AS PRINCIPAIS NUANCES DOS CRIMES CIBERNÉTICOS

Karine da Silva Vieira[1]
Marcos Túlio Fernandes Melo[2]

RESUMO

O presente artigo teve como objetivo avaliar as principais nuances acerca dos crimes cibernéticos, bem como a aplicação da legislação brasileira diante do tema. Para isso, foi necessário entender o espaço em que se enquadra esse tipo penal, para então compreender as consequências jurídicas aplicáveis. No intuito de obstar a execução dos crimes de informática, foram promulgadas as leis 12.735 e 12.737, ambas do ano de 2012, causando impactos na sociedade da informação por meio da inserção e alteração de artigos do Código Penal Brasileiro. Desta forma, este artigo, buscou analisar detalhadamente o texto das leis supramencionadas e de outros objetos jurídicos elaborados, assim como as modificações resultantes ao ordenamento jurídico pátrio.

Palavras-chave: Crimes cibernéticos. Crimes virtuais. Legislação brasileira.

1. INTRODUÇÃO

A agilidade da internet nos proporciona a realização de atividades como o entretenimento, pagamento de despesas, trabalho, namoro, dentre outros. Todavia, facilita a ação de pessoas desonestas que se aproveitam do anonimato e da falta de segurança da rede para conseguir dados e informações dos usuários. A cada dia, aumenta mais a prática de diferentes atos cometidos por meio da internet.

Diante dessa nova era digital, a legislação brasileira tem a difícil tarefa de se adequar a esses avanços tecnológicos para não se tornar refém desta criminalidade sem identidade certa. Porém, não há dúvidas sobre a evolução tecnológica em nosso país, mas à medida que se aumentam os crimes virtuais, questiona-se: como o sistema jurídico brasileiro aborda tal delito?

Mesmo que lentamente, algumas medidas, de acordo com a necessidade, vêm sendo projetadas pela legislação brasileira no intuito de coibir a criminalidade virtual, por exemplo,

---

[1]UNIVAG – Centro Universitário. Área do Conhecimento de Ciências Sociais Aplicadas. Curso de Direito. Aluna da disciplina TCC II, turma DIR 13/1 CN. E-mail – karinevieiradireito@gmail.com.
[2] UNIVAG – Centro Universitário. Área do Conhecimento de Ciências Sociais Aplicadas. Curso de Direito. Mestre, Orientador. E-mail – marcostulioadvocacia@hotmail.com.

a Lei 12.737/2012, denominada e comumente conhecida como “Lei Carolina Dieckmann”, que tipifica criminalmente os delitos cibernéticos, caracterizando condutas que não eram previstas especificamente como infração penal, acrescentando e alterando alguns artigos do Código Penal Brasileiro.

Mesmo diante da extrema necessidade de uma legislação específica para pormenorizar os crimes cibernéticos, há projetos e leis que nos encaminham a acreditar que talvez possa ser possível deter a ação de muitos criminosos que agem por meio da internet.

2. SURGIMENTO DOS CRIMES CIBERNÉTICOS

Acredita-se que os crimes cibernéticos vêm sendo praticados no mundo por mais de cinco décadas, desde as primeiras referências até os dias atuais, propagando e se desenvolvendo conforme a globalização dessa nova era digital.

Segundo Jesus: “Para a doutrina internacional, os crimes virtuais tiveram inicio na década de 1960, quando foram identificadas as primeiras referências sobre o tema, cuja maior parte foi de delitos de alteração, cópia e sabotagem de sistemas computacionais.” [3]

Todavia, a doutrina diverge-se em relação ao primeiro delito de informática cometido. Enquanto para alguns o primeiro delito ocorreu no âmbito da MIT (*Massachusetts Institueof Technology) no ano de 1964,* em que um aluno de 18 anos teria cometido um ato classificado como crime cibernético, outros defendem que o primeiro caso ocorreu na Universidade de Oxford em 1978, onde um estudante copiou de uma rede de computadores uma prova.

O que se sabe, é que foi na década de 1970 que os hackers começaram a ser citados e relacionados aos crimes virtuais, todavia, tenha sido em 1980 o maior alastramento dos mais diferentes delitos pertinentes aos crimes cibernéticos.

> Na década de 70 a figura do *Hacker* já era citada com o advento de crimes como invasão de sistema e furto de software, mas foi em 1980 que houve maior propagação dos diferentes tipos de crimes como a pirataria, pedofilia, invasão de sistemas, propagação de vírus, surgindo então com isso à necessidade de se despender maiores preocupações com a segurança virtual que exige uma atenção especial para identificação e punição dos responsáveis, que a essa altura estão em todos os lugares do mundo.[4]

---

[3] JESUS, Damásio Evangelista de. **Manual de Crimes Informáticos.** 1ª ed. São Paulo: Saraiva, 2016, pg. 17.
[4] CARNEIRO, Adeneele Garcia. **Crimes Virtuais: elementos para uma reflexão sobre o problema na tipificação.** Disponível em: < http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529 > Acesso em: 18 nov. 2017.

No Brasil, foi com o aumento populacional da revolução tecnológica que se despertou uma maior preocupação com os crimes desta especialidade.

> O Brasil começou a se preocupar com esse assunto especialmente a partir das últimas décadas, com o aumento da popularização dessa inovação tecnológica, promulgando, na Constituição Federal de 1988, leis relativas à competência do Estado sobre questões de informática.[5]

É difícil assegurar quando necessariamente surgiram os crimes cibernéticos, mas sabemos que nos últimos anos os ataques a computadores ou por meio destes, tomaram uma proporção imensa. Diante do aumento da população informatizada torna-se mais difícil o combate a este tipo de criminalidade.

3. DOS CRIMES CIBERNÉTICOS: CONCEITO E CLASSIFICAÇÃO

Nos dias atuais, a ciência da informática desenvolveu grandes instrumentos para os mais variados meios de comunicação. Diante dessa diversidade tecnológica, nos tornamos uma sociedade comunicativa sem saber sequer como é feita esta comunicação conforme aduz Damásio de Jesus: "Vivemos uma sociedade em que nos comunicamos muito, sem saber como tal comunicação é possível, como, quando e por onde. A dominância é flagrante, embora nem todos reconheçam. A informação é poder." [6]

Sabemos que, atualmente o homem e os sistemas informatizados estão demasiadamente ligados, podendo-se dizer que é quase impossível um retrocesso à sociedade totalmente desvinculada dos meios tecnológicos.

Ocorre que, esse desenvolvimento tecnológico proporcionou avanços positivos. Também propiciou a utilização deste para a prática de diversos delitos, por ser um espaço público, universal e amplo. "A internet é uma grande praça pública, o maior espaço coletivo do planeta". [7]

Os crimes executados por meio da web receberam inúmeras denominações e, apesar de não haver uma definição própria, conceitua Roque como sendo: "toda conduta, definida em

---

[5] CARNEIRO, Adeneele Garcia. **Crimes Virtuais: elementos para uma reflexão sobre o problema na tipificação.** Disponível em: < http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529 > Acesso em: 18 nov. 2017

[6] JESUS, Damásio Evangelista de. **Manual de Crimes Informáticos.** 1ª ed. São Paulo: Saraiva, 2016, p. 12.

[7] CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. 1ª ed. Rio de Janeiro: Brasport, 2014, p.3.

lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material". [8]

Foi em 1984, através do escritor americano William Gibson, autor do livro Neuromancer, que surgiu o termo "ciberespaço", tratando-se de um espaço virtual constituído por computadores utilizados por usuários ligados a web.

Na definição de Gibson:

> Uma alucinação consensual vivida diariamente por bilhões de operadores autorizados, em todas as nações, por crianças aprendendo altos conceitos matemáticos... Uma representação gráfica de dados abstraídos dos bancos de dados de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz abrangendo o não-espaço da mente; nebulosas e constelações infindáveis de dados. Como marés de luzes da cidade.[9]

É unanimidade entre doutrinadores que, para que este seja apontado como crime é necessário que tenha sido praticado por meio ou contra sistemas de informática.

Nesse sentido conceitua Cassanti:

> Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital.[10]

Na visão de Castro: "Crime de informática é aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através de computador." [11]

Este requisito engloba também, os delitos já existentes praticados através da internet, pois, para que se adentre à rede, é necessário a utilização de um computador, razão pela qual qualquer crime preexistente no Código Penal Brasileiro, realizado por meio dos sistemas de informática, considera-se um crime cibernético. "Inclui-se nesse conceito os delitos praticados através da internet, pois pressuposto para acessar a rede é a utilização de um computador." [12]

Assim, há uma necessidade de classificar os crimes cibernéticos, porém, existem diversas classificações doutrinárias relativas ao tema amplamente discutido.

---

[8] ROQUE, Sérgio Marcos. **Criminalidade Informática: crimes e criminosos do computador.** 1ª ed. São Paulo: ADPESP Cultural, 2007, p. 25.

[9] GIBSON, William. **Neuromancer**. São Paulo: Aleph, 2003, p. 67.

[10] CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. 1ª ed. Rio de Janeiro: Brasport, 2014, p.6.

[11] CASTRO, Carla Rodrigues Araújo. **Crimes de informática e seus aspectos processuais**. 2ª ed. Rio de Janeiro: Lumen Juris, 2001, p. 9.

[12] CASTRO, op. cit., p. 9.

Na visão de Damásio de Jesus: “os crimes de informática são classificados em: próprios, impróprios.” [13]

ALMEIDA e col. “classificam os crimes virtuais próprios como sendo aqueles dos quais o sujeito realiza a conduta criminosa, mediante o sistema de informática da vítima na qual o computador é utilizado como um meio para executar o delito.” [14] Neste caso, o objeto na qual se pretende atingir é o próprio computador, os dados e informações contidos nele ou seu sistema de informática.

Geralmente, estes crimes são cometidos por hackers, ou crackers conforme denomina a doutrina, no intuito de invadir um sistema de informática ou para modificar, alterar ou inserir dados falsos, pois estes contêm um amplo conhecimento informático.[15]

Com relação aos crimes virtuais impróprios, conceitua Damásio de Jesus: “crimes informáticos impróprios: em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro.” [16] Neste caso, utiliza-se o computador para a execução dos crimes já previstos pela legislação brasileira.

Distingue-se tal classificação, pela não essencialidade do computador para a realização do crime, podendo este se dar de várias formas além do sistema informático.

4. DA EVOLUÇÃO LEGISLATIVA À LEI 12.737/2012 - “CAROLINA DIECKMANN”

Sempre foi desafiante discutir sobre crimes cibernéticos diante do Código Penal Brasileiro, pois, mesmo que este abrange grande parte dos crimes cibernéticos, é omisso em conteúdos onde o sistema informático teria de ser o bem protegido pelo Código Penal. Todavia, com o desenvolvimento da tecnologia, criou-se uma sociedade denominada “da informação”, imensamente submetido à informática, o que fez com que o direito passasse a reconhecer outros valores pertinentes. Foi então, que se deu inicio a uma discussão sobre

[13]JESUS, Damásio Evangelista de. **Manual de Crimes Informáticos.** 1ª ed. São Paulo: Saraiva, 2016, p. 48.
[14] ALMEIDA; MENDONÇA; CARMO; SANTOS; SILVA; AZEVEDO. **Crimes Cibernéticos**. 2015. Disponível em: <https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217> Acesso em: 08 set. 2017.
[15] SCHMIDT, Guilherme. **Crimes Cibernéticos**. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos> Acesso em: 18 nov. 2017.
[16] JESUS, op. cit., p. 49.

normas protetoras dos direitos dos indivíduos frente às novas tecnologias, bem como do uso mal-intencionado destas.[17]

Anterior à lei 12.737/2012, o legislador brasileiro, caminhava a um longo tempo, no sentido de que é mais adequado as alterações ao Código penal e Código de Processo Penal ao invés deformação de leis próprias. Tudo que o Brasil tinha em termos legislativos, com relação a crimes virtuais, era o Projeto de Lei n° 933/99, que criou a Lei n° 9.983 de 14 de julho de 2000. A princípio, esta lei nasceu para proteger os sistemas de previdência social, mas consecutivamente englobou toda a administração pública, modificando o Código Penal para prever disposições enquadrando informática.

Dentre os vários outros projetos de lei que tramitaram no Congresso, ressalta-se o Projeto de Lei n. 84/99, apresentado em 24 de fevereiro de 1999. Tal projeto, tramitou no Congresso por cerca de 13 (treze) anos. Consta na justificativa do Projeto que não se poderia permitir que pela falta de lei, que institua exclusivamente os crimes cibernéticos, que alguns indivíduos pudessem continuar usando computadores e suas redes para a criminalidade, razão em que se justificava a necessidade de uma legislação que elucidava os crimes praticados nas redes de informática e suas respectivas penas. Este Projeto converteu-se então na Lei n° 12.735/2012, contendo apenas 04 (quatro) artigos na qual 02 (dois) destes foram vetados pela então presidente da república Dilma Rousseff.

A lei 12.735/2012 prevê então a tipificação de condutas realizadas por meio dos sistemas eletrônicos, digitais ou similares, cometidos contra os sistemas de informática. Além disso, dispõe que deverão os órgãos da policia judiciária estruturar setores e equipes especializadas para o combate a infrações na rede de informática e dispositivos de comunicações, conforme regulamento.

Como já mencionado, não foi nada fácil aprovar uma legislação que tipificasse os crimes cibernéticos, todavia, mesmo que talvez não resolvesse o obstáculo da falta de estrutura investigativa, foram elaboradas novas figuras delitivas no Código Penal. Para isso, infelizmente, foi necessário que uma atriz popular, pessoa pública, fosse vítima de um delito praticado por meio da rede de informática para que o legislativo concluísse uma discussão repercutida por anos no Congresso Nacional, para enfim ser aprovada a Lei n° 12.737/2012.

Em maio de 2012 diversas fotos íntimas da atriz Carolina Dieckmann foram divulgadas na internet. A princípio a suspeita principal era de que os invasores seriam possivelmente funcionários de uma loja de assistência técnica na qual a atriz teria deixado seu

---

[17] JESUS, Damásio Evangelista de. **Manual de Crimes Informáticos.** 1ª ed. São Paulo: Saraiva, 2016.

computador para concerto. Todavia, segundo as investigações da Delegacia de Repressão aos Crimes de Informática (DRCI) da Polícia Civil do Rio de Janeiro, o crime foi iniciado por crackers do interior de Minas Gerais e de São Paulo, que enviaram um spam para a atriz Carolina Dieckmann servindo-lhe como isca, que ao ser aberto liberou uma porta de acesso para a invasão dos criminosos ao computador, e desta forma terem alcance aos arquivos contendo as imagens. [18]

O caso repercutiu até o Congresso Nacional de modo que levou a Câmara dos Deputados a aprovar o projeto de lei que tipifica os crimes de informática, prevendo punições para os delitos como violação de senha, invasão de computadores e de outros dispositivos de informática.

Diante disso, no dia 3 de dezembro 2012, foi publicada no Diário Oficial da União a Lei 12.737/2012 popularmente conhecida como "Lei Carolina Dieckmann", que só entrou em vigor no de 02 de abril de 2013. Desta forma a lei tipificou como crime, ações como esta sofrida pela atriz. Interessante ressaltar, que a referida lei transitou pela Câmara desde o ano de 1999, porém, somente foi sancionada após grande comoção do caso da atriz Carolina Dieckmann.

Sobre isso aduz Masson:

> Como de praxe, os debates sobre uma legislação específica para os crimes ligados à *internet* (**crimes cibernéticos**) se arrastavam há anos, em velocidade de conexão discada. Mas a atividade dos congressistas, impulsionada pela opinião pública, recebeu imenso *upload* depois da invasão do computador pessoal de Carolina Dieckmann. [19]

A referida lei então auxilia pessoas que tem sua vida privada invadida, e foi criada para discernir a verdadeira função da tecnologia dos sistemas informáticos de um recurso para se cometer de crimes.

5. DAS INCLUSÕESE ACRÉSCIMOS NO CÓDIGO PENAL

Veremos as introduções e acréscimos a seguir, no código penal a partir da lei 12.737/2012:

---

[18] FALCÃO, Juliana. **Fim do Caso: Carolina Dieckmann.** Disponível em: <http://vilamulher.uol.com.br/famosos/mundo-da-fama/fim-do-caso-carolina-dieckmann-elogia-agilidade-da-policia-6-1-80-1646.html>Acesso em: 08 set. 2017.

[19] MASSON, Cleber. **Código Penal comentado**. 5ª ed. São Paulo: Método, 2017, p. 671.

> 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: Vigência 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: Vigência 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.[20]

A consumação deste delito, conclui-se simplesmente com o ato de invadir um dispositivo informático alheio, independentemente se este esta ou não conectado à rede de computadores, mediante violação indevida de mecanismo de segurança, tendo como finalidade obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do proprietário do dispositivo informático, ou instalar vulnerabilidade para obter vantagens ilícitas, mesmo que este objetivo não seja efetivamente alcançado.[21]

Antes mesmo da inclusão do artigo 154-A no Código Penal, já se discutia entre os doutrinadores brasileiros, qual o bem jurídico que se tornaria protegido. A princípio, entendia-se que os crimes cibernéticos, ainda não tipificados, tratavam de conteúdo patrimonial. Todavia, com a publicação da lei 12.737/12, a doutrina majoritária entende que artigo 154-A protege a privacidade em sentido irrestrito, na qual a intimidade é sua espécie. A maior argumentação diz respeito à localização topográfica do crime no código penal, portanto, trata-se de crimes contra a pessoa, exclusivamente contra o seu direito a liberdade, no sentido de privacidade.

Na visão de Nucci:

> A nova figura típica de invasão de dispositivos informáticos, insere-se no contexto de crimes contra a liberdade individual, sendo este o bem jurídico mediato tutelado. No entanto, de forma imediata, ingressou-se no campo dos crimes contra a

---

[20] 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: 08 set. 2017.

[21] MASSON, Cleber. **Código Penal comentado**. 5ª ed. São Paulo: Método, 2017.

> inviolabilidade dos segredos, com proteção acerca da intimidade, da vida privada, da honra, da inviolabilidade de comunicação e correspondência, enfim, da livre manifestação do pensamento, sem nenhuma intromissão de um terceiro.[22]

Desta forma, conclui-se que o bem jurídico tutelado são os interesses pessoais, e não a rede de computadores como é de se imaginar.

Por meio da internet, a comunicação social, tornou-se mais simples e de fácil acesso, razão pela qual, criou-se a figura típica incriminadora no intuito de punir quem viole não apenas da comunicação telemática como também aos dispositivos informáticos, que mantém dados pertinentes do seu proprietário.

Já o novo artigo 154-B, no mesmo diploma, fala da ação penal:

> Art. 154-B - Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime e 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.[23]

Portanto, trata-se de crime que se apura mediante ação penal pública condicionada à representação, pois, é necessária a autorização da vítima para a propositura da ação penal pelo Ministério Público. Contudo, nos crimes cibernéticos cometido contra a Administração Pública, direta ou indireta, a ação é incondicionada.

O atual artigo 266 do *codex* citado anteriormente, diz:

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa. Parágrafo único - Aplicam-se as penas em dobro, se o crime é cometido por ocasião de calamidade pública. § 1° Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. § 2°Aplicam-se as penas em dobro se o crime e cometido por ocasião de calamidade pública. [24]

“Este delito consuma-se com a prática da conduta criminosa, pouco importando se este causou dano aos serviços telégrafos, radiotelegráfico ou telefônico.” [25]

É importante esclarecer que, aqui não se trata de invasão de sistemas ou dispositivos informáticos, mas de evidente invalidação pela sobrecarga.

---

[22] NUCCI, Guilherme de Souza. **Código Penal Comentado**. 14ª ed. Rio de Janeiro: Forense, 2014, p. 811.
[23] 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: 08 set. 2017.
[24] 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: 08 set. 2017.
[25] MASSON, Cleber. **Código Penal comentado**. 5ªed. São Paulo: Método, 2017, p. 1003.

Antes este artigo não era expresso ao tratar da probabilidade de sistemas informáticos serem objeto do ataque envolvendo a interrupção, todavia, a lei 12.737/12 supriu a brecha, e completou o dispositivo.

Segundo Túlio Vianna e Machado:

> Trata-se de crime contra a incolumidade pública, o que pode ser facilmente constatado até mesmo por sua localização no Título VIII do CPB. Esse crime, portanto, abarca tão somente condutas que atingem um número indeterminado de pessoas e nunca uma vítima ou grupo de vítimas determinado.[26]

Destaca-se que, a lei só resguarda o serviço telemático ou de informação que seja de utilidade púbica, um critério atualmente difícil de definir e que deve ser apreciado pelo magistrado em cada caso.

São considerados serviços de utilidade pública para Nucci:

> Serviços de utilidade pública são aqueles que objetivam facilitar a vida do indivíduo na sociedade, colocando à disposição deste utilidades que lhe proporcionarão mais conforto e bem-estar. Ao contrário de serviços públicos, que visam manter necessidades gerais e essenciais da sociedade para que elas possam se desenvolver, os serviços de utilidade pública atendem às conveniências de membros da sociedade individualmente considerados.[27]

Desta forma, se a lei protege os serviços de utilidade pública não essencial, mas que proporciona benefícios a determinados cidadãos, entende-se que serviços públicos informáticos também é o objeto jurídico da legislação.

Importante frisar ainda que, a pena do delito em questão, será majorada em dobro, quando o delito se der por ocasião de calamidade pública.

Por fim, o artigo 298 do código penal, ainda estabelece:

> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena - reclusão, de um a cinco anos, e multa. Falsificação de cartão. Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.[28]

O Código Penal brasileiro, em seu artigo 298, já previa a falsificação de documento particular ou alteração de documento particular. O que a lei 12.737/12 alterou, foi a inclusão de um parágrafo onde equipara o cartão de crédito e débito ao documento particular.

---

[26] VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos Conforme a Lei 12.737/2012.** 1ª ed. Belo Horizonte: Fórum, 2013, p. 14.

[27] NUCCI, Guilherme de Souza. **Código Penal Comentado**. 14ª Ed. Rio de Janeiro: Forense, 2014, p. 100.

[28] 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: 08 set. 2017.

Para Jesus: “O escopo do legislador foi fazer frente às fraudes bancárias envolvendo clonagem de cartões. Porém, o artigo não se aplica às fraudes financeiras praticadas pela internet.” [29]

Estando as Leis n° 12.735/2012 e 12.737/2012, vigorando desde abril de 2013, podemos dizer que o Brasil já conta com leis específicas de crimes cibernéticos e que mesmo que modestas, contendo uma apenas um comando e outra um novo tipo penal, auxiliam na luta contra os crimes da nova era virtual.

Necessário destacar que, para a doutrina brasileira, qualquer pessoa pode ser parte de um crime virtual.

O sujeito ativo não necessita de nenhuma qualidade específica, razão pela qual é indiferente se este é um técnico em informática ou um aventureiro na área.

Já o sujeito passivo, destaca-se que seja um dispositivo informático de outra pessoa, tanto a título de propriedade quanto posse.

Observa-se que “Tratando-se de mera detenção (ex.: Fulano entrega o notebook a Beltrano para que este o leve ao conserto, momento em que ocorre a violação), o sujeito passivo é o proprietário ou o possuidor e não o detentor.” [30]

6. PECULIARIDADES DOS CRIMES CIBERNÉTICOS

Para grande parte da doutrina nacional, a maioria dos crimes consumados na rede de computadores recai, da mesma maneira, no mundo concreto.

Neste sentido, aduz Pinheiro:

> A Internet surge apenas como um facilitador, principalmente pelo anonimato que proporciona. Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital. As principais inovações jurídicas trazidas no âmbito digital se referem à territorialidade e à investigação probatória, bem como às necessidades de tipificação penal de algumas modalidades que, em razão de suas peculiaridades, merecem ter um tipo penal próprio.[31]

---

[29] JESUS, Damásio Evangelista de. **Manual de Crimes Informáticos.** 1ª ed. São Paulo: Saraiva, 2016, p. 106.
[30] NUCCI, Guilherme de Souza. **Código Penal Comentado**. 14ª Ed. Rio de Janeiro: Forense, 2014, p. 813.
[31] PINHEIRO, Patrícia Peck. **Direito digital.** 4ª ed. São Paulo: Saraiva, 2010.

Assim sendo, diante da ausência de uma legislação que trata estritamente de um crime cibernético, quem o cometeu, terá de ser julgado dentro do próprio do Código Penal, mantendo-se, entretanto, as devidas divergências.

No Brasil, a legislação pertinente que regula os crimes virtuais, encontra-se um tanto ultrapassada, pois, não foi capaz de acompanhar de forma proporcional a evolução da execução do delito. Mediante a isso, são vários os crimes virtuais sem lei especifica, mas que podem ser julgados por leis nacionais preexistentes.

O difícil enquadramento de alguns crimes cibernéticos, deriva do fato de serem condutas que tem por finalidade a violação da própria rede de informática como bem jurídico independente, não existindo uma proteção especifica ao caso.

Não podemos dizer que as Leis 12.737/12 e 12.735/12 são suficientes para solucionar todos os problemas relacionados aos crimes cibernéticos no Brasil, pois, este envolve não somente leis criminais, mas sim educação digital, políticas criminais e estrutura investigativa.

Diante disso, o ultimo avanço legislativo que tivemos com relação aos crimes cibernéticos, foi a Lei 12.965/2014, denominada como “Marco Civil da Internet”.

Esta lei surgiu no intuito de oferecer mais segurança jurídica para os usuários da web como os internautas, provedores, empresas e administração pública, e tem o escopo de evitar decisões contraditórias proferidas pelo Judiciário, em casos semelhantes envolvendo tecnologia da informação.

Talvez, ainda não seja o suficiente, porém, é um avanço considerável.

O Marco Civil da Internet é o responsável por estipular os princípios e garantias normativas da relação civil virtual na rede de computadores. Tem como objetivo, prever condutas criminosas nos sistemas de informática, bem como prezar pelos ideais da imparcialidade da rede, da privacidade dos usuários, da liberdade de se expressar e dos direitos humanos.

Desta forma expõe o artigo 3° da Lei 12.965/2014:

> Art. 3o A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede; VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio

> relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.[32]

Um dos pontos mais discutíveis da lei refere-se sobre a neutralidade da rede, que se constitui na "democratização" da velocidade e qualidade ao acesso à internet, sem distinção de conteúdos disponíveis no ramo da internet, desta forma assegura a neutralidade, que os provedores não constituem o poder de interferência na velocidade ou acesso a qualquer serviço de internet, havendo raras exceções apenas de caráter técnicos, como de exemplo:

> O texto do Marco Civil diz que as empresas só podem dar preferência a certos tipos de dados em suas redes se, e somente se, "decorrer de requisitos técnicos indispensáveis à fruição adequada dos serviços e aplicações", de outra forma, não[33].

Em relação aos princípios auferidos pela lei, um destes é o princípio da liberdade de expressão, na qual o intuito é garantir a impossibilidade da censura diante dos sites e redes sociais que, por exemplo, ficam impossibilitados de excluírem um conteúdo realizado pelo usuário, sem que haja uma determinação judicial, ressalvados os conteúdos contendo atos sexuais explícitos e privados.

> Em se tratando de imagens, vídeos ou outros materiais que contenham cenas de nudez ou de atos sexuais de caráter privado, o provedor de aplicações de internet responderá subsidiariamente com o divulgador, quando, após notificação, deixar de tornar indisponível o acesso a esse conteúdo. Aqui a diferença é que não se requer ordem judicial para a solicitação da indisponibilidade do conteúdo, podendo ser feita pelo próprio interessado mediante notificação.[34]

Garante o Marco Civil da Internet, a privacidade dos usuários, impedindo que suas informações pessoais possam ser vendidas ou oferecidas para empresas terceiras sem a autorização do usuário, além de prever o sigilo das comunicações realizadas pelos usuários no sistema informático.

Diante disso, a ação das empresas que operam na web, passou a ter o dever de ser mais transparente, pois, a nova legislação objetiva proteger direitos dos usuários.

---

[32] BRASIL. Lei 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>Acesso em: 08 set. 2017.

[33] TEMPERINEE, Alessandro. **Marco Civil. Um resumo do que você precisa saber. Papo Universitário.** Disponível em:<https://papouniversitario.anhembi.br/2014/05/marco-civil-internet/> Acesso em: 02 nov. 2017.

[34] FILHO, Eduardo Tomasevicius. **Marco Civil da Internet**. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S010340142016000100269> Acesso em: 02 nov. 2017.

O texto da lei está longe de ser perfeito, pois ainda há um caminho longo a ser percorrido para findar os delitos cibernéticos, todavia, é nítido o avanço legislativo sobre o tema, pois este deve se adequar a realidade.

CONSIDERAÇÕES FINAIS

Esse trabalho buscou analisar pormenorizadamente os delitos cometidos no meio cibernético. Teve como objetivo específico, explorar o conceito e curiosidades diante dos crimes digitais, assim como, averiguar as medidas concebidas pela legislação brasileira no intuito de conter os crimes digitais.

Pudemos perceber então, que os crimes dessa natureza sobrevieram de longos tempos, percorreu as décadas, se atualizando conforme os avanços tecnológicos.

Hoje, diversas classes sociais estão conectadas à internet, muitas pessoas até dependem de um computador ou celular para manter sua renda, tudo se vincula à tecnologia desde a produção de alimentos, meios de comunicações até a energia elétrica.

Os crimes de informáticas são bem mais comuns do que se imagina, milhares de pessoas todos os dias são vítimas de algum delito, seja por meio de invasão aos dados pessoais ou até mesmo por meio das redes sociais onde se encontram milhares de pessoas conectadas.

Diante disso, a discussão do assunto em questão demonstrou-se de suma importância, por se tratar de um tema atual em que se busca um entendimento e uma definição sobre os diversos crimes abrangidos no mundo digital.

Ressalta-se que, apesar da legislação brasileira suprir algumas necessidades no direito nacional, ainda, há muitos lapsos a serem preenchidos, pois, as leis citadas neste trabalho não são totalmente eficiente, vez que o índice de criminalidade virtual ainda é crescente.

Desta forma, faz-se essencial a educação e conscientização da sociedade em respeitar os limites do mundo virtual, a intimidade, privacidade alheia para então se evitar os crimes cibernéticos.

Por fim, o objetivo principal deste artigo é mostrar a todos os operadores do direito, a importância de se atentarem aos crimes realizados por meio dos sistemas de informática, em especial na internet, e a necessidade do poder público providenciar ferramentas de maior rigidez na repressão de condutas ilícitas que venham a ocorrer no ambiente cibernético, pois, gradativamente a coletividade está se deslocando para uma sociedade cada vez mais virtual.

REFERÊNCIAS

ALMEIDA; MENDONÇA; CARMO; SANTOS; SILVA; AZEVEDO. **Crimes Cibernéticos**. 2015. Disponível em: <https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217> Acesso em: 08 set. 2017.

BRASIL. Lei 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 **- Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 08 set. 2017.

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: 08 set. 2017.

BRASIL. Lei 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>Acesso em: 08 set. 2017.

CARNEIRO, Adeneele Garcia. **Crimes Virtuais: elementos para uma reflexão sobre o problema na tipificação.** Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529> Acesso em: 18 nov. 2017.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. 1ª ed. Rio de Janeiro: Brasport, 2014.

CASTRO, Carla Rodrigues Araújo. **Crimes de informática e seus aspectos processuais**. 2ª ed. Rio de Janeiro: Lumen Juris, 2001.

FALCÃO, Juliana. **Fim do Caso: Carolina Dieckmann.** Disponível em: <http://vilamulher.uol.com.br/famosos/mundo-da-fama/fim-do-caso-carolina-dieckmann-elogia-agilidade-da-policia-6-1-80-1646.html>Acesso em: 08 set. 2017.

FILHO, Eduardo Tomasevicius. **Marco Civil da Internet**. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S010340142016000100269> Acesso em: 02 nov. 2017.

GIBSON, William. **Neuromancer**. São Paulo: Aleph, 2003.

JESUS, Damásio Evangelista de. **Manual de Crimes Informáticos**. 1ª ed. São Paulo: Saraiva, 2016.

MASSON, Cleber. **Código Penal comentado**. 5ª ed. São Paulo: Método, 2017.

NUCCI, Guilherme de Souza. **Código Penal Comentado**. 14ª ed. Rio de Janeiro: Forense, 2014.

PINHEIRO, Patrícia Peck. **Direito digital.** 4ª ed. São Paulo: Saraiva, 2010.

ROQUE, Sérgio Marcos. **Criminalidade Informática: crimes e criminosos do computador.** 1ª ed. São Paulo: ADPESP Cultural, 2007.

SCHMIDT, Guilherme. **Crimes Cibernéticos**. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos> Acesso em: 18 nov. 2017.

TEMPERINEE, Alessandro. **Marco Civil. Um resumo do que você precisa saber. Papo Universitário.** Disponível em:<https://papouniversitario.anhembi.br/2014/05/marco-civil-internet/> Acesso em: 02 nov. 2017.

VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos Conforme a Lei 12.737/2012.** 1ª ed. Belo Horizonte: Fórum, 2013.