CENTRO UNIVERSITÁRIO TABOSA DE ALMEIDA-ASCES UNITA

BACHARELADO EM DIREITO

JULYANN VINICIUS SILVA BRAGA

DIREITO PENAL E AS NOVAS TECNOLOGIAS: Uma análise da lei 12.737/12 que modificou o Código Penal brasileiro e seus problemas práticos.

CARUARU-PE

2018

JULYANN VINICIUS SILVA BRAGA

DIREITO PENAL E AS NOVAS TECNOLOGIAS: Uma análise da lei 12.737/12 que modificou o Código Penal brasileiro e seus problemas práticos.

Artigo científico apresentado ao Centro Universitário Tabosa de Almeida (ASCES-UNITA), como requisito para a conclusão do curso de Direito, com orientação do Professor Especialista Marupiraja Ribas.

CARUARU-PE

2018

BANCA EXAMINADORA

Aprovado em: ____/___/_____

_____

Presidente: Prof. Esp. Marupiraja Ramos Ribas

_____

Primeiro Avaliador: Prof.

_____

Segundo Avaliador: Prof.

RESUMO

Com a evolução da sociedade e da tecnologia, as informações passaram a ser obtidas com mais facilidade, sobretudo em relação as informações virtuais, com esse avanço também veio problemas, principalmente ligados ao Direito Penal com os chamados crimes cibernéticos. No nosso ordenamento jurídico não existia previsão legal para esses crimes até o ano de 2012, e as vítimas podiam ingressar apenas na área cível e o agente que cometeu o crime sofria apenas punições pecuniárias e ficavam impunes da reprimenda penal. Depois de um ato de grande repercussão na mídia envolvendo fotos íntimas da atriz Carolina Dieckmann foi dada celeridade para aprovação do projeto de lei (PLC 35/2012) que já tramitava no congresso nacional e a partir disso foram criadas tipificações para os crimes cometidos por meio eletrônico. O trabalho científico utilizou do método de pesquisa quantitativo, demonstrando em números e estatísticas o crescimento do crime virtual. O resultado objetivado pelo presente artigo é demonstrar que a lei 12.737/12 veio com o propósito de preencher a lacuna que existia no nosso ordenamento jurídico, mas devido a pressão para sua aprovação, ela não identificou os meios para garantir sua eficácia plena. As penas previstas na lei provocaram baixa reprimenda penal, fazendo com que a lei não alcance seu caráter preventivo, pois na maioria das vezes os acusados são beneficiados pela suspensão condicional do processo e não chegam a cumprir a pena.

Palavras-chave: Evolução da sociedade e da tecnologia; crimes cibernéticos; baixa reprimenda penal.

ABSTRACT

With the evolution of society and technology, information was more easily obtained, especially in relation to virtual information, with this advance also came problems, mainly linked to criminal law with so-called cyber crimes. In our legal system there was no legal provision for such crimes until the year 2012, and the victims could only enter the civil area and the agent who committed the crime suffered only pecuniary punishment and remained unpunished for criminal reprimand. After an act of great repercussion in the media involving intimate photos of the actress Carolina Dieckmann, speed was approved for the approval of the bill (PLC 35/2012) that was already processed in the national congress and from this, typifications were created for crimes committed through electronic. The scientific work used the method of quantitative research, demonstrating in numbers and statistics the growth of virtual crime. The aim of this article is to demonstrate that Law 12.737 / 12 came to fill the gap that existed in our legal system, but due to pressure for its approval, it did not identify the means to guarantee its full effectiveness. The penalties foreseen in the law caused a low penal reprimand, making the law not reach its preventive character, because most of the times the accused are benefited by the conditional suspension of the process and do not get to fulfill the sentence.

Keywords: Evolution of society and technology; cyber crimes; low criminal reprimand.

SUMÁRIO

INTRODUÇÃO

O presente artigo científico se propõe discutir como o direito penal, deve se adaptar ao uso das novas tecnologias, notoriamente em relação aos crimes cibernéticos.

O tema foi estabelecido a partir da evolução em que a tecnologia informática vem crescendo e como ela modificou a aplicação do Direito, especificamente na seara penal, que careceu de uma mudança na legislação para abranger esses crimes.

Com o avanço da sociedade no que se refere a respeito dos meios tecnológicos sobretudo aqueles relacionados ao mundo digital e divulgação de informações, foi possível notar a ausência de previsão legal para ações praticadas no ambiente virtual.

O artigo científico tem como objetivo detectar as mudanças introduzidas no Código Penal brasileiro no capítulo VI, que trata dos crimes contra a inviolabilidade dos segredos e a sua aplicação prática relacionando com a eficácia e o efeito preventivo causado pela norma penal.

A primeira parte demonstra o surgimento das tecnologias, e sua importância para a sociedade, como um meio facilitador de interação social e faz a ligação de como o Direito Penal está se adaptando a essas novas tecnologias.

A segunda parte do trabalho vem analisar o conceito de crime disposto no nosso sistema jurídico, expondo todas as teorias definidoras do que é crime para nosso sistema penal

Contextualizando o conceito de crime cibernético e suas peculiaridades, que o torna um crime bastante complexo devido o conhecimento técnico que é exigido do sujeito ativo.

Na ultima parte do trabalho a lei 12.737/12 é analisada, exemplificando todas as suas elementares para tipificação do crime, sobre o sujeito ativo e passivo da conduta e sobre quais bens jurídicos a lei pretende proteger, e a problemática do trabalho.

Identificando os erros contidos no texto legal que proporciona ao agente infrator meios de cometer a conduta a criminosa e não ser punido pelo nosso

sistema penal, e fazendo uma relação com o despreparo da polícia investigativa em solucionar os crimes.

1 **DIREITO PENAL E AS NOVAS TECNOLOGIAS**

O Direito Penal é uma ciência jurídica que sofre bastante influência da sociedade, por ser o principal ramo capaz de retirar um direito fundamental do indivíduo que é o direito à liberdade. Conforme o Art. 5 da Constituição Federal de 1988[1] :

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade...

Com o avanço da humanidade novas tecnologias da informação foram criadas, entre elas é considerada uma das mais importantes a criação dos computadores e da rede de informação conhecida por internet.

O surgimento dos computadores se deu em meados da década de 30 nas regiões do Atlântico médio nos Estados Unidos, localizado entre a nova Inglaterra e os estados do Atlântico Sul, essa região compreende as cidades de Nova York, Nova Jersey e Pennsylvania, formando o primeiro núcleo e mais importante na produção de computadores nos EUA (Estados Unidos da América). Trata sobre esse aspecto o Professor Doutor Hindenburgo F. Pires :

> O surgimento do primeiro computador eletrônico digital da chamada Primeira Geração Tecnológica foi concebido em 1939 por John Vincent Atanasoff, professor de física, e Clifford Berry, seu assistente, ambos do *Iowa College*, que o chamaram de *Atanasoff-Berry Computer* ou *ABC*. Este computador foi desenhado para solucionar equações algébricas lineares [2]

Os primeiros computadores foram desenvolvidos para uso militar e coleta de dados por parte do governo dos EUA e de algumas empresas como a ATeT-Bell, contudo foi durante o período da guerra fria que a produção teve uma ênfase maior, pois foi criada uma região específica para a produção das maquinas.

---

[1] BRASIL. Constituição da República Federativa do Brasil de 1988.
[2] PIRES, Hindenburgo Francisco. **O Surgimento dos Primeiros Computadores**. Disponível em: www.educacaopublica.rj.gov.br . Acesso em: 10/09/17.

Com a criação dessa área voltada para o desenvolvimento tecnológico, chamada de Vale do Silício, houveram grandes investimentos públicos e de empreendedores individuais.

Entretanto, somente 30 anos depois com o surgimento de novas tecnologias foi possível a comercialização em massa dos computadores, através da redução dos custos de produção e do processo de miniaturização dos equipamentos, com isso o poder de processamento conseguiu aumentar de forma considerável usando um espaço ínfimo em relação a primeira geração, dando início à criação dos computadores pessoais na década de 70.

Com a criação dos computadores era preciso um meio de conectar todos entre si para enviar e receber dados, dessa forma por meio de um projeto de pesquisa militar do governo dos EUA denominado de ARPA (Advanced Research Projects Agency), foi criada a internet com o objetivo inicial de conectar todos os centros universitários de pesquisa com o Departamento de Defesa do país conhecido como O Pentágono, para a troca rápida e segura de informações.

A primeira comunicação feita por meio da internet se deu nos anos 70, quando os computadores já estavam com o poder de processamento mais avançado, a ferramenta usada foi o E-mail que possibilitou a troca de dados dentro das universidades.

Todavia, a linguagem utilizada para a comunicação em rede era bastante complicada, por isso a utilização em grande escala da internet se deu apenas nos anos 80, com o surgimento dos primeiros servidores de internet.

Com o surgimento dessas tecnologias que interferiram de forma significativa no cotidiano, várias condutas praticadas por meio dessas inovações merecem a tutela do Direito, principalmente no âmbito penal. Como está relatado nos noticiários:

> O Brasil ocupa lugar de destaque no cenário global de cibercrimes. Em 2016, 42,4 milhões de brasileiros foram vítimas de crimes virtuais. Em comparação com 2015, houve um aumento de 10% no número de ataques digitais. Segundo dados da Norton, provedora global de soluções de segurança cibernética, o prejuízo total da prática para o país foi de US$ 10,3 bilhões. Em maio de 2012, o Brasil acompanhou um dos casos mais emblemáticos de crime cibernético cometidos no país: o roubo e a divulgação de mais de 30 fotos íntimas da atriz Carolina Dieckmann. Hackers do interior de Minas Gerais e de São Paulo invadiram o e-mail da artista e a chantagearam, por meio de mensagens anônimas, pedindo R$ 10 mil para apagar

> as imagens. O caso foi parar no Congresso Nacional: a Câmara dos Deputados aprovou e colocou em vigor a Lei nº 12.737 apelidada de Lei Carolina Dieckmann, que tipifica delitos cometidos em meios eletrônicos e na internet.[3]

Por meio de alterações legislativas a seara criminal vem se atualizando na questão de crimes cometidos com intermédio dessas tecnologias, tanto na fase inquisitorial (Inquérito Policial), com servidores especializados na área e na fase processual com leis que permitem a punição de indivíduos que cometem os chamados crimes cibernéticos.

2 CONTEXTUALIZAÇÃO DOS CRIMES CIBERNÉTICOS

Correspondente ao avanço da internet, surgiu várias condutas criminosas praticadas por meio virtual. Essas ações são denominadas de crimes cibernéticos, que são realizados por pessoas com conhecimento específico em sistemas e meios informatizados no vasto campo titulado de ciberespaço.

2.1 Conceito de crime

A nossa legislação vigente não traz de forma expressa o conceito de crime, essa definição é cedida pela doutrina criminal. Existem 3 conceitos que determinam o que é crime, cada um utilizando de forma diversa os elementos do ato ilícito. O primeiro conceito de crime adotado para o estudo é o conceito formal de crime, ele define o crime como qualquer violação da lei penal, uma conduta diversa ao ordenamento jurídico, que merece uma atribuição de pena ao agente que praticou. Como leciona o grande doutrinador, Fernando Capez:

> O conceito de crime resulta da mera subsunção da conduta ao tipo legal e, portanto, considera-se infração penal tudo aquilo que o legislador descrever como tal, pouco importando o seu conteúdo. Considerar a existência de um crime sem levar em conta sua essência ou lesividade material afronta o princípio constitucional da dignidade humana.[4]

O segundo conceito exposto pela doutrina é chamado de material, essa definição de crime é considerada de forma aberta, pois permite ao legislador

---

[3] DINO, Divulgador de Notícias. Crimes Virtuais afetam 42 milhões de brasileiros. Disponível em: www.economia.estadao.com.br. Acesso em 10/09/17

[4] Capez, Fernando. Curso de Direito Penal Parte Geral. 15.ed. São Paulo: Saraiva, 2011.p 134

definir qual o tipo de conduta e bem juridicamente tutelado, que podem sofrer a reprimenda penal. Apresenta o Doutor Rogério Greco em sua obra:

> O conceito material sobreleva a importância do princípio da intervenção mínima quando aduz que, somente haverá crime quando a conduta do agente atentar contra os bens mais importantes. Contudo, mesmo sendo importante e necessário o bem para a manutenção e a subsistência da sociedade, se não houver uma lei penal protegendo-o por mais relevante que seja, não haverá crime se o agente vier a atacá-lo, em face ao princípio da legalidade.[5]

O último conceito de crime e o adotado no nosso sistema jurídico criminal é o analítico, esse conceito é dividido em duas correntes, a corrente bipartida e tripartida. A corrente bipartida entende que o crime é composto por dois elementos, o fato típico e antijurídico e culpabilidade é usada apenas na dosimetria da pena. Já para a corrente tripartida o crime é formado pelo, fato típico, antijurídico e a culpabilidade.

Essas duas correntes dão origem a duas teorias, são elas: teoria causalista e a finalista. A primeira defende que a conduta é algo casual e não estuda a vontade do agente em praticar a conduta criminosa, já a segunda teoria estuda o comportamento humano de quem praticou o ato ilícito, afastando o dolo e a culpa que integrava a culpabilidade, para uma análise no tipo penal. Segue esse entendimento o professor Rogério Greco: “Estamos com a maioria da doutrina, nacional e estrangeira, que adota a divisão tripartida do conceito analítico, incluindo a culpabilidade como um de seus elementos característicos”.[6]

Portanto, o crime no nosso ordenamento jurídico é considerado pela doutrina majoritária composto pelos 3 elementos supracitados, e na falta de um desses requisitos a conduta não será considerada como um ilícito penal, porém há grandes divergências entre os doutrinadores em casos específicos sobre qual teoria deve ser adotada.

2.2 Histórico e Conceito dos crimes cibernéticos

[5] Greco, Rogério. **Curso de Direito Penal** Parte Geral.11. ed. Rio de Janeiro: Impetus, 2009.p 143

[6] Greco, Rogério. **Curso de Direito Penal** Parte Geral.11. ed. Rio de Janeiro: Impetus, 2009.p 147

O crime cibernético teve seu surgimento na década de 60, com as primeiras invasões e sabotagem de sistemas informatizados. Com a expansão da tecnologia nos anos 80, a preocupação com os crimes virtuais já chamava atenção da sociedade e da segurança nacional dos (EUA), devido ao aumento de crimes como: pirataria e invasão de sistemas utilizando malwares.

No nosso país os ataques cibernéticos surgiram no ano de 1996, quando houve uma invasão ao site da universidade federal do Ceará, porém os danos causados pelos crimes virtuais são enormes, em 2002 segundo uma pesquisa da empresa britânica (mi2g) o Brasil liderou o ranking mundial de cibercrimes:

> Outro recorde alcançado pelos piratas do Brasil foi o número de grupos de hackers na lista TOP 10, dos "dez mais ativos". O Brasil ocupa todas as posições –sim, os dez grupos hackers que mais atuaram durante o mês de novembro de 2002 são brasileiros. Desses, os cinco mais ativos são BYS (Breaking Your Security), Ir4dex, Endiabrad0s, Virtual Hell e rya (Rooting Your Admin).[7]

O crime virtual é conceituado como o ato ilícito praticado pelo agente infrator, utilizando-se o computador como meio para a prática criminosa. Se posiciona nesse sentido o professor Manuel Lopes Rocha:

> A criminalidade informática, como aqueles que tem por instrumento ou por objeto sistema de processamento eletrônico de dados, apresentando-se em múltiplas modalidades de execução e de lesão de bens jurídicos.[8]

Por esse motivo, o crime cibernético pode ser caracterizado como um ilícito que requer para a configuração do tipo penal, uma característica especial do agente infrator devido o meio que é utilizado para cometer o crime, que exige um certo conhecimento técnico do sujeito ativo da conduta.

2.3 Classificação dos crimes cibernéticos

---

[7] Ângelo, **Brasil lidera ranking mundial de hackers e crimes virtuais**. Folha de S.Paulo. Disponível em: http://www1.folha.uol.com.br/folha/informatica/ult124u11609.shtml. Acesso em: 12/11/2017

[8] Rocha, **Crimes Virtuais**. Agente Criminoso Virtual. Disponível em: http://blogcrimesvirtuais.blogspot.com.br/p/agente-criminoso-virtual.html. Acesso em: 10/11/2017

Os crimes virtuais podem ser classificados de dois tipos diferentes, a depender do objetivo da conduta do criminoso, são eles: os crimes cibernéticos próprios e impróprios.

Crimes virtuais próprios ou puros são aqueles em que o agente que pratica a conduta, utiliza o computador como meio para o crime contra outro computador ou equipamento periférico, por exemplo, os crimes tipificados nos artigos 154-A e 313-A da lei 12.737/12, que falam sobre a invasão de dispositivo informático e a inserção de dados falsos em sistema de informação. Nessa modalidade é elemento essencial do crime, o uso do computador ou equipamentos equivalentes, nesses delitos o legislador buscou proteger a inviolabilidade da informação automatizada.

Crimes cibernéticos impróprios são aqueles que sua prática também é realizada por meio de um equipamento virtual, mas sua destinação não é atingir outro componente eletrônico, exemplo desses crimes são os delitos contidos no capítulo V do Código Penal brasileiro, como a injúria e a difamação.

Discorre sobre essa classificação o Doutor Rogério Greco:

> Há, assim, crimes cometidos com o computador (The computer as a tool of a crime) e os cometidos contra o computador, isto é, contra as informações e programas nele contidos (The computer as the object of a crime).[9]

Portanto para a caracterização do crime é preciso saber qual a finalidade da conduta do agente que praticou o crime, qual foi o meio usado, em razão de existir crimes que necessitam de forma obrigatória o uso do computador, como é o caso dos crimes próprios. Já de outro lado nos crimes impróprios o equipamento informático não é essencial para a configuração do tipo penal, pois pode ser realizado sem o uso deste.

2.4 Sujeitos dos crimes cibernéticos

Existem vários tipos de sujeito ativo nos crimes virtuais e uma certa complexidade na sua identificação, por tanto para efeitos de estudo é importante fazer a classificação dos vários grupos que praticam o crime cibernético. O professor e especialista em crimes virtuais Alexandre Jean Aaoum, define cada

[9] Greco, Comentário sobre o crime de invasão de dispositivo informático -Art.154-A do Código Penal. Rogério Greco. Disponível em: http://www.rogeriogreco.com.br/?p=2183. Acesso em: 10/11/2017

tipo de sujeito ativo nos cibercrimes: “Hacker é a pessoa que tem grande capacidade técnica sobre os sistemas de informática e redes em geral, e usa desse conhecimento pata ter acesso a sistemas e redes privadas”.[10]

Por ser a figura mais conhecida na sociedade em geral, o hacker sempre é visto como um criminoso, porém na maioria das vezes ele atua como um pesquisador, que encontra a falha no sistema e relata aos seus desenvolvedores.

Cracker é uma das várias espécies do gênero hacker, eles possuem a mesma habilidade do hacker, porém usam de forma criminosa descobrindo a falha no sistema e roubando informações, com a instalação de programas piratas que retiram a proteção do equipamento.

Phreakers é outro tipo de hacker com finalidade diversa dos anteriores, tiveram seu surgimento nos anos 90 com o objetivo de burlar sistemas telefônicos para realizar chamadas grátis e se atualizaram com o tempo, hoje são responsáveis pela invasão de smartphones para obter informações por meio de interceptações telefônicas ou qualquer dado enviado pelo equipamento eletrônico.

Lammers são as pessoas que não possuem técnicas avançadas, usam seu conhecimento básico para praticar pequenas invasões, como: exclusão de páginas das redes sociais, são considerados hackers ineptos.

Defacer é uma das espécies mais conhecida atualmente, são responsáveis por mudanças nos designers das paginas de um sitio na internet, atuam apagando as informações da página e expondo seu crime por meio de mensagens.

Consequentemente, podemos definir que hacker não é necessariamente aquela pessoa que invade sistemas para praticar condutas ilícitas, e sim entender a palavra hacker como um gênero que contém várias espécies, alguns usam o conhecimento de forma positiva e outros de forma negativa.

Em relação ao sujeito passivo dos crimes cibernéticos, é considerado como um crime comum que pode ser praticado contra qualquer pessoa física ou jurídica, que tenha seus bens ou informações violadas.

---

[10] OPICE BLUM, Renato M. S. **Direito Eletrônico** – a Internet e os tribunais. 1. Ed. São Paulo: EDIPRO, 2001. p. 211.

3 ANÁLISE DA LEI 12.737/12 E SEUS PROBLEMAS PRÁTICOS

A lei 12.737/12 não é uma lei independente, ela veio com o objetivo de modificar alguns artigos já existentes no Código Penal brasileiro, por isso é considerada como um diploma legal alterador.

A finalidade dessa alteração foi adequar os dispositivos legais para tipificar as condutas que são praticadas de forma exclusiva pelo meio informatizado, já que até a publicação da lei não existia legislação específica para punir os crimes cometidos no âmbito virtual.

O projeto de lei 2793/11 já vinha sendo discutido na câmara desde o ano de 2011, porém ganhou celeridade na sua aprovação depois de um crime informático cometido contra a atriz Carolina Dieckmann, que teve 36 fotos íntimas divulgadas na internet.

A nova redação dada pela lei 12.737/12, foi inserida no capítulo dos crimes contra a inviolabilidade dos segredos, prevendo então um novo tipo penal denominado pela doutrina como novatio legis incriminador. Como leciona o professor Fernando Capez “é a lei posterior que cria um tipo incriminador, tornando típica a conduta considerada irrelevante penal pela lei anterior”[11]. Essa alteração foi necessária devido a vedação existente no nosso sistema penal da analogia em desfavor do réu.

3.1 Tipo penal artigo 154-A

O artigo 154-A define a Invasão de dispositivo informático:

> 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.[12]

[11] CAPEZ, Fernando**. Curso de Direito Penal.** 11. Ed. São Paulo: Saraiva, 2007. p. 56
[12] BRASIL. Lei n° 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 21/11/2017

Esse tipo penal tem como primeiro elemento da sua fase de execução a invasão, e que essa invasão seja realizada contra equipamento alheio, por tanto o dispositivo informático não pode pertencer ao agente criminoso.

O segundo elemento do crime cibernético é a prescindibilidade da conexão com a internet, pois o criminoso pode instalar o malware mesmo sem a ligação com qualquer provedor ou fazê-la usando mecanismos físicos de armazenamentos de dados como: pen drives, onde o programa que captura os dados fica acondicionado sem qualquer conexão com a rede, portanto a consumação do crime pode se dar em momento posterior, pois o software malicioso fica inativo dentro do sistema operacional do dispositivo e não subtrai os dados naquele momento.

Outra característica importante do crime é a violação indevida do mecanismo de segurança, pois se o agente estiver com autorização como é o caso das empresas que realizam reparos nas redes, será considerado um atípico penal. Além da violação indevida do mecanismo de segurança é preciso que haja a instalação de malwares que obtém, adulteram ou destroem informações sem autorização expressa da vítima.

O legislador teve a atenção de punir não só o agente que pratica a invasão mais também, aquele que comercializa o dispositivo ou programa para o cometimento do crime, como é o caso do parágrafo 1º: "§ 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."[13]

Dessa maneira, a mudança na legislação veio para punir quem pratica e quem fornece os materiais necessários para o crime, se não houvesse essa previsão legal específica o fornecedor responderia apenas como partícipe.

Outra figura desse tipo é a conduta criminosa que causa prejuízo econômico, disposta no parágrafo 2º: "§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico".[14]

Nessa modalidade se restar provado que a vítima sofreu um prejuízo econômico advindo da conduta criminosa, o agente infrator terá sua pena aumentada.

---

[13] BRASIL. Lei n° 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 21/11/2017

[14] BRASIL. Lei n° 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 21/11/2017

Em alguns casos esse tipo penal vai ser qualificado, dependendo da finalidade da conduta, como exposto no parágrafo 3°:

> "§ 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"[15]

Essa qualificadora vai incidir sobre a conduta, se o agente criminoso invadir o sistema e obter dados específicos como: dados que estão inseridos nos e-mails da vítima, contratos comerciais que detenham informações relevantes para o funcionamento da empresa e se utilizar do acesso remoto que é a possibilidade de comandar o equipamento da vítima de qualquer lugar. A intenção tem que ser realmente a de obter informações, pois se não existir esse dolo específico o crime não existirá.

Continuando com a lógica do parágrafo 3º, o diploma legal visa agravar mais ainda a conduta de quem praticou a invasão e obteve os dados, se o agente propaga essas informações, essa conduta está descrita no parágrafo 4°: "§ 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 obtidas."[16]

Essa tipificação foi voltada para a punição dos agentes que negociam essas informações, devido ao crescimento da venda desses dados em mercados clandestinos, em que banco de dados como por exemplo o da Receita Federal são invadidos e os dados dos contribuintes são vendidos para terceiros.

Em muitos casos essas ações criminosas são patrocinadas por terceiros, e esses podem responder junto com o invasor na modalidade de partícipe, porém não deixa de ser aplicada a agravante ao mandante.

No seu último parágrafo ela disciplina outro tipo de agravante, que para ser aplicada leva em consideração outro requisito, como expõe o parágrafo 5º:

---

[15] BRASIL. Lei n° 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 21/11/2017

[16] BRASIL. Lei n° 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 21/11/2017

> §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."[17]

Nessa modalidade o requisito a ser observado é o cargo ou função ocupado pelo sujeito passivo do crime, devido as informações que possuem e a extensão do dano que pode ser causado a sociedade com a divulgação dessas informações públicas.

3.2 Ação penal artigo 154-B e alterações nos artigos 266 e 298.

No seu artigo 154-B, a lei estabelece qual o tipo de ação penal vai ser usada nos casos de crime cibernéticos:

> 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."[18]

A ação vai depender de quem foi o sujeito passivo do crime, no caso do delito ser cometido contra qualquer pessoa física ou jurídica segue a regra que é a ação pública, porém condicionada a representação. Nos casos em que envolver qualquer ente da administração pública direta ou indireta ou concessionária de serviço público a ação vai ser pública incondicionada.

A lei 12.737/12 também acrescentou outras definições em tipos penais existentes, como no caso do artigo 266, que foi alterado pelo artigo 3º da referida lei:

> Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:
> **"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública**
>
> Art. 266. .....
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

---

[17] BRASIL. Lei n° 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 21/11/2017

[18] BRASIL. Lei n° 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 21/11/2017

> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.[19]

A lei recebeu dois parágrafos, adicionando o serviço informático como um meio no qual sua perturbação ou interrupção de forma dolosa, constitui o crime previsto no caput. Surgiu devido a preocupação em resguardar principalmente os sistemas públicos que são prestados a sociedade.

Outra mudança realizada pela lei, foi no artigo 298:

> **Falsificação de documento particular** (Redação dada pela Lei nº 12.737, de 2012) Vigência
> 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** (Incluído pela Lei nº 12.737, de 2012) Vigência
> Parágrafo único. Para fins do disposto no **caput**, equipara-se a documento particular o cartão de crédito ou débito. (Incluído pela Lei nº 12.737, de 2012) Vigência[20]

Foi um grande passo na nossa legislação penal, pois com a equiparação dos cartões de crédito e débito a documentos particulares, surgiu a possibilidade de punir o agente que comete esse tipo de falsificação, em um contexto em que esse tipo de crime acontece corriqueiramente que é a clonagem de cartões.

3.3 Problemas práticos da lei 12.737/12

A legislação veio com o objetivo de suprir as lacunas no texto legal e punir o agente que comete o delito, porém alguns pontos retiram a eficácia plena desse tipo penal. Os problemas acontecem desde a fase de investigação do crime, até o final com a condenação do acusado.

3.4 Erros Legislativos

O primeiro ponto a ser abordado sobre os problemas desse diploma legal é a ausência de uma característica essencial da norma penal, que é seu efeito preventivo causado pela pena imposta ao delito.

---

[19] BRASIL, Lei nº 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 21/11/2017

[20] BRASIL. Lei n° 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 21/11/2017

Nos casos dos crimes cibernéticos a pena máxima que o agente criminoso pode receber de acordo com a lei 12.737/12 caput é de 1 ano de reclusão e multa, podendo chegar no máximo a 3 anos e 3 meses na modalidade mais gravosa do crime.

Devido essa baixa reprimenda penal por parte da nossa legislação, o crime é considerado de menor potencial ofensivo devido sua pena máxima não ultrapassar 1 ano, como está descrito na lei 9.099/95 no seu artigo 61:

> Art. 61. Consideram-se infrações penais de menor potencial ofensivo, para os efeitos desta Lei, as contravenções penais e os crimes a que a lei comine pena máxima não superior a 2 (dois) anos, cumulada ou não com multa. (Redação dada pela Lei nº 11.313, de 2006)[21]

Com isso, o criminoso que não tiver antecedentes criminais não ficará recluso da sociedade e será beneficiado com alguns institutos penais como a suspensão condicional do processo, que ao final se cumprido todos os requisitos será extinta a punibilidade.

A sociedade espera da norma penal a sua efetividade e quando isso não acontece, todo organismo social é abalado e a característica do Direito Penal que é a ultima ratio fica com sua aplicabilidade reduzida, por ser o ramo do direito que tem a função de retirar do individuo a sua liberdade de forma legal quando este atua de forma contrária a legislação.

A pena baixa para esse tipo de delito foi um erro do legislador na criação da norma, que não observou a dimensão do dano causado na vida das pessoas que são vítimas desse crime, esse erro foi causado devido a celeridade que foi dada para aprovação da lei, com o objetivo de atender ao clamor social pelo fato ocorrido com a atriz Carolina Dieckmann.

Outros erros legislativos são encontrados na redação do caput do artigo 154-A, que diz:

> 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.[22]

---

[21] BRASIL, lei 9.099/95 de 26 de setembro de 1995. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9099.htm. Acesso em: 24/11/2017

[22] BRASIL, Lei nº 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 21/11/2017

Para tipificação do crime a lei exigi um conjunto de elementos, não basta apenas a conduta de invadir o dispositivo informático, esse dispositivo tem que conter um mecanismo de segurança. Sobre mecanismos de segurança pode ser entendido como qualquer meio que permita que apenas pessoas específicas tenham acesso as informações contidas no dispositivo, como exemplo dessas ferramentas existem os login e senhas que permitem o acesso apenas a usuários que os detenham.

Muitos usuários desses equipamentos informáticos costumam não colocar senhas em seus dispositivos, e foi nesse ponto em que o legislador pecou na criação da norma, pois se o equipamento que foi invadido pelo criminoso não conter quaisquer mecanismos de proteção o agente infrator da norma penal ficará impune, já que o delito não estará tipificado.

Outro erro identificado na norma é que o crime não é considerado se o agente invadir o sistema, mesmo que ele contenha mecanismo de segurança, pois a lei exigi que a finalidade da conduta seja a de obter, adulterar ou destruir os dados do equipamento da vítima.

Portanto, se o agente invade o sistema burlando qualquer forma de proteção de dados do equipamento, mas não obtém para si as informações, as adultera ou destrói, não será passível de punição.

Além disso, o artigo define que essas condutas sejam realizadas sem o consentimento do proprietário do dispositivo, pois a invasão tem que ser sem consentimento expresso ou tácito, portanto se uma pessoa autoriza outra a fazer o uso do equipamento e esta faz uma das 3 condutas previstas no caput, obtém, adultera ou destrói as informações, não será punida como acontece de forma semelhante nos casos supracitados.

Desta forma, estamos diante de uma lei penal fraca, que foi elaborada sem o devido cuidado do legislador, que pretendia ocupar a lacuna existente para essa modalidade de crime, porém o que aconteceu foi a certeza da insegurança, pois as sanções que decaem sobre o criminoso são mínimas.

3.5 Dificuldades na investigação do crime

Umas das grandes dificuldades para apuração do delito é a identificação de sua autoria, devido ao tempo que leva da consumação do crime, até a sua apuração na fase investigativa.

Para localizar o criminoso é necessário o endereço de IP do computador, que funciona como um cadastro que cada máquina ligada a rede possui, essa informação pertence aos provedores de internet e são solicitadas pela polícia para saber quem é o usuário que está por trás do endereço eletrônico.

Acontece que o tempo que é gasto para conseguir essas informações junto as empresas de internet, é crucial para a investigação. Em 2015 foi realizada uma CPI devido a esses problemas nas investigações, e vários delegados foram ouvidos e relataram que depois da vigência do marco civil da internet as dificuldades só aumentaram, pois antes as empresas atendiam aos requerimentos da polícia para obtenção do IP, e hoje a maioria só disponibilizam por via judicial e devido a morosidade do judiciário a investigação acaba sendo enviada para o ministério público apenas para ser arquivada.

Segundo estudo realizado pela Norton, uma das principais fabricantes de antivírus do mundo, no Brasil leva em média 43 dias para solucionar um crime cibernético, enquanto em outros países chegam a autoria em apenas 9 dias.

Outro problema encontrado é a falta de recursos que são disponibilizados para a solução do crime, desde a questão orçamentária, até profissionais especializados na área.

CONSIDERAÇÕES FINAIS

A lei veio com o objetivo de preencher a lacuna existente na nossa legislação em relação aos crimes cibernéticos, devido ao crescimento desse tipo de delito. Porém na elaboração da norma não foi dada a devida atenção que um dispositivo legal necessita.

A norma foi aprovada ás pressas, pois já tramitava em regime de urgência nas casas legislativas e as indagações sobre como seria sua aplicação prática foi deixada de lado.

A lei foi produzida com várias lacunas e obscuridades que dificultam a sua eficácia, e que não atendem a finalidade desse diploma em sua plenitude, como nos casos em que o seu próprio texto legal pode isentar o criminoso de pena por erros textuais na construção da lei, que não permitem a tipificação do crime.

O legislador errou em transformar um fato isolado em lei, um tipo penal que não engloba a sua finalidade, e sim construção de uma norma que se adaptaria apenas em uma conduta criminosa idêntica à que foi praticada contra a atriz Carolina Dieckmann.

Outra lei que foi publicada posteriormente e que deveria ajudar na aplicação prática da lei dos crimes cibernéticos, como a lei do marco civil da internet, prejudicaram mais ainda na descoberta da autoria delituosa, colocando obstáculos nas já difíceis investigações realizadas pela polícia.

Temos no nosso país uma legislação desorganizada quando se trata da regulação de crimes eletrônicos, o que beneficia esse tipo de conduta que causas enormes prejuízos as vítimas

É preciso uma alteração nesse diploma legal, para que o direito penal possa garantir a sua base que é resguardar os bens jurídicos por ele tutelado, observando a realidade em que está inserido, devido esses crimes se atualizarem de forma muito mais rápida que nossa legislação.

REFERÊNCIAS

Ângelo, **Brasil lidera ranking mundial de hackers e crimes virtuais**. Folha de S.Paulo. Disponível em: http://www1.folha.uol.com.br/folha/informatica/ult124u11609.shtml. Acesso em: 12/11/2017

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em:21/09/2017

_____, Lei nº 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 21/11/2017

_____, lei 9.099/95 de 26 de setembro de 1995. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9099.htm. Acesso em: 24/11/2017

_____. Lei n° 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 21/11/2017

CAPEZ, Fernando**. Curso de Direito Penal.** 11. Ed. São Paulo: Saraiva, 2007.

Capez, Fernando. Curso de Direito Penal Parte Geral. 15.ed. São Paulo: Saraiva, 2011.

DINO, Divulgador de Notícias. Crimes Virtuais afetam 42 milhões de brasileiros. Disponível em: www.economia.estadao.com.br. Acesso em 10/09/17

GRECO, Rogério. **Curso de Direito Penal** Parte Geral.11. ed. Rio de Janeiro: Impetus, 2009.

_____, Comentário sobre o crime de invasão de dispositivo informático - Art.154-A do Código Penal. Rogério Greco. Disponível em: http://www.rogeriogreco.com.br/?p=2183. Acesso em: 10/11/2017

OPICE BLUM, Renato M. S. **Direito Eletrônico** – a Internet e os tribunais. 1. Ed. São Paulo: EDIPRO, 2001. p. 211

PINHEIRO, Patrícia Peck. **Direito Digital**. 2. ed. São Paulo: SARAIVA, 2008

PIRES, Hindenburgo Francisco. **O Surgimento dos Primeiros Computadores**. Disponível em: www.educacaopublica.rj.gov.br . Acesso em: 10/09/17.

ROCHA, **Crimes Virtuais**. Agente Criminoso Virtual. Disponível em: http://blogcrimesvirtuais.blogspot.com.br/p/agente-criminoso-virtual.html. Acesso em: 10/11/2017

.