ou rede de internet e classificam-se de acordo com a sua forma de cometimento (WENDT; JORGE, 2012)[5].

Diante a ausência de uma legislação específica que abordasse a temática, cabe ao ordenamento penal vigente julgar aquele que comete crime cibernético. De acordo com uma pesquisa desenvolvida pelo site Safernet, entre os principais crimes cibernéticos, estão: pirataria, pornografia infantil, calunia, difamação, injúria, estelionato, entre outros (SANTOS; MARTINS; TYBUCSH, 2017)[6].

A pornografia infantil caracteriza-se pelo ato de fotografar ou publicar cenas de sexo explícito que contenham crianças ou adolescentes, nos moldes do art. 241 do ECA. Injúria, difamação e calúnia são considerados crimes contra a honra e estão regulamentados nos artigos 138, 139 e 140 do Código Penal. No ambiente da internet, os crimes de calúnia e difamação, consideradas ofensas à honra objetiva, são caracterizados caso a ofensa seja enviada para grande público e não somente para a vítima, já tratando-se de injúria, considerada ofensa à honra subjetiva, a ofensa é direcionada para a própria vítima (SANTOS; MARTINS; TYBUCSH, 2017).

Tratando-se do crime de estelionato no ambiente da internet, o sujeito ativo mantém a vítima em erro, sob a finalidade de obter vantagem ilícita para si próprio. Também considera-se crime cibernético exaltar ou elogiar criminoso ou ato criminoso de maneira pública, caracterizando crime de apologia de crime ou de criminoso. Outro exemplo, consiste no oferecimento, utilizando a internet, de consumo a substância entorpecente, ou que sujeite a pessoa a depender-se fisicamente ou psicologicamente, caracterizando tráfico de drogas (SANTOS; MARTINS; TYBUCSH, 2017).

4. A INTERPRETAÇÃO DA LEI PENAL À LUZ DO PRINCÍPIO DA LEGALIDADE

Assim como dispõe Matsuyama e Lima (2017)[7], o princípio da legalidade consiste em um dos mais importantes do ordenamento penal brasileiro. Ele encontra-se positivado no art. 5º, inciso XXXIX da Constituição Federal de 1988: “Não há crime sem lei anterior que o defina,

[5] WENDT, Emerson; JORGE, Higor Vinícius Nogueira. Crimes cibernéticos: Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012. p 10.

[6] SANTOS, Liara Ruff dos; MARTINS, Luana Bertasso; TYBUCSH, Francielle Benini Agne. Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo. 2017.

[7] MATSUYAMA, Keniche Guimarães; LIMA, JAA. Crimes cibernéticos: atipicidade dos delitos. 2017.

nem pena sem prévia cominação legal", também é receptível a menção ao referido princípio no art. 1º do Código Penal. Nesse sentido, Rogério Greco (2015)[8] define:

> 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. Tudo o que não for expressamente proibido é lícito em Direito Penal. (GRECO, 2015, p.144).

Conforme estabelece a própria Lei Maior, no ordenamento jurídico brasileiro, não se concebe que um fato seja considerado como crime sem que exista lei anterior que descreva tal conduta como delituosa. A legislação consiste na única fonte capaz de impor punição à prática de atos que ela mesma caracteriza como sendo ilícitos, configurando na limitação ao poder do Estado de interferir na esfera de liberdades dos indivíduos. O autor Cleber Masson (2015)[9] entende que o princípio em questão, versa pela:

> [...] exclusividade da lei para a criação de delitos (e contravenções penais) e cominação de penas, possuindo indiscutível dimensão democrática, pois revela a aceitação pelo povo, representado pelo Congresso Nacional, da opção legislativa no âmbito criminal. De fato, não há crime sem lei que o defina, nem pena sem cominação legal (*nullum crimen nulla poena sine lege*). (MASSON, 2015, p.82).

5. O DIREITO PENAL CIBERNÉTICO ENQUANTO RAMO DO DIREITO PENAL

Não há consenso sobre qual a terminologia a ser empregada para os crimes que acontecem no âmbito virtual ou informático. Patrícia Santos da Silva (2015)[10] , na intenção de demostrar esse problema, afirma:

> [...]que não há uma nomenclatura sedimentada pelos doutrinadores acerca do conceito de crime cibernético. De uma forma ou de outra o que muda é só o nome atribuído a esses crimes, posto que devem ser observados o uso de dispositivos informáticos, a rede de transmissão de dados para delinquir, o bem jurídico lesado, e ainda deve a conduta ser típica, antijurídica e culpável. (SILVA, 2015, p.39).

---

[8] GRECO, Rogério. Curso de Direito Penal. 17. ed. Rio de Janeiro: Impetus, 2015.

[9] MASSON, Cleber. Direito penal esquematizado – Parte geral – vol. 1. 9.ª ed. Rio de Janeiro: Forense; São Paulo: Método, 2015.

[10] SILVA, Patrícia Santos da. Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015.

A internet se tornou a promessa de um futuro melhor para a humanidade, por ser uma espetacular ferramenta de troca de conhecimento. A liberdade é a característica mais atribuída à internet. Como um mundo sem fronteiras. Mas há um lado nocivo trazido por esta ausência de normas e regras (SILVA, 2015).

Importante lembrar-nos que a função do Direito Penal consiste em coibir condutas divergentes daquelas tipificadas, impondo sanção e protegendo bens jurídicos. Para isso, uma estrutura normativa é gerada, criando uma lógica própria. Essa normatividade tem uma dupla função, já que ao tempo em que a pena (enquanto sanção normativa) é uma forma de garantir a eficácia do sistema penal, esta possui seu limite já imposto, servindo como uma garantia.

Os autores Jesus e Milagre (2016)[11], trazem consigo a classificação mais precisa de delito informático, dividindo o delito em quatro tipos, crimes de informática próprios, crimes de informática impróprios, crimes de informática mistos e crimes de informática mediato ou indireto.

> a) crimes informáticos próprios: em que o bem jurídico ofendido é a tecnologia da informação em si, Para estes delitos, a legislação penal era lacunosa, sendo que, diante do princípio da reserva penal, muitas práticas não poderiam ser enquadradas criminalmente;
> b) crimes informáticos impróprios: em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum tipo penal;
> c) crimes informáticos mistos: são crimes complexos em que, além de proteção do bem jurídico informático (inviolabilidade dos dados), a legislação protege outro bem jurídico. Ocorre à existência de dois tipos penais distintos, cada qual protege um bem jurídico;
> d) crime informático mediato ou indireto: trata-se delito informático praticado para a ocorrência de um delito não informático consumando ao final.
> Em Direito Informático, comumente um delito informático é cometido como meio para a prática de um delito-fim ordem patrimonial. Como, por exemplo, no caso do agente que captura dados bancários e usa para desfalcar a conta corrente da vitima. Pelo principio da consunção, o agente só será punido pelo delito-fim (furto) (JESUS; MILARE, 2016, p. 49).

A codificação penal transcende a esfera jurídica, sendo também resultado de uma relação social. Os comportamentos divergentes daqueles aceitos, e até impostos, pela sociedade, são considerados como Anomia. Esse conceito sociológico tem papel fundamental no entendimento da tipificação de condutas humanas pelo Direito Penal. Essas condutas são a base para a tipificação de crimes em uma sociedade, já que o Direito Penal retira os conceitos de condutas humanas a partir de condutas possíveis e já valoradas pela sociedade.

[11] JESUS, Damásio de, e MILAGRE, José Antonio. Manual de crimes informáticos. São Paulo: Saraiva, 2016.

Nesse sentido, Conde (1988)[12] assegura que o ponto de partida é a Tipicidade das condutas ilícitas praticadas no mundo virtual, sendo a norma jurídica o ator principal nas relações jurídicas. A construção dessa dogmática passa, necessariamente por uma análise da tipificação dos tipos penais cibernéticos.

6. A LEI 12.737/2012 E A (DES)CONSTRUÇÃO DE UMA DOGMÁTICA PENAL DOS CRIMES CIBERNÉTICOS

O sistema penal brasileiro já havia reconhecido algumas condutas como próprias do sistema informático. A lei nº 9.983/03 foi editada incluindo no sistema jurídico brasileiro os artigos 313-A e 313-B. Mas somente no ano de 2012, foi editada e sancionada com a intenção de ser a primeira lei específica de crime cibernética no sistema brasileiro, a Lei nº 12.737/2012[13] (Lei Carolina Dieckmann). Ela ganhou esse apelido por consequência de um caso de invasão de dispositivo informático por meio de Hackers de uma atriz brasileira que foi, inclusive, chantageada.

A referida Lei criou o artigo 154-A, que fora acrescido no Código Penal brasileiro, *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.

A partir do estudo do presente dispositivo é notável observar que o núcleo do tipo é invadir, porém a base do tipo penal é a conduta humana, e invadir é um verbo de conduta real, não conduta informática. O verbo mais lógico seria acessar, ou ter acesso.

Outro aspecto interessante que deve ser observado consiste na condicionante de modo, tendo em vista que a invasão deve ser mediante violação indevida de mecanismo de segurança. Torna-se perceptível a imprecisão do legislador, que possibilita a realização do tipo penal com a violação de senha de bloqueio de tela, por exemplo, de um celular. Esse tipo penal tem dolo

---

[12] CONDE, Francisco Muñoz. Teoria Geral do Delito. Porto Alegre:Sergio Antonio Fábris Editor, 1988.

[13] BRASIL. Lei 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2012/lei/l12737.htm. Acesso em 11 de maio de 2021.

específico, já que o agente ao invadir tem que ter como vontade específica obter, adulterar ou destruir dados ou informações ou instalar vulnerabilidade para obter vantagem indevida. Como se percebe não se pune a conduta culposa. O dolo específico também se torna possível seguindo o §1º desse mesmo artigo.

O renomado doutrinador Guilherme Nucci (2014)[14], abordando o tipo penal definido no caput do artigo 154-A classifica-o como:

> [...] crime comum (pode ser cometido por qualquer pessoa); formal (delito que não exige resultado naturalístico, consistente na efetiva lesão à intimidade ou vida privada da vítima, embora possa ocorrer); de forma livre (pode ser cometido por qualquer meio eleito 129 pelo agente); comissivo (as condutas implicam ações); instantâneo (o resultado se dá de maneira 47 determinada na linha do tempo), podendo assumir a forma de instantâneo de efeitos permanentes, quando a invasão ou a instalação de vulnerabilidade perpetua-se no tempo, como rastro da conduta; unissubjetivo (pode ser cometido por uma só pessoa); plurissubsistente (cometido por vários atos); admite tentativa (NUCCI, 2014, p. 814).

Conforme alega Castro (2018)[15], diante das circunstâncias analisadas da presente Lei, torna-se evidente a pressa do legislador em criar esse tipo penal, já que havia à época uma pressão midiática para a incriminação dessa conduta, por envolver uma atriz de grande prestígio em todo o país.

O tipo penal fora mal redigido e com o abuso de elementos normativos, contrariando a taxatividade. Dentre esses tipos penais elencados, o que se pode perceber é que todos possuem como elemento subjetivo a modalidade dolosa. Não quis o legislador brasileiro incriminar a modalidade culposa. O legislador da referida codificação, possui pouca informação sobre o sistema informático, e isso é agravado pala falta de reflexão por parte da Dogmática Penal Brasileira, refletindo a lacuna normativa e a falta de debate em torno da moralidade das condutas cibernéticas, bem como as consequências e prejuízos causados por essas condutas (CASTRO, 2018).

A inexistência da culpabilidade é preocupante, pois a mesma consiste na condição regular necessária para fundamentar juridicamente uma responsabilidade, sendo constituída por livre arbítrio e juízos sobre a realidade, criando um sistema de subjetividade individual de aferição da culpabilidade do agente. Não é apenas a percepção cultural, mas a percepção da

[14] NUCCI, Guilherme de Souza. Código penal comentado. 14. ed. Rio de Janeiro: Forense, 2014.

[15] CASTRO, Aldemario Araujo. A internet e os tipos penais que reclamam ação criminosa em público. 2018. Disponível em: https://egov.ufsc.br/portal/sites/default/files/anexos/13308-13309-1-PB.pdf. Acesso em 11 de maio de 2021.

realidade em si, o que alteraria a capacidade de entender o caráter ilícito da conduta e de se adequar perante tal entendimento.

7. CONVENÇÃO DE BUDAPESTE

Essa referida convenção consiste em um ordenamento desenvolvido pelo Conselho da Europa em 2002, em que seu objetivo girava em torno da proteção da sociedade contra a criminalidade no ciberespaço. A princípio, a Convenção de Budapeste promovia a escolha de uma legislação comum que objetivasse uma maior cooperação entre os Estados da União Europeia, mas atualmente encontra-se aberta à assinatura por todos os países que a desejarem, tendo em vista que os crimes cibernéticos atingem todos os territórios do mundo (FERNANDES, 2013)[16].

Desde o planejamento até a elaboração da Convenção de Budapeste, transcorreram aproximadamente cinco anos, enquanto isso, no território brasileiro os julgadores pouco estão se importando para a aprovação de projetos de lei com a temática em questão, levando à instabilidade no meio social e à insegurança no âmbito jurídico (FERNANDES, 2013).

No Direito Internacional, existe o Direito Internacional Uniforme, utiliza por quase todos os países do mundo, que ocorre quando coincidem os direitos primários entre ordenamentos, seja porque têm a mesma origem, ou por sofrerem influências idênticas, ou, ainda, quando países adotam sistemas jurídicos clássicos total ou parcialmente, de outros Estados (FERNANDES, 2013).

Uma hipótese a favor da segurança jurídica do Direito Brasileiro em vista da tipificação dos crimes cibernéticos, configura-se no fato do Brasil adotar a Convenção de Budapeste, tendo em vista que, o conteúdo dos projetos de leis, que se encontram há anos sob o julgamento do Congresso Nacional, é similar aos tratados pela referida Convenção (FERNANDES, 2013).

8. CONSIDERAÇÕES FINAIS

Os delitos cometidos através da internet são presentes em todo o mundo, entretanto, o Brasil encontra-se atrasado por não dispor de uma legislação específica e adequada à regulamentação e punição àqueles que cometem as condutas delituosas em questão.

---

[16] FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. *REVISTA DA FACULDADE DE DIREITO DA UFMG*, 2013, 2013.62: 139-178.

A falta de tipificação adequada para os delitos praticados no ambiente cibernético, promove insegurança tanto para a sociedade quanto para o âmbito jurídico brasileiro. As tentativas fracassadas de projetos de lei ou mesmo a publicação apressada de legislações, como é o caso da Lei nº 12.737/2012, geraram inúmeras consequências em desfavor da adequada classificação e regulamentação dos crimes em questão. É necessária cautela na instauração de um ordenamento sob o referido tema, tendo em vista que o ambiente virtual está em constante evolução, devendo ser estudado de forma adequada.

Sendo assim, a favor da segurança do desenvolvimento da sociedade e da segurança do âmbito jurídico brasileiro, faz-se necessário um maior investimento no âmbito de segurança da informação, além de treinamento especializado dos agentes para que haja uma persecução penal efetiva e atual, lembrando que o Código Penal brasileiro é de 1940, período em que não existia as tecnologias usadas atualmente e notoriamente, não existiam os crimes cibernéticos (FERNANDES, 2013).

Com a existência de condutas atípicas que não podem ser punidas em decorrência do princípio da legalidade ou da reserva legal, é essencial a elaboração de um ordenamento específico além da adoção do Brasil a tratados internacionais que disciplinam sobre o conteúdo em questão para adequação da legislação interna, como é o caso da Convenção de Budapeste.

Diante a expansão do espaço cibernético em todo o mundo, a adoção à Convenção consistiria no dever preventivo do Estado, tendo em vista que promoveria a utilização de normas claras e eficientes, de modo que promova segurança à sociedade e punição àqueles que se utilizam de meios escusos para provocar danos matérias e morais a terceiros.

REFERÊNCIAS

BRASIL. Lei 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 11 de maio de 2021.

CASTRO, Aldemario Araujo. A internet e os tipos penais que reclamam ação criminosa em público. 2018. Disponível em: https://egov.ufsc.br/portal/sites/default/files/anexos/13308-13309-1-PB.pdf. Acesso em 11 de maio de 2021.

CONDE, Francisco Muñoz. Teoria Geral do Delito. Porto Alegre:Sergio Antonio Fábris Editor, 1988.

FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. REVISTA DA FACULDADE DE DIREITO DA UFMG, 2013, 2013.62: 139-178.

GRECO, Rogério. Curso de Direito Penal. 17. ed. Rio de Janeiro: Impetus, 2015.

JESUS, Damásio de, e MILAGRE, José Antonio. Manual de crimes informáticos. São Paulo: Saraiva, 2016.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Fundamentos de Metodologia Científica, 8ª Ed. Atlas, 2017.

MASSON, Cleber. Direito penal esquematizado – Parte geral – vol. 1. 9.ª ed. Rio de Janeiro: Forense; São Paulo: Método, 2015.

MATSUYAMA, Keniche Guimarães; LIMA, JAA. Crimes cibernéticos: atipicidade dos delitos. 2017.

MOTTA-ROTH, Désirée; HENDGES, Graciela H. Produção textual na universidade. São Paulo: Parábola Editorial, 2010.

NEVES, J. L. Pesquisa qualitativa: características, usos e possibilidades. Caderno de pesquisa em administração, v. 1., n. 3., 1996.

NUCCI, Guilherme de Souza. Código penal comentado. 14. ed. Rio de Janeiro: Forense, 2014.

SANTOS, Liara Ruff dos; MARTINS, Luana Bertasso; TYBUCSH, Francielle Benini Agne. Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo. 2017.

SILVA, Patrícia Santos da. Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. Crimes cibernéticos: Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012. p 10.