FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ
CURSO DE DIREITO

LUIZ CARLOS CINTRA DE SOUZA FILHO

ANÁLISE DOS CRIMES CIBERNÉTICOS À LUZ DA LEI CAROLINA DIECKMANN: A PERSISTÊNCIA DE CARÊNCIA NORMATIVA

RECIFE
2015

LUIZ CARLOS CINTRA DE SOUZA FILHO

ANÁLISE DOS CRIMES CIBERNÉTICOS À LUZ DA LEI CAROLINA DIECKMANN: A PERSISTÊNCIA DE CARÊNCIA NORMATIVA

Monografia apresentada à Faculdade Damas da Instrução Cristã, como requisito parcial à obtenção do Título de Bacharel em Direito.

Orientador: Profº. Drº. Leonardo Siqueira.

RECIFE
2015

Souza Filho, Luiz Carlos Cintra de
Análise dos crimes cibernéticos à luz da Lei Carolina Dieckmann: a persistência de carência normativa. / Luiz Carlos Cintra de Souza Filho. – Recife: O Autor, 2015.

52 f.

Orientador(a): Prof. Dr. Leonardo Siqueira
Monografia (graduação) – Faculdade Damas da Instrução Cristã. Trabalho de conclusão de curso, 2015.

Inclui bibliografia.

1. Direito. 2. Carência normativa. 3. Crimes cibernéticos. 4. Lei Carolina Dieckmann. I. Título.

34	CDU (2.ed.)	Faculdade Damas
340	CDD (22.ed.)	TCC 2016-405

Luiz Carlos Cintra de Souza Filho

ANÁLISE DOS CRIMES CIBERNÉTICOS À LUZ DA LEI CAROLINA DIECKMANN: A PERSISTÊNCIA DE CARÊNCIA NORMATIVA

DEFESA PÚBLICA em Recife____, de_____ de 2015.

BANCA EXAMINADORA:

Presidente: Professor Dr.º Leonardo Siqueira.

1º Examinador: Prof.º Dr._____.

_____.

2º Examinador: Prof.º Dr._____.

_____.

RECIFE
2015

Dedico a todos aqueles que repudiam o ultraje à dignidade da pessoa humana.

AGRADECIMENTOS

A Deus, porque sem Ele não vejo sentido para a minha jornada nesta vida.

À minha família, sempre me amparando e me acolhendo.

À Faculdade Damas da Instrução Cristã, responsável pelo meu conhecimento científico e preparo para a minha atuação profissional.

Ao Orientador Professor Doutor Leonardo Siqueira, que, pela sua especial didática de ensino, em muito contribuiu no desenvolvimento e conclusão deste trabalho.

Ao Professor Doutor André Carneiro, pelo seu espontâneo e valioso apoio, meu muito obrigado.

Ao Professor Doutor Ricardo Silva, pela sua zelosa, eficiente e competente orientação.

Ao Professor Doutor Cláudio Brandão, pela sua inestimável atenção e incentivo, minha particular gratidão.

Ao Corpo Docente da Faculdade Damas da Instrução Cristã.

Ao Corpo Discente da Faculdade Damas da Instrução Cristã.

Às Irmãs da Faculdade Damas da Instrução Cristã.

Aos Funcionários da Faculdade Damas da Instrução Cristã.

E a todos que me ajudaram, meu sincero desejo de que sejam recompensados.

“A injustiça que se faz a um, é uma ameaça que se faz a todos.”
Montesquieu, Charles-Louis

RESUMO

Este trabalho científico se propõe a analisar a problemática existente na Lei n.º 12.737/2012, conhecida como Lei Carolina Dieckmann, que alterou o Código Penal Brasileiro, acrescentando os artigos 154-A e 154-B, em virtude de conter previsão de criminalização e punição de invasão apenas a aparelho informático que possua sistema de segurança, deixando sem amparo os demais aparelhos virtuais. A justificativa primordial da análise é tipificar os delitos informáticos, sua evolução e suas espécies, dado o aumento da utilização de aparelhos tecnológicos, nomeadamente da internet e seus aplicativos, abrindo enormes espaços para a prática de variados delitos, ante a carência normativa do Brasil. Aborda-se a questão da vítima de invasão de dados virtuais, que pode sofrer um grave prejuízo financeiro e/ou moral, sem a devida reparação dos danos, suportando os males da impunidade. Adentra-se no tratamento legislativo no Brasil dos crimes cibernéticos, indicando que a Lei n.º 12.737/2012, serviu como início de enfrentamento do problema, mas não criminalizou a invasão a aparelhos virtuais sem sistema de segurança. O bem jurídico tutelado é analisado, especialmente sob o prisma da invasão da privacidade e da intimidade. Fala-se da tipicidade, consumação e tentativa. Chega-se à conclusão do tema, no sentido de que o Brasil precisa avançar na elaboração de uma lei mais clara e severa, para inibir os crimes cibernéticos.

Palavras-chaves: Crimes Cibernéticos. Lei Carolina Dieckmann. Carência normativa.

ABSTRACT

This scientific work aims to analyze the existing problems in Law No. 12.737/2012, known as the Carolina Dieckmann Law, which amended the Brazilian Penal Code, adding the articles 154-A and 154-B, by virtue of containing criminalization forecast and punishment of invasion only in computer equipment that has security system, leaving the other virtual machines with no support. The primary justification of the analysis is to typify the computer crimes, their evolution and species, given the increased use of technological devices, including the internet and its applications, opening up huge spaces for the practice of various offenses, due to the deficiency on rules in Brazil. This thesis discusses the issue of victims of virtual data invasion, who might have a major financial and / or material damage, without due compensation for damage, thus supporting the harms of impunity. This paper also discusses the legislative treatment of cybercrime in Brazil, indicating that Law No. 12.737/2012, served as the beginning of tackling the problem, but not criminalized the invasion of virtual devices without security system. The safeguarded legal asset is analyzed, especially through the prism of invasion of privacy and intimacy. There is also a discussion on typicality, consummation and trial. Finally it comes to the conclusion on this issue, in the sense that Brazil needs to move forward in developing a more clear and strict law to inhibit cybercrime.

Key words: Cybercrime. Carolina Dieckman Law. Rules shortage.

SUMÁRIO

INTRODUÇÃO

Analisa-se a problemática existente na lei 12.737/2012, em virtude de conter previsão de criminalização e punição de invasão apenas a aparelho informático que possua sistema de segurança, deixando sem amparo os demais aparelhos virtuais.

A justificativa deste trabalho científico é, primordialmente, abordar os possíveis delitos informáticos, sua evolução e suas espécies, por notar-se nos últimos anos um aumento significativo do uso de aparelhos tecnológicos e a igualmente expansão da internet e seus aplicativos, abrindo enormes possibilidades para a prática dos mais variados delitos, ante a evidente carência normativa do Brasil.

Diante dessa expansão da internet e a carência da lei 12.737/2012 surge o seguinte problema de pesquisa: é possível em determinado crime cibernético o agente ficar impune?

A hipótese para este trabalho é: a invasão de aparelhos cibernéticos não protegidos com sistema sofisticado de segurança, causando prejuízos morais e/ou econômicos à vítima, não é considerada delito. O bem jurídico violado fica sem a tutela estatal.

O objetivo geral deste trabalho é analisar os crimes cibernéticos baseado na Lei n.º 12.737/2012, falando da invenção do computador, da criação da internet, do surgimento dos crimes cibernéticos em geral, sua evolução, as espécies, casos concretos de vítimas de invasão virtual, legislação existente, notadamente a Lei n.º 12.737/2012 – Lei Carolina Dieckmann, o bem jurídico tutelado como sendo, especialmente, e não exclusivamente, a privacidade e a intimidade dos usuários virtuais, a tipificação dos crimes, apontamentos sobre consumação e tentativa, e a conclusão da análise do tema.

Os objetivos específicos deste trabalho são: no segundo capítulo: abordar a evolução e as espécies. No terceiro tratar dos temas relativos ao direito tais como antecedentes, bem jurídico tutelado, tipicidade, consumação. No quarto capítulo sintetizar a conclusão do trabalho.

O primeiro capítulo desta obra, aponta a Lei n. 12.737, de 30.12.2012, popularmente conhecida como Lei Carolina Dieckmann, como uma das ações legislativas do Brasil que tratou de tipificar os delitos cibernéticos, acrescentando ao Código Penal Brasileiro, os comandos dos artigos 154-A a 154-B, na hipótese de invasão de dados individuais, profissionais, comerciais, industriais e de outros aparelhos tecnológicos desde que protegidos com sistema de segurança.

O segundo capítulo especifica os crimes cibernéticos, sua evolução, as espécies conhecidas atualmente e aspectos relacionados às vítimas.

O terceiro capítulo adentra no tratamento legislativo no Brasil dos crimes cibernéticos, ressaltando a previsão legal contida na Lei n.º 12.737/2012. Fala-se da legislação anterior, bem como de lei posterior e de projeto de lei para o futuro da segurança informática, contra os crimes cibernéticos. O bem jurídico tutelado é analisado sob o prisma da invasão da privacidade e da intimidade, com posicionamentos doutrinários e as classificações que servem como parâmetro para o enquadramento do agente delituoso, a consumação do delito e a tentativa.

O quarto capítulo traz a síntese dos pontos importantes que levaram à conclusão de cada um dos três capítulos desta obra, conluindo que os vários aspectos fáticos e legais analisados justificam dizer que a Lei 12.727/2012 deveria ter avançado mais, a fim de deixar os cidadãos melhor protegidos, considerando crime a invasão cibernética com fins maliciosos, pretendendo causar dano moral ou econômico, mesmo que esses aparelhos virtuais não possuam sistema de segurança.

2 – CRIMES CIBERNÉTICOS

2.1 Evolução

Tudo começa com um computador, que é qualquer equipamento ou dispositivo capaz de armazenar e manipular, lógica e matematicamente, quantidades numéricas representadas fisicamente. Em geral, entende-se por computador um sistema físico que realiza algum tipo de computação. Foi na II Guerra Mundial que realmente nasceram os computadores atuais. A Marinha americana, em conjunto com a Universidade de Harvard, desenvolveu o computador Mark I, projetado pelo professor Howard Aiken, com base no calculador analítico de Babbage. Mesmo que a tecnologia utilizada nos computadores digitais tenha mudado dramaticamente desde os primeiros computadores da década de 1940, quase todos os computadores atuais ainda utilizam a arquitetura de Von Neumann proposta no final daquela década.[1]

Quando a máquina chamada de computador foi criada ninguém imaginou que ela seria muito mais do que mais uma ferramenta para facilitar a vida do ser humano. Seria, o computador, naquela época, um aparelho com potencial de armazenamentos de dados e capacidade de transmissão de informações sem a pretensão da dimensão que veio a tomar. Mas veio a internet e, com ela, acredita-se que seria óbvio o aumento exponencial da sua utilização.

O que hoje forma a Internet, começou em 1969 com a ARPANET, criada pela ARPA, uma subdivisão do Departamento de Defesa dos Estados Unidos. Ela foi criada para a guerra, pois com essa rede promissora, os dados valiosos do governo americano estariam espalhados em vários lugares. Visou-se interligar todas as centrais de computadores dos postos de observação militar dos americanos, a fim de antever uma possível investida Russa. A ideia era permitir a continuação do funcionamento automático das informações contidas nas centrais de computadores, auxiliando e fornecendo informações a outros centros bélicos.

Em seguida, a ARPANET passou a ser usada pelas universidades, onde os estudantes trocavam, de forma ágil para a época, os resultados de seus estudos e pesquisas. Foi na década de 80 que ocorreu a transição da citada ARPANET para o que atualmente se denomina Internet. Foi nessa época que surgiu o conceito de *hacker*, a denominação ciberespaço e outras terminologias até hoje utilizadas. Em 1982 foi estabelecido o padrão IP/TCP, até hoje usado na rede, tornando-se obrigatório em 1983. Em 1990, a ARPANET foi desativada pelo

[1] PINHEIRO, Emeline Piva. Crimes virtuais: uma análise da criminalidade informática e da resposta estatal. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/29397-29415-1-PB.pdf. Acesso em 03.06.2015.

Departamento de Defesa, sendo substituída pelos *backbones* da NSFNET e foi criado um sistema de hipertexto com o auxílio do CERN. Neste ano, o Brasil também foi conectado a NSNET[2].

Em outra versão, tem-se que no período da guerra fria, mais especificamente durante o ano de 1962, pesquisadores americanos começaram a imaginar um sistema imune a ataques aéreos, que fosse capaz de interligar muitos computadores, permitindo o compartilhamento de dados entre eles. Passados sete anos, a primeira versão desse sistema ficou pronta, recebendo a denominação de *Advanced Research Projects Agency* ou Agência de Projetos de Pesquisa Avançada (ARPAnet). Sua principal característica era não possuir um comando central, de modo que, em caso de destruição de um ou mais computadores, todos os outros equipamentos ligados ao sistema continuariam operando.[3]

É fato, então, que a internet foi criada, primeiramente, com objetivos estritamente militares. A já mencionada ARPANET foi o embrião do que hoje é a maior rede de comunicação do planeta e surgiu em 1969, com a finalidade de atender a demandas do Departamento de Defesa dos Estados Unidos (DOD). A idéia inicial era criar uma rede que não pudesse ser destruída por bombardeios e fosse capaz de ligar pontos estratégicos, como centros de pesquisa e tecnologia. O que começou como um projeto de estratégia militar, financiado pelo "*Advanced Research Projects Agency* (Arpa)", uma agência americana, acabou se transformando naquilo que conhecemos hoje por Internet. Nos tempos da Guerra Fria, os militares de alto escalão dos Estados Unidos tiveram a ideia de criar uma rede que não formasse uma pirâmide (centralizada), mas sim, que os dados ficassem livres para serem acessados em qualquer rota, ainda que computadores fossem destruídos, os dados não seriam perdidos, pois estariam na rede caminhando em todos os sentidos.

No Brasil, o Instituto de Geografia e Estatística (IBGE) passou a utilizar um computador UNIVAC 1105 e em 1964 foi criado o Centro Eletrônico de Processsamento de Dados do Estado do Paraná. O Brasil criou o Serviço Federal de Processamento de Dados e se associou à INTELSAT, além de criar a Empresa Brasileira de Telecomunicações, ligada ao Ministério das Comunicações. O primeiro computador brasileiro, o "patinho feio", foi fabricado em 1972, pela USP. Outros eventos também impulsionaram o uso da internet no Brasil, tais como: a criação de Computadores Brasileiros S.A. (COBRA), em 1972; a criação da Secretaria Especial de

---

[2] REV. FAC. DIREITO UFMG. Crimes cibernéticos: o descompasso do estado e a realidade. David Augusto Fernandes. Belo Horizonte, n. 62, pp. 139 - 178, jan./jun. 2013.

[3] _____._____.

Informática, extinta em 1992; a conexão à Bitnet da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), do Laboratório Nacional de Computação Científica (LNCC) e da Universidade Federal do Rio de Janeiro (URJR), em 1988. A internet aqui, a princípio, interligava as principais universidades do país e não tinha interface gráfica, trocava-se apenas e-mails. Em 1995 houve a liberação comercial do uso da internet, com velocidade máxima da conexão de 9,6 Kbps. Nesse mesmo ano, criou-se o Comitê Gestor da Internet no Brasil (CGI.br).[4]

Conforme Bogo, citado na *Rev. Fac. Direito UFMG*[5], a internet surgiu no Brasil em 1991, trazida pela Rede Nacional de Pesquisas (RNP), com o objetivo de conectar redes de universidades e centros de pesquisas, indo posteriormente para as esferas federal e estadual. Somente em 1995, o Ministério de Comunicações e de Ciência e Tecnologia autorizou sua abertura para a comercialização, através da RNP, e depois com a Embratel. Já sua regulamentação foi feita pelo Comitê Gestor da Internet, criado por meio da Portaria Interministerial nº 147, e alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003, que tinha como funções integrar todas as iniciativas de serviços de internet no país e promover a qualidade técnica, a inovação e a disseminação dos serviços ofertados.

As considerações históricas colocadas sobre o surgimento do computador e, posteriormente, da internet, servem como ponto de partida para se chegar às consequências do invento. O computador é um grande passo tecnológico a serviço do Estado e da sociedade. Porém, como tudo que avança desmedidamente, fica-se a mercê de benefícios e malefícios. Onde está o homem, pode está a solução ou o problema. Por isso, o computador, e mais ainda, a internet, trouxe muitos transtornos aos seus usuários, uma verdadeira avalanche de novos tipo criminais.

Surge, então, o cibercrime, o qual teria tido o seu começo em 1982, com uma brincadeira de um adolescente de ensino médio (Richard Skrenta), que enviou aos seus colegas o vírus Elk Cloner para computadores Apple 2. Esse vírus, um disquete infectado, propagava um poema, daí criando o primeiro vírus de auto-propagação. Essa brincadeira gerou o aperfeiçoamento e popularização dos *rootkits*, que são ferramentas inventadas nos anos 70, que escondia os

---

[4] WENDT, Emerson. Crimes cibernéticos: ameaças e procedimentos de investigação. Emerson Wendt. 2.ª ed. – Rio de Janeiro: Brasport, 2013, p. 8-9.

[5] REV. FAC. DIREITO UFMG. *C*rimes cibernéticos: o descompasso do estado e a realidade. David Augusto Fernandes. Belo Horizonte, n. 62, pp. 139 - 178, jan./jun. 2013 141.

usuários criminosos que obtinham registros de acessos, manipulação de arquivos e de todas as funções de um sistema ou rede.[6]

Não é pacífica a notícia do aparecimento do que hoje denomina-se vírus de computador. Contudo, encontra-se a referência acima citada em diversos estudos dos crimes cibernéticos.

WENDT, estudioso do tema, também relata o episódio do adolescente Richard Skrenta, como o possível criador do primeiro vírus a infectar computadores e acrescenta que, em 1984, Fred Cohen apresentou um *paper*, chamado de *Experiments with Computer Viruses*, criando o termo "vírus de computador".[7]

Com a internet sendo cada vez mais utilizada, surgiram muitos outros vírus que causavam sérios transtornos aos usuários, tais como: lentidão no sistema, descarregamento de bateria de celular, corrupção de arquivos do disco rígido e ocupação de memória dos computadores.

Nesse contexto, a ideia da necessidade de proteção dos dados informáticos surgiu como resposta aos ataques através dos vírus maliciosos, que rapidamente aumentaram e se sofisticaram.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança brasileira (CERT.br), atende a qualquer rede brasileira conectada à internet, agregando informações quanto aos incidentes a ele reportados, registrando, analisando e tomando providências caso a caso. O percentual de incidentes é expressivo em 2009, agravando-se em 2011 e piorando em 2012. E, atualmente, esses crimes se renovam e se reinventam a cada instante.

Ainda no início das práticas delituosas, surgiu o *Trojan Horse* (Cavalo de Tróia), que é um programa que libera entradas em sistemas, possibilitando a invasão em computadores onde são instalados. O Cavalo de Tróia, até os dias de hoje, constitui uma grande ameaça aos usuários de internet. Não se usa mais os disquetes, mas o *Trojan Horse* pode se propagar através de e-mails, *instant messengers*, *pendrives* e qualquer outro meio de fácil armazenamento e disseminação de informação.

O avanço da internet fez surgir uma verdadeira revolução na informática, e com essa novidade vieram certos termos que serviram, e ainda servem, para designar pessoas ou atividades nos meios informáticos. Nesse cenário, surge a expressão linguística *hacker*, a qual

---

[6] MARIACAROL. Crimes virtuais e segurança. Disponível em: < http://paraentender.com/internet/crimes-virtuais>. Acesso em 02.06.2015.

[7] _____. _____. p. 10-11.

não tem significação pacífica no universo dos ilícitos em comento. O *hacker* é um indivíduo que se aprimora e se especializa nas habilidades de "haganear" pela internet, invandindo computadores de determinadas pessoas ou, o que é mais comum, praticando ilícitos, indistintamente, em qualquer computador que consiga atingir, com intuito de apenas se divertir com o transtorno das vítimas, ou para mostrar poder e conhecimento, ou para praticar crimes cibernéticos.

Os *hackers* se tornaram criaturas tão presentes e tão temidas no mundo informático que passou a existir como expressão linguística. No Dicionário Aurélio a definição do que seja *hackers* é a seguinte: "*Indivíduo hábil em enganar os mecanismos de segurança de sistemas de computação e conseguir acesso não autorizado aos recursos destes, a partir de uma conexão remota em uma rede de computadores; violador de um sistema de computação".* Pode-se dizer, também, que são *hackers* os sujeitos que se agrupam e "vivem" no meio virtual como se fora seu habitat natural.

Entre os *hackers* mais organizados e agregados, os mais conhecidos devido a sua voracidade em ataques a *sites* são: *silver lords, brazil hackers sabotage***,** *prime suspectz, tty0, demônios***.** Estes cinco grupos brasileiros foram "haqueados" pelo site alemão *Alldas.de*, como os mais ativos mundialmente em termos de ataques virtuais a grandes empresas e a altos órgãos governamentais dos mais diversos países. *Cracker, black-hat* ou *script kiddie*, neste ambiente virtual, denomina aqueles *hackers* que tem como *hobby* atacar computadores. Portanto a palavra *hacker* é gênero e o *craker* espécie.[8]

Ressalta-se que, a despeito das denominações supramencionadas, os dois termos servem para designar pessoas com especial habilidade em informática, seja para o bem ou para o mal.

A propósito, apenas para não passar a ideia de que foi esquecido, frisa-se que existe o lado sádio e de grande utilidade da internet, em que o mundo virtual é utilizado para diversão dos internautas, como fonte de informações diversas, realizações de negócios, divulgação de marcas comerciais e até de cumprimento de obrigações públicas e privadas.

Um exemplo de internet para lazer, é a criação do *Habbo Hotel*, que é hoje a maior rede social do mundo voltada para o público adolescente. Criado em 2000, o *Habbo Hotel* nasceu como um jogo virtual para reunir a moçada do mundo inteiro, mas acabou se transformando

---

[8]RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. ANO 2002. **Revista Jus Navigandi**, Teresina, ano 7, n. 58, 1 ago. 2002. Disponível em: <http://jus.com.br/artigos/3186/o-problema-na-tipificacao-penal-dos-crimes-virtuais>. Acesso em 03.06.2015.

numa poderosa ferramenta de marketing por iniciativa das próprias empresas, interessadas em participar da festa. O conceito do *site* é semelhante ao do *Second Life*, só que o *Habbo Hotel* foi bem sucedido.[9]

A forma ideal do uso da internet é divulgar notícias, denunciar abusos diversos, propiciar relacionamentos de amizade, difundir aspectos culturais, permitir que empresas e consumidores possam realizar negócios seguros e, até, incentivar o lado criador de seus usuários, seja informando, trocando ideias e interagindo com o fim de melhorar o cidadão cultural e politicamente.

Todavia, não é só isso que costuma acontecer. São grandes as queixas de pessoas que foram lesadas por indivíduos que se utilizam da internet para fraudar, falsificar, dar golpes, destruir dados e/ou divulga-los, sem autorização consciente do proprietário do aparelho informático.

Pois, com o desenvolvimento tecnológico, o ser humano passou a utilizar-se amplamente do sistema informatizado para se comunicar, resolver seus problemas, pagar suas contas, inscrever-se em concursos, interagir com outros seres humanos nas várias redes pessoais existentes na internet. Mas, de outro lado, a percepção criminosa visualizou que este meio tecnológico seria muito rentável para seus objetivos, aproveitando-se da ingenuidade e do despreparo de quem acessa a rede, tanto pessoa física como jurídica, ao não providenciar meios seguros para o acesso à internet.[10]

O avanço do uso da internet trouxe, ainda, importantes transformações nas entidades que antes tinha como lema o sigilo de suas informações. Mas,*" Poucas coisas continuarão secretas, e as mantidas em sigilo não permanecerão em segredo por muito tempo... O verdadeiro objetivo em segurança agora é retardar a redução das meias-vidas de segredos".* Hoje em dia, com a internet, a velocidade com que a transparência moldará uma organização depende de seu nicho competitivo. Empresas comerciais estão mais expostas aos efeitos da opinião pública, porque clientes podem passar facilmente para outras alternativas. Se for negligenciada, uma marca cultivada ao longo de décadas pode ser arruinada em meses. Caso não se adapte às exigências modernas, podem perecer. *Quando organizações se veem expostas, descobrem*

---

[9] EXAME, Revista. Internet: cada marca no seu quarto. Marcio Orsolini. ANO 44. Edição 966, n.º 7, de 21.04.2010, p. 70.

[10] REV. FAC. DIREITO UFMG. Crimes cibernéticos: o descompasso do estado e a realidade. David Augusto Fernandes. Belo Horizonte, n. 62, p. 139 - 178, jan./jun. 2013.

rapidamente que não podem mais depender de métodos antigos; elas precisam reagir à nova transparência ou acabar extintas. [11]

Recentemente, os usuários do Facebook foram enganados pela ação de agentes mal intencionados, conforme reportagem da UOL. Destacou-se que houve um golpe envolvendo o programa de Xuxa expondo centenas de celulares. O caso, ocorrido entre segunda à noite e terça-feira, dos dias 21 a 22 de setembro de 2015, fez centenas de pessoas divulgaram seus números de telefone no Facebook, após um pedido na página Xuxa Oficial: "Galera, deixa o número de vocês! Vou ligar". O *post* acabou desaparecendo da página, mas perfis não oficiais do programa de televisão da apresentadora lançaram apelos parecidos, enganando multidões de fãs no afã de falar com Xuxa e concorrer a prêmios de até R$ 2 mil, supostamente prometidos pelo programa.

Quase idênticas, páginas oficiais e falsas se diferenciam apenas por um pequeno ícone azul ao lado do título. Discreto, este símbolo foi criado pelo Facebook para ajudar internautas a conferirem a autenticidade de páginas de artistas e empresas. Perguntou-se, na reportagem, se, afinal, é seguro mostrar telefones pessoais em páginas públicas – mesmo que oficiais – nas redes sociais? A resposta de especialistas em segurança *online*, foi no sentido de que não é seguro, já que o perigo não está necessariamente nas intenções de quem pede seus dados, mas nos milhões de pessoas que poderão vê-los em caixas de comentários e usá-los, via de regra, para o mal.[12]

Aos 83 anos, Stênio Garcia é a mais nova vítima de *hackers*. O ator teve fotos íntimas ao lado da mulher, Marilene Saade, vazadas na internet. Nas imagens, os dois aparecem nus em frente a um espelho. Stênio Garcia e sua mulher, Marilene Saade, foram prestar queixas na delegacia do Rio de Janeiro depois que suas fotos íntimas vazaram na internet, na noite de terça-feira (29.09.2015). O casal acredita que a invasão ocorreu no celular. Marilene Saade disse que "Quando aconteceu com a Carolina Dieckmann, ainda não existia o *whatsapp*, pela internet é

[11] SCIENTIFIC AMERICAN, Brasil. Nosso futuro transparente. Daniel C. Dennett; Deb Roy.ANO 13, n.º 155, abril/2015, p. 65; 67.

[12]UOL tv e famosos. Golpe envolvendo programa de xuxa expõe centenas de celulares no FACEBOOK. ANO 2015. <http://tvefamosos.uol.com.br/noticias/bbc/2015/09/23/golpe-envolvendo-programa-de-xuxa-expoe-centenas-de-celulares-no-facebook.htm>, acesso em 23.09.2015.

mais fácil descobrir quem foi. Mas estou com um grande advogado, Ricardo Brajterman, e vamos descobrir quem fez isso".[13]

Lamentável o fato de termos que admitir a vulnerabilidade da privacidade de qualquer pessoa que guarde em aparelhos tecnológicos dados pessoais tão íntimos, como no caso de Stênio Garcia. Por enquanto, não há como socorrer, satisfatoriamente, quem não tenha a cautela de se privar de expor sua intimidade em meios eletrônicos.

A questão não é apenas nacional. Há pouco tempo, um *site* de relacionamento canadense denominado ASHLEY MADISON, direcionado a pessoas comprometidas que desejam trair a pessoa amada, teve seus dados roubados por um grupo de *hackers* chamado de *Impact team.* Os dados dos usuários do *site*, com nomes, e-mails, e outras informações pessoais, foram todos publicados na internet. O caso teve enorme repercussão na impresa internacional. Sobre o episódio, como porta voz, o policial canadense, Brice Evans, falou que "Essa é uma das maiores violações de dados no mundo e é única, pois expôs dezenas de milhares de informações pessoais, incluindo informações dos cartões de crédito. As consequências das ações do Time de Impacto – têm e vão continuar tendo um efeito social e econômico de longo prazo. Já há desdobramentos de crimes e vítimas. Nesta manhã, tivemos casos de possíveis suicídios que estariam associados à divulgação dos perfis dos usuários do ASHLEY MADISON".[14]

Como se vê, a questão da privacidade é coisa que deve ser tratada com muita seriedade. Devem os usuários ter os cuidados de usar serviços de boa política de privacidade, usar em seu computador criptografia e comunicadores seguros. Esses são os conselhos dos especialistas, que informam que países como a Argentina, Chile e Colômbia, já possuem leis para proteger os usuários de meios tecnológicos. No Brasil, se uma pessoa for vítima de um crime cibernético, certamente terá muita dificuldade para provar que o seu caso tem enquadramento legal e, pois, proteção do Estado.

Um outro meio ilícito do uso da internet e de outros meios informáticos é a prática de xingamentos, que, atualmente, tem-se popularizado como *bulling* virtual. Para tanto, o agente invade o sistema informático com intuito de inserir o xingamentos à pessoa vítima da invasão. Esses xingamentos são denominados no Direito Penal como injúria.

---

[13] _____. Abalada, mulher de Stênio Garcia fala sobre fotos íntimas vazadas: "Estou com vergonha". Disponível: http://entretenimento.r7.com/famosos-e-tv/abalada-mulher-de-stenio-garcia-fala-sobre-fotos-intimas-vazadas-estou-com-vergonha-30092015. Acesso em 1.º.10.2015.

[14] GLOBONEWS40. Sem fronteira. Jorge Pontual10.09.15, 23:30h. ANO 2015.

Para BONFIM[15], a injúria se caracteriza pela ofensa à honra subjetiva da pessoa humana, o que se conhece por xingamento. Existe a honra-dignidade e honra-decoro. A primeira diz respeito aos atributos morais da pessoa, por exemplo, chamar uma mulher de "sem vergonha". A honra-decoro está ligada aos atributos físicos e intelectuais, por exemplo, chamar uma pessoa obesa de "homem-balão" – atributo físico, ou dizer que certa pessoa é "burra" – atributo intelectual. É de se frisar que a injúria pode ser indireta, como, por exemplo, chamar o obeso de "magrinho" ou um analfabeto de "gênio".

Ressalta-se, tratando-se de ofensa à honra, que a imagem da pessoa humana é bem jurídico protegido constitucionalmente e, assim, há de ser protegido de ataques que possam advir de invasões a aparelhos tecnológicos que a contenha. Pois, como se sabe, até a imagem do condenado é alvo de proteção legal. Por isso, BRITO[16], sobre artigos da Lei de Execução, comenta que o art. 198 procura preservar a imagem do condenado, dispondo que "é defesa ao integrante dos órgãos da execução penal, e ao servidor a divulgação de ocorrência que perturbe a segurança e a disciplina dos estabelecimentos, bem como exponha o preso à inconveniente notoriedade durante o cumprimento da pena.

Como se vê, mesmo fora das questões da informática o Direito Penal já se preocupa com a honra e a dignidade da pessoa humana, muito mais preocupação existe hoje, pois a informática possibilitou o acesso rápido às informações das pessoas e, uma vez o agente operando a invasão às informações de sua vítima, pode cometer danos com mais rapidez e precisão, a depender de sua habilidade em invadir sistemas eletrônicos. Tudo isso deve levar o legislador a reforçar a proteção dos usuários virtuais, criminalizando não apenas as invações a sistemas de segurança, mas, igualmente, criminalizando e punindo toda e qualquer invasão de dispositivo informático.

2.2 Espécies

Diz-se que os crimes cibernéticos são delitos informáticos, envolvendo condutas humanas praticadas na internet e em outros meios relacionados a sistemas informáticos. O computador ou qualquer outro aparelho de comunicação virtual, seria uma arma para a prática do mal, ainda

[15] BONFIM, Edilson Mougenot. Direito penal, 2: parte especial. Edilson Mougenot Bonfim. 3.ª ed. – São Paulo: Saraiva, 2007, p. 99.

[16] BRITO, Alexis Couto de. Execução penal. Alexis de Couto Brito. 3.ª ed. – São Paulo: Editora Revista dos Tribunais, 2013, p. 140.

que não esteja ligada a redes de computadores, mesmo sem a ferramenta denominada de computador.

O crime cibernético, de forma ampla, é todo delito em que tenha sido utilizado um computador, uma rede ou ferramentas de acesso ao mundo virtual. O computador ou dispositivo eletrônico pode servir de agente, de facilitador ou de vítima do crime. O delito pode ocorrer apenas no computador, ou, também, em outras localizações, como *tablets* e celulares.

Os crimes digitais podem ser classificados em três categorias: o crime digital puro, o misto e o comum ou puro. A primeira é quando o computador é o alvo, ou seja, quando a ação ilícita tem como objetivo atingir ou o *hardware* – parte física do computador – ou o *software*, que é a sua parte lógica, virtual, ou os dados nele contidos. A segunda, o crime digital misto, é o que utiliza o computador como ferramenta imprescindível para a consumação do crime. E, a terceira categoria, o crime digital comum ou puro, é quando o computador é utilizado como depósito de provas, sendo, portanto, novo meio para atingir um crime antigo, já enquadrado no Código Penal, sendo, nesse caso, o computador instrumento não essencial para a realização do crime.[17]

Para compreender melhor a ampla variedade de crimes cibernéticos, segundo alguns estudiosos do tema, é preciso dividi-los em duas categorias gerais, crimes cibernéticos do tipo I e II. Os crimes cibernéticos do tipo I apresentam as seguintes características: Do ponto de vista da vítima, trata-se de um evento que acontece geralmente apenas uma vez. Por exemplo, a vítima baixa sem saber um Cavalo de Tróia que instala um programa de registro de digitação no computador. Também é possível que a vítima receba um e-mail contendo o que parece ser um *link* para uma entidade conhecida, mas que na realidade é um *link* para um *site* malicioso. Isso é facilitado por *software* de atividades ilegais, tais como programas de registro de digitação, vírus, *rootkits* ou Cavalos de Tróia. Os crimes cibernéticos do tipo II incluem, mas não se limitam a atividades como assédio e molestamento na Internet, violência contra crianças, extorsão, chantagem, manipulação do mercado de valores, espionagem empresarial complexa e planejamento ou execução de atividades terroristas. As características do crime cibernético do tipo II são, geralmente, uma série contínua de eventos com interações com a vítima. O criminoso forma uma relação ao longo do tempo, o que facilita a efetivação do crime.

[17] RT-TRIBUNAIS NORDESTE Revista dos. Os crimes digitais sob a vertente do Código Penal Brasileiro. Dayane Karla Barros de Farias Duarte; José Armando Ponte Dias Junior. Vol. 7/2014 | p. 277 – 291. Set - Out / 2014. Vol. 8/2014 | p. 227 - 291 | Nov - Dez / 2014.DTR\2014\21275.

Normalmente, eles usam programas que não estão incluídos na classificação de atividades ilegais. Usam, por exemplo, mensagens instantâneas ou arquivos que podem ser transferidos usando FTP.[18]

Nota-se que falhas ou vulnerabilidades no *software* fornecem um ponto de apoio para o criminoso. Exemplos desse tipo de crime cibernético incluem o *phishing*, o roubo ou a manipulação de dados ou serviços através de pirataria ou vírus, roubo de identidade e fraude no setor bancário ou de comércio eletrônico.

Tratando-se o *phishing* de uma fraude eletrônica, através da qual o agente obtém informações da vítima, senhas e dados pessoais, levando-a a erro, fazendo-se passar por terceiro, como por um banco ou um estabelecimento comercial ou levando o lesado a confiar em arquivos informáticos infectados por *softwares* daninhos, que capturam ou copiam dados, verifica-se que o objetivo do agente é a obtenção de vantagem patrimonial ilícita. É o tipo já descrito no artigo 171 do Código Penal. Neste caso, o artifício e o ardil encontram-se circunscritos ao gênero da fraude, ou seja, o engodo, o engano, a artimanha do agente, no sentido de fazer com que o lesado incorra em erro e ali, por vezes, permanecendo. De outro modo, a conduta em que o agente se utilizando de meios ardilosos, insidiosos, fazendo com que o lesado incorra, ou seja, mantida em erro, a fim de que o próprio agente pratique a subtração, está situada no disposto no artigo 155, § 4º, inciso II, segunda figura (fraude), do Código Penal, que é utilizada pelo agente, a fim de facilitar a subtração por ele levada a efeito.[19]

Existem ainda outros tipos de crimes praticados, tanto contra organizações quanto contra indivíduos. São estes: *Spamming* - conduta não ilícita, mas antiética, podendo se tornar ilícita, caso se configure como assédio; *Cookies* - são arquivos de texto que são gravados no computador de forma a identificá-lo; *Spywares* - são programas espiões que enviam informações do computador do usuário para desconhecidos na rede. Os *Spywares* podem vir acompanhado de *Hijackers*, ou seja, alterações nas páginas de *Web* em que o usuário acessa. É o crime mais utilizado nos dias atuais, pois é através de alterações nas páginas, que estariam teoricamente seguras, que os *hackers* conseguem enganar os usuários mais desavisados e distraídos, que acabam fornecendo as informações desejadas.

---

[18] NORTON BY SYMANTEC. O que é crime cibernético? ANO 1995-2015. Disponível em: <http://br.norton.com/cybercrime-definition>. Acesso em 02.06.2015.

[19] FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. Rev. Fac. Direito UFMG, Belo Horizonte, n. 62, pp. 139 - 178, jan./jun. 2013.

A propagação de *spywares* já foi muito comum em redes de compartilhamento de arquivos, como o *Kazaa* e o *Emule*; *Hoaxes* - são e-mails, na maioria das vezes, com remetente de empresas importantes ou órgãos governamentais, contendo mensagens falsas, induzindo o leitor a tomar atitudes prejudiciais a ele próprio; *Sniffers* - são programas espiões semelhantes ao *spywares* que são introduzidos no disco rígido e tem capacidade de interceptar e registrar o tráfego de pacotes na rede; *Cyberbullying* - definido como quando a Internet, telefones celulares ou outros dispositivos são utilizados para enviar textos ou imagens com a intenção de ferir ou constranger outra pessoa; Pornografia infantil, ação de pedófilos; Pirataria - baixar músicas, filmes e softwares pagos na Internet para depois copiar em CD ou DVD e distribuí-los gratuitamente ou mediante pagamento (sendo que o dinheiro não é repassado ao detentor dos direitos legais).[20]

Acredita-se que todos os usuários de internet já se depararam com mensagens que seriam de origem de órgãos públicos, trazendo assunto inquietante, como, por exemplo, e-mail com a aparência da página oficial da Polícia Federal, contendo intimação para responder a algum tipo de crime. Ainda, pode ocorrer de o usuário receber mensagem que seria de um banco avisando sobre o bloqueio ou encerramento de conta corrente. O infrator lança a mensagem e espera que o usuário, por coincidência, tenha conta naquele banco e acredite que sua conta está com problemas e, nessa ilusão, ou ingenuidade, acabe consultando a mensagem e, nessa ocasião, contrai para o seu computador um vírus que, certamente, irá lhe trazer prejuízos.

Frisa-se, por oportuno, que existem invasões virtuais que servem apenas para dissiminar ideologias repulsivas de seus atores. Dentro desse contexto, surgem os discursos de ódio, manifestações discriminatórias dirigidas a grupos específicos, que possuem determinadas identidades não aceitas pelo emissor da mensagem. Quer dizer, o discurso de ódio parte do pressuposto de que certa identidade é a normal, e as demais são consideradas equivocadas, antinaturais e, em face disso, são veementemente rejeitadas, de forma discriminatória e, muitas vezes, violenta. o discurso de ódio consiste na manifestação de ideias que incitam à discriminação racial, social ou religiosa em relação a determinados grupos, minorias, na maior parte das vezes. Busca desqualificar o grupo como detentor de direitos, representando o desprezo e a discriminação a determinadas pessoas, como nordestinos, negros, judeus, árabes, islâmicos, homossexuais, mulheres, entre outros.

---

[20] WIKIPEDIA. Crime Informático. ANO 2013. Disponível em: < http://pt.wikipedia.org/wiki/Crime_inform%C3%A1tico>. Acesso em 02.06.2015.

Aprofundando mais o conceito, observa-se que o discurso de ódio, baseado na dicotomia superior (emissor) e inferior (atingido), compõe-se de dois elementos: a discriminação e a externalidade. Pelo primeiro, o discurso deve manifestar discriminação, ou seja, desprezo por pessoas que compartilham características comuns. Pelo segundo, verifica-se que exige a transposição de ideias do plano mental para o fático, uma vez que, enquanto o pensamento permanece na mente do autor, inexiste dano. Além disso, é possível dividir o discurso de ódio em dois momentos: o insulto e a instigação. Enquanto o primeiro consiste na agressão à dignidade de determinado grupo de pessoas por conta de um traço compartilhado, o segundo é voltado a eventuais terceiros, "[...] leitores da manifestação e não identificados como suas vítimas, os quais são chamados a participar desse discurso discriminatório, ampliar seu raio de abrangência, fomentá-lo não só com palavras, mas também com ações.[21]

Quanto mais se fala sobre os crimes cibernéticos sem a edição de legislação coibitiva, mais os crimes aumentam. Dá para crer que o criminoso se beneficia com a discursão sem ação, pois isso é entendido como banalização do mal.

Urge combater as invasões virtuais com uma legislação que venha a tutelar a todos: o usuário *expert* – muito habilidoso em informática, e o usuário que necessita de usar internet ou outra ferramenta tecnológica, mas não é versado nessa área. Comparativamente, todos aqueles que não possuam deficiência impeditiva pode dirigir um carro, mas isso não significa que todos aqueles que não entendem de mecânica automobilística tenha que sofrer danos no seu veículo ou através dele. Não há sentido lógico-jurídico nesse raciocínio. Identicamente, o Estado não deve deixar à deriva os usuários de sistemas tecnológicos que não são especializados em informática.

[21] RDC - Revista Científica Direitos Culturais. Discurso de ódio na internet e multiculturalismo: uma questão de conflito entre liberdade de expressão versus dignidade da pessoa humana. Rosane Leal da Silva; Letícia Almeida de la Rue; Danielli Gadenz. – , v. 9 – n. 18 – Maio/Agosto/2014 – p. 129-151.

3 - TRATAMENTO LEGISLATIVO NO BRASIL DOS CRIMES CIBERNÉTICOS

3.1. Antecedentes

Importa citar a Convenção de Budapeste, a qual foi o resultado de um trabalho desenvolvido pelo Conselho da Europa, onde se procurou priorizar a proteção da sociedade contra a criminalidade no ciberespaço. Propunha-se a escolha de uma legislação comum que objetivasse uma maior cooperação entre os Estados da União Européia, sendo que tal tarefa já vinha sendo desenvolvida desde a década de 1990. Com a efetivação da Convenção de Budapeste, adotada em 2002 pelo Conselho da Europa, e a abertura à assinatura por todos os países que a desejarem, ficou demonstrada a atualidade desta nova modalidade de crime e a necessidade de ele ser combatido por toda a sociedade mundial, visto que não só atinge a Europa, mas todo o mundo.[22]

A despeito dos vários países que assinaram e de tantos outros que ratificaram a Convenção de Budapeste, o Brasil continua de fora dessas preocupações e providências, permanecendo modesto em editar leis que venham a dar meios de o usuário acionar o Judiciário indicando o dano sofrido e o respectivo enquadramento legal, a fim de obter a necessária tutela estatal e a consequente punição do criminoso.

A tutela jurisdicional é obrigação do Estado, tarefa competente aos juízes, que, portanto, não podem esquivar- se de tal ônus, como se observa no item XXXV do art. 5º da CF, e também no art. 126 do CPC. Todavia, observemos o que adverte o art. 2º do estatuto processual. Não pode o juiz agir por iniciativa própria, *Ne procedat judex ex officio*, como um Dom Quixote a reparar malefícios, na pitoresca imagem criada por Calamandrei.[23]

Frisa-se que ao Judiciário não compete agir sem provocação, como corolário do princípio da inércia, e nem decidir sem amparo legal, em obediência ao princípio da anterioridade da lei e, ademais, deve respeitar a divisão dos Poderes, eis que, cabe ao Poder Legislativo editar as leis e ao Judiciário aplicá-las.

Ainda sobre a função do Estado na proteção de terceiros, CUNHA JÚNIOR[24] expõe que essa função consiste no dever do Estado de proteger os titulares de direitos fundamentais

---

[22] REV. FAC. DIREITO UFMG. Crimes cibernéticos: o descompasso do estado e a realidade. David Augusto Fernandes. Belo Horizonte, n. 62, pp. 139 - 178, jan./jun. 2013 141.

[23] IV ANUÁRIO BRASILEIRO DE DIREITO INTERNACIONAL. Jurisdição no Ciberespaço. Alexandre Atheniense. ANO IV. V. 2, ano 2013, p. 99 – 112.

[24] CUNHA JÚNIOR, Dirley. Curso de direito constitucional. Edições Podium: Bahia, 2008, p. 529.

perante terceiros. Isso significando que o reconhecimento constitucional de um direito implica também para o Estado, para além do dever de abstenção (função de defesa), o dever de prestação consistente na obrigação de adotar medidas positivas e eficientes, vocacionadas a proteger o exercício dos direitos fundamentais perante atividades de terceiros que venham a afetá-los.

Dentre os direitos a serem protegidos, o autor citado acima aponta o direito de sigilo de dados, que deve ser tutelado pelo Estado contra eventuais agressões de terceiros, ou seja, contra a invasão de sistemas informáticos. No Direito de Informática ou da Informática, a norma penal deve coibir essas novas condutas "virtuais" e criminosas por assim dizer, mas deve fazê-lo com extrema cautela, uma vez que a identificação da autoria nesses tipos de crimes é de difícil apontamento. É que o Estado é carente da mesma tecnologia utilizada para o cometimento de certas condutas que vão se alterando a cada dia, não obstante convergirem para o mesmo fim, isto é, a prática daqueles "velhos" delitos arrolados nas legislações penais e no próprio Código Penal. Sob o impacto no mundo jurídico desses novos meios de cometimentos de condutas criminosas, além de abordar outras questões importantíssimas sobre o tema, inúmeras condutas criminosas praticadas por esse instrumento "internet" ainda podem perfeitamente serem incursas em dispositivos do nosso "velho" código penal. Evidentemente há outras que dependerão, para que tenham força coercitiva, de novas previsões e definições legais. Na área da Informática especificamente várias mudanças ainda estão por ocorrer.[25]

A Lei n.º 12.737/2012, alterando dispositivo do Código Penal, como o art. 154-A, da parte especial, título I – Dos Crimes Contra a Pessoa; capítulo VI – Dos Crimes Contra a Liberdade Individual; seção IV – Dos Crimes Contra a Inviolabilidade dos Segredos; objetiva proteger a privacidade do indivíduo no tocante aos dados e informações pessoais ou profissionais armazenados em dispositivo de informática que, de alguma forma, teve a sua segurança violada sem a autorização do titular. A referida lei também acrescentou ao Código Penal o art. 154-B, que dispõe: *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.*

Essas alterações ocorreram de forma apressada, eis que em 2011 houve um grande clamor por haver sido divulgadas fotos da atriz Carolina Dieckmann. O e-mail da vítima, que continha

[25] FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. Rev. Fac. Direito UFMG, Belo Horizonte, n. 62, pp. 139 - 178, jan./jun. 2013

fotos suas nua, as quais teriam sido enviadas a seu namorado, foi invadido por um *hacker*, o qual exigiu da atriz um valor em dinheiro a fim de evitar a divulgação das fotos. A atriz não cedeu à chantagem e as fotos foram divulgadas. Em razão da repercussão do episódio, no dia 16 de maio de 2012 o plenário da Câmara dos Deputados aprovou o projeto do deputado Paulo Teixeira, que tipifica principalmente o crime de invasão de dispositivo informático. Em 30 de novembro de 2012 foi sancionada a lei em comento, sendo popularmente conhecida como Lei Carolina Dieckmann.

A lei Carolina Dieckmann visa proteger dispositivos informáticos de invasões, evitando a violação desses aparelhos, desde que os mesmos estejam protegidos com sistema de segurança. O art. 154-A do estatuto em análise prevê que, invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o imtuito de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita, é conduta a ser apenada com detenção, de três meses a um ano, e multa, caso a conduta não constituir crime mais grave. Aumentando-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. Dar-se o aumento da pena de um terço à metade se o crime for praticado contra as diversas autoridades elencadas na respectiva lei.

São combatidas duas condutas incriminadoras. A primeira tem a ver com invasão de dispositivo de informática alheio, tais como: computadores domésticos ou de pessoas jurídicas, *notebooks*, *laptops*, *tablets*, *smartphones*, *ipads* ou aparelhos celulares, que estejam ligados a uma rede de computadores, ou não, e com ação de violar indevidamente mecanismo de segurança, com o fim de obter, adulterar ou destruir dados ou informações sem a autorização expressa ou tácita do titular do dispositivo. A segunda conduta diz respeito à instalação de vulnerabilidades (*softwares* maliciosos) para obter vantagem ilícita. Ressalta-se a necessidade de haver a caracterização de conduta dolosa, bem como, se da ação se venha a obter a adulteração ou a destruição de dados ou informações relacionadas à vítima, com intuito de auferir vantagem ilícita, mesmo que não seja vantagem econômica.

Antes da Lei n.º 12.737/2012, algumas leis brasileiras já procuravam proteger bens informáticos, tais como: a Lei n.º 7.646/87, dispondo sobre a proteção da propriedade intelectual sobre os programas de computador e sua comercialização no país. Contudo parte dessas disposições foram modificadas e ou revogadas pela Lei n.º 9.609/98, que veio a substituí-

la. É que essas normas não trataram das principais questões, nomeadamente os crimes ligados à informática, que atualmente merecem o enfoque do direito penal. Segundo parte da doutrina, o nosso Código Penal de 1940, encharcado de tantas outras leis esparsas, ainda assim, não se alcançou o mínimo ideal de tratamento eficiente a esses crimes, modernos e assustadoramente dinâmicos.

A Lei n.º 11.829/08, que combate a pornografia infantil na internet; a Lei n.º 9.609/98, que trata da proteção intelectual do programa de computador; a Lei n.º 9.983/00, que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da Administração Pública; a Lei n.º 9.296/96 que disciplinou a interceptação de comunicação telemática ou informática; a Lei n.º 12.034/09, que delimita os direitos e deveres dentro da rede mundial, durante as campanhas eleitorais; e, mais recentemente, a Lei n.º 12.737/12, conhecida como lei Carolina Dieckman, que trata da invasão a computadores ou aparelhos informáticos, com o fim de capturar e divulgar dados particulares do proprietário do aparelho, são exemplos de tentativas legislativas para solucionar os crimes cibernéticos. Porém, devido a deficiência das disposições e a velocidade do crescimento do tipo criminal, ainda não se pode dizer que existe uma lei que abranja uma boa gama de situações nessa área.

Por isso, o Código Penal, dentre a legislação já existente, ainda costuma ser aplicado nos casos de crimes virtuais, quando se trata de calúnia, difamação, ameaça, constrangimento ilegal, injúria, falsa identidade, e apologia a crimes de racismo, pedofilia, xenofobia, homofobia e outros que possam ser enquadrados nas categorias albergadas e punidas pelo nosso direito penal.

Para WENDT, a Lei n.º 12.737/2012 representou um grande avanço no ordenamento jurídico brasileiro. Porém, segundo o autor, alguns de seus aspectos têm gerado polêmica e preocupação, como, por exemplo,com relação às suas penas, consideradas exarcerbadamente brandas e, citando Renato Opice Blum, expõe que as penas cominadas são, aparentemente, pouco inibidoras, permitindo a aplicação das facilidades dos procedimentos dos Juizados Especiais. Mas, a tendência mundial é justamente oposta, no sentido de que o caso seria para uma punição mais severa, como uma condenação à prisão, além do pagamento do valor de indenização.[26]

[26] WENDT, Emerson. Crimes cibernéticos: ameaças e procedimentos de investigação. Emerson Wendt. 2.ª ed. – Rio de Janeiro: Brasport, 2013, p 234.

As penas da Lei n.º 12.737/2012, na visão da lição acima citada, não são suficientemente inibidoras da conduta criminosa. O agente que deseja praticar o ilícito cibernético não se depara com leis desestimulantes a ponto de se sentirem ameaçados e, por isso, não fream o seu intento criminoso.

Ressalta-se que, em matéria de invasões a sistemas informáticos, especificamente quanto à Lei n.º 12.737/12, pode-se interpretar que o legislador quis tutelar o bem jurídico em comento que estivesse munido dos adequados meios de proteção a impedir ou dificultar a tão temida invasão dos aparelhos. É o que se deduz do art. 154-A: *Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança* (...).

A Lei n..º 12.737/2012, de acordo com o *caput* do art. 154-A, acima citado, deixa margem a que se conclua que se trata de crime comum, comissivo, instantâneo, formal, unissubjetivo, plurissubsistente e doloso. No que toca ao seu § 1º, objetivou o legislador equiparar a conduta do agente que produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador àquela tipificada no *caput*. Buscou-se sancionar, desta forma, a conduta daquele agente que desenvolve, difunde, distribui de forma gratuita ou onerosa o *software* malicioso.

Noutra visão, entendendo eficiente a lei em análise, o § 2º do art. 154-A majorou a pena base do delito de 1/6 a 1/3, se a invasão ao equipamento informático causar prejuízo econômico à vítima, ou seja, a lei sanciona de modo mais severo quando a invasão atingir a esfera patrimonial. Já o § 3º do art. 154-A, dispondo que, 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, a pena-base será a de reclusão, de seis meses a dois anos, e multa, se a conduta não constituir crime mais grave.[27]

Ainda no campo daqueles que entendem eficaz a Lei n.º 12.737/2012, é expressado que o intuito do legislador foi o de punir de forma mais eficaz o agente que consegue controlar de forma remota o dispositivo informático, bem como obtenha conteúdo de comunicação eletrônica privada, segredo comercial ou industrial e informações sigilosas e, neste ponto, cumpre destacar que se mostra irrelevante que venha se tratar de segredo temporário. O § 4º, por sua vez, prevê causa de aumento de pena aplicável na hipótese em que as informações

[27] BONIJURIS Revista. Delitos cibernéticos: implicações da lei 12.737/12. Wanderlei José dos Reis. ANO XXVII. Fevereiro 2015, n. 615 | V. 27, n. 2, www.bonijuris.com.br

obtidas por intermédio das ações previstas no § 3º forem divulgadas, comercializadas ou transmitidas a terceiros. Importante inovação é disposta no § 5º, que estabelece o aumento de pena de 1/3 à metade se o crime for praticado contra contra autoridades[28]:

De outro turno, a Lei n.º 12.737/12 também estabeleceu, no art. 154-B do Código Penal, que os crimes previstos no seu art. 154-A somente se procederão mediante representação, exceto às hipóteses em que a prática delituosa se efetivar contra a administração pública direta ou indireta de qualquer dos poderes da União, estados, municípios e Distrito Federal ou contra empresas concessionárias de serviços públicos.[29]

Posteriormente, e como tentativa de trazer segurança ao uso da internet no Brasil, foi editada a Lei n.º 12.965/14, com vigência a partir de 23.04.2014, conhecida como o Marco Civil da Internet. O Marco Civil da Internet sem propõe a que a operação das empresas que atuam na *web* sejam transparente, com proteção dos dados pessoais e a privacidade dos usuários são garantias estabelecidas pela nova Lei. As empresas que trabalham com informações de clientes não poderão repassá-las para terceiros sem consentimento do titular dos dados, ressalvadas os casos onde existem ordem judicial.

Isso quer dizer que ao se encerrar uma conta em uma rede social ou serviço na Internet pode-se solicitar a exclusão dos dados de forma definitiva. Com o Marco Civil da Internet os dados são de seus proprietários, e não de terceiros. É a garantia da privacidade das comunicações. A afirmação em Lei de que o conteúdo das comunicações privadas em meios eletrônicos é dado sigiloso é um avanço importante, que garante aos novos meios de comunicação a mesma proteção já garantida aos meios de comunicação tradicionais.[30]

O Marco Civil considera a internet uma ferramenta fundamental para a liberdade de expressão e diz que ela deve ajudar o brasileiro a se comunicar e se manifestar como bem entender, nos termos da Constituição. O texto chega a apontar que "o acesso à internet é essencial ao exercício da cidadania". Um dos pontos essenciais do Marco Civil é o

---

[28] Art. 5.º, § 3.º. (i) o 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.

[29] REIS, Wanderlei José dos. Delitos cibernéticos: implicações da lei 12.737/12. Revista Bonijuris. Fevereiro 2015. Ano XXVII, n. 615. V. 27, n. 2.

[30] CULTURA DIGITAL. Marco Civil da Internet entra em vigor. ANO 2014. Disponível em: http://culturadigital.br/marcocivil/. Data do acesso: 18.09.2015.

estabelecimento da neutralidade da rede, que, em linhas gerais, quer dizer que as operadoras estão proibidas de vender pacotes de internet pelo tipo de uso.[31]

Para o futuro, como investida para a internet mais segura, o Senado aprovou, no dia 14.07.2015, projeto que pode facilitar as ações de repressão a crimes sexuais contra crianças e adolescentes praticados pela internet. O Projeto de Lei do Senado (PLS) 494/2008, de iniciativa da CPI da Pedofilia, disciplina a preservação de dados de usuários da internet e a transferência de informações aos órgãos de investigação policial. O projeto, que se encontra em análise na Câmara dos Deputados, estabelece que provedores de internet e empresas de telecomunicações situados no Brasil devem manter dados cadastrais e de conexão de seus usuários por pelo menos três anos. Já os fornecedores de serviço de conteúdo ou interativo, como operadoras de redes sociais, ficam obrigados a armazenar os dados por seis meses.

Na forma do projeto em análise, o Ministério Público e a polícia poderão pedir a preservação dos dados, independentemente de autorização judicial – que será exigida apenas para a transferência dos dados à autoridade que os solicitou. O projeto torna obrigatória a exigência de dados mínimos de identificação de todo destinatário de um endereço de internet protocolo (IP) e determina prazos máximos para resposta aos requerimentos de investigação criminal e instrução processual: duas horas, se houver risco iminente à vida; 12 horas, quando houver risco à vida; e três dias, nos demais casos.[32]

No cenário nacional atual, a promulgação da Lei 12.737/2012 trouxe para o ordenamento jurídico os delitos informáticos próprios, a partir da proteção da segurança informática em suas três vertentes. Infelizmente, o legislador criou também tipos de punição antecipadíssima, visando combate a atos preparatórios. Observe-se o § 2.º do art. 154-A que determinou que comete delito informático quem "produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática de invasão informática". A própria legislação quebrou a lógica da divisão da conduta conforme autoria ou participação, punindo aquele que faz a faca com a mesma pena daquele que dá a facada. Nesse sentido, o bem jurídico

[31] UOL. Disponível em: http://olhardigital.uol.com.br/noticia/5-pontos-essenciais-para-entender-o-marco-civil-da-internet/41053. Data do acesso: 18.09.2015.

[32] INTERNET LEGAL. Senado aprova projeto que regula armazenamento de dados de usuários da internet. ANO 2015. Disponível em: http://www.internetlegal.com.br/2015/07/senado-aprova-projeto-que-regula-armazenamento-de-dados-de-usuarios-da-internet/

fica esvaziado, posto que perde sua finalidade paradigmática, quebrando seu uso para geração de proporcionalidade e ofensividade.[33]

Percebe-se que a Lei n.º 12.737/2012, por prever penas apenas para os crimes de invasão de dados informáticos com sistema de segurança, necessita de uma legislação mais abrangente, desistimuladora dos criminosos de internet e outros meios eletrônicos. Por isso, como vimos linhas atrás, já existe Projeto de Lei com previsão de maior rigor para esses crimes que causam transtornos, danos econômicos ou danos à honra dos usuários de sistemas eletrônicos de armazenamentos de dados pessoais, comerciais e profissionais.

Apesar das inúmeras críticas acerca das técnicas legislativa utilizadas, a legislação trouxe proteção de integridade e confidencialidade no sentido de punir a "invasão informática", colocando na mesma rotulagem penal a obtenção e a destruição de dados ou informações privadas. Nesse sentido a lei apontou como conduta antijurídica o invadir de 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.Em si, a disponibilidade como desdobramento da segurança informática não nos pareceu ter recebido proteção direta. Apenas no verbo "adulterar" e na parte final do respectivo artigo, quando aponta a instalação de vulnerabilidades, indicou a reprovabilidade de atitude. E mesmo assim indiretamente, pois alterações e instalação de vulnerabilidades podem impedir a disponibilidade de arquivos mas também podem gerar violação de integridade e de confidencialidade somente. Em suma, a legislação trouxe ao cenário brasileiro, mesmo que com redação confusa, o início do debate acerca de um novo bem jurídico e a potencialidade penal de protegê-lo.[34]

A Lei Carolina Dieckmann, na visão de alguns estudiosos, foi um grande avanço, mas apenas para alertar a sociedade e os legisladores de que não foi suficiente a coibir a ação dos criminosos virtuais. Isso porque, a previsão de crime quando da invasão de aparelhos informáticos que não possuam sistema de segurança e, como dá para deduzir, sistema sofisticada de segurança, não convence a sociedade, a qual necessita de enquadramento como criminoso qualquer agente que invada aparelho eletrônico, mesmo que o mesmo não possua

---

[33] REVISTA BRASILEIRA DE CIÊNCIAS CRIMINAIS. O bem jurídico nos crimes informáticos. Spencer Toth Sydow. | vol. 113/2015 | p. 193 - 212 | Mar - Abr / 2015. DTR\2015\3604.

[34] _____._____.

sistema sofisticado de segurança. Pois, caso a chave da porta de uma residência esteja sem o trinco funcionando, não dá o direito de pessoa mal intencionada entrar na casa e pegar e levar tudo que entender que poderá lhe causar lucro ou grave embaraço ao proprietário. Se o roubo e o furto são crimes, também a invasão da privacidade dos dados de uma pessoa há de ser crime, desde que não haja autorização para captura desses dados.

3.2. O bem jurídico tutelado

O debate acerca do bem jurídico é atualíssimo e não há dúvida de que tipos penais são criados a partir de interesses políticos e pressões da mídia e da opinião popular. Destarte, o cenário penal atual é altamente retalhado. Há delitos sem qualquer respaldo na teoria da exclusiva proteção do bem jurídico, sem qualquer respaldo constitucional, há delitos que desrespeitam a própria teoria da tipicidade, que dispensam relação de causalidade, que antecipam a tutela penal para níveis autoritários e até mesmo delitos sem aplicabilidade prática que apenas visam interesses eleitoreiros. O Brasil trouxe para seu ordenamento jurídico lei que alterou o Código Penal, a Lei n.º 12.737/2012, e que levou em consideração a Convenção de Budapeste como referência de criação de tipos violadores de um bem jurídico denominado "segurança informática". Se a legislação previsse proteção desse bem jurídico sem levar em conta seus objetivos desdobramentos, poderia gerar intensos debates, especialmente pela volatilidade de conceitos da informática. Mas a legislação foi mais específica e tentou resguardar – ainda que de modo atécnico – a confidencialidade, a integridade e a disponibilidade de dados, sistemas e informações. Com isso, o debate do bem jurídico em si restringe-se, no que se refere à seara penal informática brasileira, aos tipos penais informáticos impróprios e a níveis excessivos de abstração de termos trazidos pela lei e pelo receio de que o legislador brasileiro, no meio informático, também inicie a tipificação de atos preparatórios, mesmo que sem antijuridicidade material.[35]

Para BRANDÃO[36], o bem jurídico é o bem ideal que se incorpora no objeto de ataque concreto. Mas que, ao analisar a estrutura do Direito Penal, constata que a ele não interessa tanto esse "algo concreto", isto é, o objeto da ação, mas o valor abstrato que se materializa neste algo: o bem jurídico. Ressalta o autor que, modernamente, define-se o bem jurídico à luz da

---

[35] REVISTA BRASILEIRA DE CIÊNCIAS CRIMINAIS. O bem jurídico nos crimes informáticos. Spencer Toth Sydow. Vol. 113/2015 | p. 193 - 212 | Mar - Abr / 2015. DTR\2015\3604.

[36] BRANDÃO, Cláudio. Curso de direito penal: parte geral – 2. ed. Cláudio Brandão – Rio de Janeiro: Forense, 2010, p. 125-128.

sociedade, e que um dos grandes artífices dessa concepção é Claus Roxin que cria doutrina original, no sentido de que o Estado não pode ter a função de realizar fins divinos ou transcendentais, mas a função do Estado é garantir a um grupo de indivíduos – os seus súditos – as condições de existência que satisfaçam as suas necessidades vitais. *Em cada situação histórica e social aqueles pressupostos imprescindíveis para assegurar a existência de um grupo humano são considerados bens jurídicos.* Eles se concretizam numa série de condições valiosas como a vida, a liberdade, o patrimônio, e que cabe ao Direito Penal assegurar esses bens jurídicos, punindo a sua violação.[37]

Prosseguindo, o autor, ainda citando Urs Kindhãuser, aponta que o Direito Penal serve para proteger os bens jurídicos, e que essa proteção não se refere, isoladamente, aos bens ditos como pessoas, coisas ou instituições, mas, também, à relação desses bens com os sujeitos que devem ser beneficiados por ele. A tutela de bens jurídicos, nesse diapasão, significa a proteção dos princípios que salvaguardam o indivíduo no sentido de sua participação igualitária na interação social.[38] Ademais, o autor aponta o pensamento de Urs Kindhãuser, segundo o qual, bens jurídicos são aqueles que representam a identidade jurídica de uma sociedade e de sua perpetuação.[39]

Nesse contexto, o computador é apenas uma ferramenta utilizada para a prática virtual ilícita. Nesse caso, os bens jurídicos tutelados seriam a liberdade individual; o direito ao sigilo pessoal e profissional; a intimidade, quando alguém invade um computador apenas para ver os e-mails, tomando conhecimento do que neles está contido; o bem tutelado seriam os costumes, no caso de pedofilia; o bem tutelado seria o direito de propriedade, quando se invade um sistema financeiro, a fim de subtrair para si ou para outrem, objetos ou valores; o bem jurídico tutelado é o patrimônio, quando houver furto através de invasão e captação de senhas e, consequente retirada de numerário ou, sendo ainda o patrimônio como bem jurídico tutelado, quando houver invasão de um computador com a finalidade de destruí-lo ou destruir programas, causando, assim, dano informático, ou seja, dano ao patrimônio alheio; o bem jurídico tutelado é a propriedade intelectual, quando houve pirataria de músicas, filmes, *software*.

Pode-se dizer, então, que, no geral, o bem jurídico tutelado é a inviolabilidade dos dados informáticos. É a própria segurança da informação. E, para muitos, o bem jurídico tutelado é a própria informática, especificamente a internet, o espaço virtual. Isso porque, na

---

[37] _____._____, p. 27-28.

[38] _____._____, p. 67.

[39] _____._____, p. 68.

atualidade, via de regra, no espaço informático temos armazenados dados de nossa intimidade, vida privada, honra e imagem.

Daí que, agora com o fator globalização e com a explosão da utilização da internet de maneira inequívoca, como bem diz a professora Ivette Senise Ferreira, titular de Direito Penal e Diretora da Faculdade de Direito da USP ("A Criminalidade Informática"), "a informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas mãos dos criminosos. Este alcance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução". ("Direito e Internet – Aspectos Jurídicos Relevantes" p. 207).[40]

Cabe ao direito penal a proteção dos bens jurídicos mais relevantes para o meio social, ou seja, este ramo do ordenamento jurídico tutela o que é basilar para a própria existência da sociedade, que é o direito à vida; a liberdade; o patrimônio; a propriedade imaterial; a organização do trabalho; o sentimento religioso e o respeito aos mortos; a honra, imagem e privacidade; a dignidade sexual; a família; a incolumidade pública; a paz pública; a fé pública; a administração pública; o meio ambiente e tantos outros bens. Por este viés, observa-se que a concepção de bem jurídico deve estar atrelada aos valores. Houve uma onda de globalização das informações e isso trouxe a possibilidade de armazenamento de dados industriais e individuais, dados relativos a contas bancárias, números de cartões de crédito, senhas de acesso, trocas de experiências interpessoais, criação e difusão do comércio eletrônico por conta desses avanços tecnológicos. A internet se tornou um campo propício para a prática de novos delitos, principalmente ligados à honra, tais como calúnia, injúria e difamação.[41]

A propósito, o direito à intimidade refere-se ao direito de a pessoa resguardar apenas para si determinadas informações, ou seja, alcança a discrição pessoal atinente aos acontecimentos e desenvolvimento da vida do ser humano, tais como confidências, informações pessoais (nos quais se incluem os dados pessoais) e convicções. A esfera da intimidade garante ao indivíduo o direito de destoar da média social e viver, ainda que solitariamente, a sua escolha. Portanto, diz respeito àquela esfera da vida privada que o sujeito guarda apenas para si, não

---

[40] REV. FAC. DIREITO UFMG. Crimes cibernéticos: o descompasso do estado e a realidade. David Augusto Fernandes.Belo Horizonte, n. 62, pp. 139 - 178, jan./jun. 2013.

[41] BONIJURIS Revista. fevereiro 2015, ano XXVII, n. 615, v. 27, n. 2, www.bonijuris.com.br **7**

compartilhando nem mesmo com as pessoas mais próximas. Com efeito, direito à intimidade e direito à vida privada não são sinônimos, apesar de ambos serem direitos de personalidade. O direito à intimidade corresponde a todos os fatos, informações, acontecimentos ou eventos que a pessoa deseje manter em seu foro íntimo, ou seja, é o direito de estar só, enquanto o direito à vida privada denota a existência de duas esferas, a saber, pública e privada, sendo que a primeira refere-se à vida política, e a segunda, à vida doméstica.[42]

A diferenciação entre direito à vida privada *stricto sensu* e direito à intimidade possui significativa importância para eventual indenização por danos morais. Explica-se: apesar de ambos os direitos serem protegidos pelo Texto Constitucional, a intimidade deve receber maior proteção, uma vez que abarca fatos e segredos de cunho ainda mais pessoal. Consequentemente, o valor da indenização por danos que a envolvem tende a ser maior que o valor referente à violação à vida privada *stricto sensu*. Não há como ter noção de quais informações pessoais são publicizadas ou possuem potencial para ser. Por conseguinte, é que se faz necessária a proteção de dados, como novel direito fundamental, instrumental à defesa da vida privada e da intimidade, nucleares do direito à privacidade, a qual funciona como uma contraposição legítima à própria estrutura de sociedade pós-moderna.[43]

Na visão de BULOS[44], a honra é um bem imaterial de pessoas físicas e jurídicas, traduzida pelo sentimento de dignidade própria (honra interna ou subjetiva), pelo apreço social, reputação e boa fama (honra exterior ou objetiva); a imagem, como atributos exteriores da pessoa física ou jurídica, com base naquilo que ela própria transmite na vida em sociedade, sendo, portanto, uma imagem quase publicitária, sujeita a alterações a qualquer tempo, assim danos cometidos contra a imagem social podem ser indenizados.

Acrescenta o autor supra que, normalmente, os causadores desses danos às pessoas físicas ou jurídicas são os meios de comunicação em massa, tais como: televisão, rádio, internet, jornais, revistas e outros, sendo, nesse caso, tranquila a jurisprudência quanto ao reconhecimento da tutela à imagem. E, ainda, que há jurisprudência do Supremo Tribunal Federal, no sentido de que, o que acontece é que, de regra, a publicação da fotografia de alguém, com intuito comercial ou não, causa desconforto, aborrecimento ou constrangimento, não

---

[42] DOUTRINAS ESSENCIAIS DE DIREITO CONSTITUCIONAL. O direito fundamental à privacidade e à intimidade no cenário brasileiro na perspectiva de um direito à proteção de dados pessoais. Andrey Felipe Lacerda Gonçalves;Monique Bertotti; Veyzon Campos Muniz. | vol. 8/2015 | p. 597 - 614 | ago / 2015.DTR\2015\11488

[43] _____._____.

[44] BULOS, Uadi Lammêgo. Curso de direito constitucional. Uadi Lammêgo Bulos. São Paulo: Saraiva, 2007, p. 428-429.

importando o tamanho desse desconforto, desse aborrecimento ou constrangimento. Continuando a sua didática, fala da privacidade como sendo aquele valor que envolve os relacionamentos do indivíduo, tais como suas relações comerciais, de trabalho, de estudo, de convívio diário e, quanto à intimidade, esta diz respeito às relações com amigos, familiares e companheiros que participem de sua vida pessoal.

O jurista, ao qual ora se recorre, enfatiza que os direitos à vida privada, intimidade, honra e imagem funcionam como limites às intromissões abusivas e ilícitas. E diz que, tristeza, equívocos, desavenças conjugais, rompimento de namoro ou de noivado, falecimento, crises financeiras não devem servir como matéria para divulgação, e que, embora o art. 5.º, inciso XIV da CF/88 permita o acesso à informação, isso não permite que sejam divulgadas fotos, imagens, documentos injuriosos, insinuações capiciosas ou mentirosas, que maltrata a dignidade humana e, pois, o sentimento alheio.

Então, é censurável o limitado alcance da Lei n.º 12.737/12, que prevê punição apenas para as invasões sem sistema de seguranças pois, se a divulgação dos bens jurídicos mencionados acima é violação à dignidade da pessoa humana, muito mais grave é a divulgação desses bens jurídicos mediante invasão dos sistemas informáticos que armazenam esses dados. Isso porque, toda invasão a tecnologia, com ou sem dispositivo de segurança, deveria ser considerada crime e, como tal, o invasor deveria ser punido.

A concepção de bem jurídico revela um interesse existencial da sociedade que, por ser tido como imprescindível à sua própria existência comunitária, recebe um juízo de valoração pelo Direito e passa a gozar de proteção jurídica. Bens jurídicos são interesses vitais para a convivência social pacífica e plena, e por isso, gozam de proteção jurídica. Quando essa proteção é conferida pelo Direito Penal, por meio da previsão de crimes e cominação de sanções penais, está-se diante de um *bem jurídico-penal*, constituindo todo o alicerce do Direito Penal democrático e da ofensividade. Saliente-se que o vínculo existente entre Constituição e Direito Penal, a par das limitações ao *ius puniendi* exaradas pelos princípios constitucionais penais, também se relaciona com o processo de seleção dos valores sociais a serem tutelados pelo sistema penal.

Então, a Constituição se apresenta como limite à escolha dos bens jurídicos-penais, uma vez que impede sejam dotados de dignidade penal valores incompatíveis com o seu quadro axiológico. Portanto, não são apenas os bens jurídicos indicados expressamente pela Constituição os possíveis destinatários da tutela penal. Também os valores consagrados pela sociedade, ainda que sem previsão constitucional expressa, podem (e devem) ser protegidos

pelo Direito Penal, desde que compatíveis com a Constituição. Nas palavras de Bittencourt, *apud* Scolanzi[45], bens jurídicos "[...] *são bens vitais da sociedade e do indivíduo, que merecem proteção legal exatamente em razão de sua significação social.* [...] *A soma dos bens jurídicos constitui, afinal,* a *ordem social*"(2010, p. 38).

A internet, como bem jurídico, tem alçado importantes espaços, o mais atual é o espaço político, onde estamos assistindo a uma forte evolução das redes sociais na política participativa. De fato, a internet tornou-se a voz do povo na forma mais célere possível, devido às facilidades que a internet tem de espalhar informações e trocas de dados e de ideias.

No Fórum sobre Informação, Poder e Ética no Século XXI, o sociólogo Manuel Castells, que analisou as mudanças que a internet produziu na cultura e na organização social, disse: "acabou a manipulação informativa sem resposta por parte da sociedade" e alertou para "o descontentamento generalizado com os políticos que se comportam como marcas e se dedicam a crítica destrutiva, mais eleitoreira do que preocupada com o bem comum". César Maia, em recente artigo publicado na Folha de S.Paulo, cita o autor Manuel Castells, no seu livro *Comunicación y Poder*, que trata da mudança na política pela transformação da comunicação. "Hoje, o jogo do poder depende também das novas mídias, via internet e celular, que são redes horizontais ou autocomunicação de massa. O sistema se abre a mensagens de todo tipo, indivíduos e de movimentos sociais. Estes atuam sobre valores sem objetivar o poder, estão fora da sociedade civil organizada", diz Maia. "Aqui surgem práticas políticas insurretas, movimentos espontâneos dos indignados, que até desestabilizam governos. Passam por cima dos partidos e das regras do jogo. O espaço público está sendo reconstituído fora das instituições. As condições de mudança se produzem nesse novo espaço da comunicação", conclui.[46]

O tempo em que estamos vivendo revela alterações na vida e no comportamento dos homens. Nesse contexto, os direitos sociais das minorias, os direitos econômicos, os coletivos, os difusos, os individuais homogêneos passaram a conviver com outros de notória importância e envergadura. Referimo-nos aos direitos de quarta geração, relativos à informática, softwares,

---

[45] SCOLANZI, Vinícius Barbosa. Bem jurídico e Direito Penal**.** Revista Jus Navigandi, Teresina, ano 17, n. 3129, 25 jan. 2012.< http://jus.com.br/artigos/20939>. Acesso em 02.06.2015.

[46] SOCIOLOGIA, Revista. Mídias sociais: rumo à democracia participativa?. ANO IV – Edição 37 – outubro/novembro/2011.

biociências (...). Paulatinamente, o Judiciário brasileiro tem-se deparado com esses direitos, os quais são filhos do processo de globalização do Estado neoliberal.[47]

Ante o texto acima, verifica-se que a internet é do povo, é um bem que o cidadão brasileiro e o mundo tem se utilizado para as mais diversas atividades comunicativas e sociais. A internet tornou-se o meio mais importante e utilizado de socialização virtual, e, sem a presença física dos cidadãos, estes estão conseguindo difundir notícias, organizar mobilizações e até influenciar na vida cultural e política de um país. É uma arma nas mãos dos povos. Deveria ser sempre bem utilizada. Mas, como tudo que cresce desmedidamente, sua utilização não tem sido apenas para o bem. Criminosos também estão entre aqueles que se utilizam da internet. Razão pela qual, esse bem tornou-se o bem jurídico a ser tutelado.

Para PRADO[48], a sociedade se caracteriza como uma sociedade da informação, que supõe a informatização de diversos dados e setores (pessoal, econômico e social), suscitando, cada vez mais, a questão da proteção da vida privada e dos dados pessoais diante dos riscos que essa sociedade representa – a sociedade da informação. Tratando-se, pois, de direito fundamental autodeterminação informática (tutela dos dados). Isso quer dizer o direito personalíssimo referente à faculdade que tem toda pessoa de exercer o controle sobre sua informação pessoal e sobre os dados armazenados informaticamente.

Nesse contexto, importa falar sobre sigilo, do ponto de vista da informação. CALADO[49], em seu artigo, expõe que o sigilo está ligado à intimidade do indivíduo, a garantia dada a estes meios pela lei aumenta a utilização deles para a transferência de informação privadas, pessoais e personalíssimas, cada qual com seu grau de sigilosidade. Segue-se que, nos meios virtuais de circulação de dados, deve haver segurança dos dados fornecidos em meios de informática. A expansão do uso das redes de computadores se aperfeiçoarão se existir confiabilidade na circulação de informações. Pois existem dados que são pessoais e de uso exclusivo do internauta, contendo um complexo de dados necessário à identificação virtual e, até mesmo, da vida íntima do mesmo. A identidade informática é sigilosa e deve ser protegida.

---

[47] BULOS, Uadi Lammêgo. Curso de Direito Constitucional. Uadi Lammêgo Bulos. São Paulo: Saraiva, 2007, p. 403-404.

[48] PRADO, Luiz Regis. Direito penal econômico. Luiz Regis Prado. – 5.ª ed. – São Paulo: Editora Revista dos Tribunais, 2013, p. 116.

[49] ÂMBITO JURÍDICO. O Sigilo de Dados no Meio Virtual. Maria dos Remedios Calado. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9528>, acesso em 22.09.2015.

A autora em questão, citando Guilherme Feliciano (2001, p. 63), põe que "*a violação de correspondência eletrônica ou de documento eletrônico, com revelação indevida de conteúdo (se constituir segredo), caracteriza o delito.* Definir a situação dos dados informáticos e situá-los juridicamente na internet é difícil por natureza, e a cada nova questão surge debate para delimitar qual o campo de ação do Direito. Não obstante, ante a existência no mundo virtual de *logins*, senhas, códigos e chaves eletrônicas que identificam cada qual, faz-se necessárias medidas protetivas e repressivas pelo Estado, que poderá fundamentar o direito do sigilo de dados informáticos, elemento este basilar para o complexo jurídico da pessoa humana.

Tem-se que, na hipótese do bem jurídico ser penalmente tutelado, deve-se fazer um exame a partir da incriminação feita às condutas que venham a lesá-los. Se essa lesão é unicamente apenada a título de dolo, as agressões a esse bem jurídico só poderão, também, ser dolosas. Caso haja a punição a título de culpa, pelo fato do legislador ter acreditado ser essencial a prevenção em relação a essas condutas culposas, a agressão pode se dar, da mesma forma, pela imprudência.[50]

Nesse quadro, trazendo-se o texto acima para o assunto em análise, pode-se dizer que o legislador pretendeu, com a redação do art. 154-A, da Lei n.º 12.737/2012, tutelar o bem jurídico com punição a nível de invasão dolosa, eis que deixou expressamente assente que o proprietário do aparelho informático deve se prevenir de ataques tomando o cuidado de proteger o seu aparelho com dispositivos de segurança. O legislador deu a entender que, em caso contrário, a punição não seria aplicada, pois, por culpa do proprietário do bem, o mesmo restou sem os dispositivos de segurança.

Todavia, muitos entendem diferentemente do que acima foi dito. Nesse passo, temos que: O termo "mecanismo de segurança" deve ser entendido de forma ampla, pois de outra forma tornaria a lei sem eficácia já que nem sempre o titular de um dispositivo vai colocar senha, antivírus, *firewall* (*software* que protege o computador de determinados ataques virtuais) ou outra tecnologia de segurança. Além disso, se o artigo for tomado ao pé da letra, se torna antagônico: por que o legislador exigiria a violação indevida de mecanismo de segurança e, ao mesmo tempo, a ausência de autorização expressa ou tácita do titular do dispositivo. Se houve

[50] *DUC IN ALTUM*, Revista. Considerações sobre os requisitos da ação para a legítima defesa. Leonardo Siqueira. Caderno de direito, vol. 4, n.º 6, jul-dez, 2012, p. 244. Disponível em: file:///C:/Users/LCP/Downloads/170-596-1-PB%20(3).pdf. Acesso em 21.11.2015.

violação indevida obviamente não houve autorização, em contrapartida se houver autorização, não há que se falar em violação indevida do mecanismo de segurança.[51]

Discorda-se, pois, do entendimento colocado linhas atrás, pois a lei não contém palavras inúteis, sendo certo que, de fato, colocou-se como condição para a caracterização da invasão a vulnerabilidade do aparelho eletrônico da vítima. Porém, insiste-se que o bem tutelado deveria ser todo e qualquer aparelho informático, com ou sem dispositivo de segurança, por uma razão muito simples: é crime invadir a propriedade tecnológica alheia, com o intuito de danificar ou fazer qualquer tipo de alteração, captação e divulgação, esteja ou não esse patrimônio com sistema de segurança.

Portanto, vê-se que, a despeito da tutela legal já existente, o bem jurídico não está, ainda, satisfatoriamente tutelado. Faz-se necessário, por ser de bom alvitre, o aperfeiçoamento da legislação, a fim de que todos os dados de informações particulares ou corporativos, contidos nos aparelhos informáticos ou eletrônicos, como bens jurídicos que são, sejam devidamente tutelados pela nossa legislação.

3.3. Tipicidade

Quando o sistema informático é utilizados de forma a causar danos a sistema informático de outrem, faz-se mister averiguar a conduta humana do ponto de vista da teoria do crime.

No entendimento de BRANDÃO[52], afirmando que a conduta humana é a pedra angular da Teoria do Crime, acrescenta que é com base na conduta humana que se formulam todos os juízos que compõem o conceito de crime: tipicidade, antijuridicidade e culpabilidade. A tipicidade como adequação da conduta com a norma; a antijudicidade como juízo de reprovação da conduta, e culpabilidade como juízo de reprovação sobre o autor da conduta. O Direito penal não cria o conceito de conduta, ele o retira do mundo dos fatos. Assim, a ação e a omissão são, na verdade, modalidades da conduta humana. Não se pode, pois, pensar em vida humana sem o agir.

Então, o conceito de conduta, retirado dos fatos, funciona como um elo de ligação entre os elementos do crime, possibilitando a sistematização desses elementos. Portanto, deve-se enfatizar que todos os elementos do crime referem-se, de um modo ou de outro, à conduta

---

[51] JUSBRASIL. Disponível em: http://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lei-n-12737-12-art-154-a-do-codigo-penal. Acesso em 04.06.2015.

[52] BRANDÃO, Cláudio. Curso de direito penal: parte geral – 2. ed. Cláudio Brandão – Rio de Janeiro: Forense, 2010, p.135-136.

humana. A necessidade da existência de uma conduta para a constituição do conceito de crime, fato hoje tido como óbvio, é uma grande conquista de um direito penal liberal, voltado para a proteção dos bens jurídicos vitais para o homem e a sociedade. Todavia, em tempos remotos, o direito penal prescindiu do conceito de conduta para aplicar a pena, desse modo, até coisas e animais poderiam ser punidos.

Prosseguindo, o autor coloca que tipicidade é uma relação de adequação da conduta humana e o tipo penal. As condutas que não se enquadram num tipo são penalmente irrelevantes. A tipicidade determina o âmbito de liberdade de ação. Caso a ação seja descrita como crime por um tipo sofrerá uma sanção; se a ação não for descrita como crime não haverá consequência penal.

Daí, com base nos ensinamentos acima, pode-se verificar que, apesar do tratamento dispensado ao tema focar em sistemas cibernéticos, não há de se relegar o fato de que, em verdade, analisa-se a conduta humana na utilização desses sistemas, a fim de verificar se tal conduta é adequada do ponto de vista penal, para evitar a violação dos bens jurídicos indispensáveis ao ser humano e a sociedade. E, aqui, esses bens jurídicos envolvem os sistemas informáticos, os quais contêm dados relativos à liberdade de expressão, individualidade, intimidade e privacidade de seres humanos.

A violação a esses bens jurídicos vai atrair a necessária tutela estatal, punindo as condutas humanas, atentando para o princípio da legalidade: *nullum crimen, nulla poena sine lege;* ao princípio da tipicidade, que é a conduta humana perfeitamente adequada ao modelo descrito na lei; e ao elemento do crime chamado de antijuridicidade, que significa a existência na conduta humana de um juízo de valor negativo, ou desvalor, que qualifica o fato como contrário ao Direito.[53]

Frisa-se que, não importa se a invasão foi para espionar, capturar, alterar ou publicar. O sigilo individual e profissional é garantia constitucional, levando à conclusão de que a transgressão a esses bens deveriam ser mais severamente tutelados, o que tornaria a Lei n.º 12.737/2012 eficaz, sem tantas lacunas.

Pois, numa sociedade global constantemente tensa por ataques ditos terroristas, francos atiradores em escolas, pais que encarceram e mantém filhas como escravas sexuais por décadas, violações de intimidade, quebras de direitos fundamentais por policiais, operações secretas de

---

[53] BRANDÃO, Cláudio. Curso de direito penal: parte geral – 2. ed. Cláudio Brandão – Rio de Janeiro: Forense,2010, p.128-129.

espionagem e contra espionagem até mesmo de chefes de governo, guerras e conflitos armados e diante de uma grande instabilidade econômica, o direito penal tem cada vez mais sido chamado como arma principal de contenção e prevenção de violências, numa inversão lógica do princípio da *ultima ratio*. Mas a resposta que o direito penal dá é sempre radical: para mais segurança, é necessário diminuir certas garantias, certas liberdades e relativizar certos princípios. O próprio Presidente dos Estados Unidos da América do Norte, Barack Obama, manifestou-se dizendo que "quem quer segurança deve abrir mão da privacidade".[54]

O Estado tem o poder-dever de proteger os cidadãos de danos ocorridos quando da prática de delito ou crime. Essa afirmativa tem amparo no princípio da legalidade (CF Art. 5º, XXXIX), que impõe a clareza, taxatividade e proporcionalidade das penas contidas nas normas coibitivas de delitos e crimes).

3.4. Consumação e tentativa

Considerando-se a previsão legal, o crime de invasão é formal. Daí, a sua consumação ocorre com o sucesso da invasão, ainda que o agente não consiga, por motivos alheios a sua vontade, obter seu intento de alterar, destruir ou publicar os dados encontrados. Frisa-se que, mesmo que o agente não consiga auferir vantagem ilícita com a invasão, dá-se a consumação da ação do agente.

Deve-se perquerir, então, quais foram as consequências danosas dessa invasão. Deve-se levar em consideração o resultado do procedimento invasivo, no sentido de saber se o agente invadiu dispositivo robusto de seguraçã ou se, simplesmente, encontrou o sistema de proteção deficitário, negligenciado ou imprudentemente vulnerável. Pois, lembra-se que a Lei n.º 12.737/2012 prevê punição para as invasões que se encaixam no tipo penal de invasão de dispositivo de segurança.

Percebe-se que, sempre que o agente tem acesso não autorizado a sistemas informáticos sem autorização do titular do sistema, conclui-se que a atitude é, teoricamente, mais simples de ser enquadrada como criminosa, pois basta comprovar que o intento do agente foi o de obter vantagem ilícita, agindo de forma a alterar os dados obtidos, causando destruição dos mesmos, deixando-os vulneráveis ou publicando-os.

---

[54] REVISTA BRASILEIRA DE CIÊNCIAS CRIMINAIS. O bem jurídico nos crimes informáticos. Spencer Toth Sydow. Vol. 113/2015, p. 193 - 212 | Mar - Abr / 2015. DTR\2015\3604.

Segundo MILAGRE[55], para um grupo de juristas, a "espiada" não seria crime, só se falando em obtenção nos casos de cópia dos dados do dispositivo, ou quando o agente entra na "posse dos dados". Para outra corrente, o simples acesso a dados (um *select* na tabela da vítima, por exemplo) já agride o bem jurídico protegido pelo Direito Penal, e demonstra a "intenção em obter dados" eis que já permite ao *cracker,* em certos casos, se beneficiar das informações, de modo que tal "contato" com os dados estaria inserido no contexto do "obter dados", previsto no tipo penal. O agente que faz o *footprinting* (levantamento de informações do alvo) através de *nmap* ou outro *scanner,* verificando se o alvo está ativo, as vulnerabilidades do sistema, portas abertas, serviços desnecessários rodando, sistema operacional, dentre outros, em tese não comete crime, pois atos preparatórios não são puníveis e o agente não chegou a dar início a invasão (ato executório). Assim, quem encontra vulnerabilidade em sistema alheio, mesmo sem autorização para pesquisa, e comunica o administrador, está sendo responsável, não podendo incidir, *a priori,* nas penas o artigo 154-A, agora previsto no Código Penal.[56]

A mera detecção de execução não pode ser considerada crime caso o agente não tenha se utilizado de ferramentas tais que lhe possibilitasse o acesso danoso ao sistema informativo em vista. É o estudo da intenção e do modo de utilização de técnicas do invasor que dirá qual o seu comprometimento e quão o mesmo estava habilitado a invadir e, consequentemente, causar dano ao sistema visado.

A tentativa de invasão, quando o agente consegue invadir, mas não chega a causar danos, não obtém nenhuma vantagem, isso devido a existência de dispositivos de detecção de execução, não deve ser considerada crime, pois, de acordo com a doutrina do *iter criminis*, não se pune, via de regra, a mera preparação para o crime.

Também pode ocorrer tentativa de invasão sem caracterizar crime cibernético, quando o próprio titular do dispositivo violado consente em fornecer dados, ainda que tenha agido por perspicácia do invasor. Muitas vezes é o próprio dono do sistema que se deixa enganar movido por promessas de vantagens caso libere as informações solicitadas. Se tal circunstância ocorrer e o titular do dispositivo vier a sofrer dano por engendros maliciosos do invasor, o crime poderá ser punido com enquadramento diverso daquele que seria relativo a invasão danosa de dados informáticos. A simples invasão não causou danos, mas o dano ocorreu em razão da obtenção

---

[55] MILAGRE, José Antonio. Invasão de dispositivo com senha nem sempre é crime. Disponível em: http://www.conjur.com.br/2013-abr-01/jose-milagre-invasao-dispositivo-senha-nem-sempre-crime. Acesso em 24.08.2015.

[56]

de dados por uso de artifício mentiroso do agente que lucrou com a ausência de desconfiança da vítima. Nesse caso, o agente não alterou e nem destruiu dados informáticos, mas utilizou os dados obtidos por meio de perícia criativa para enganar o titular do sistema. O agente, então, fica sujeito ao seu enquadramento em delitos previstos no Código Penal, a depender do dano causado.

Acredita-se ser preciso uma legislação especial para tratar do Crime Digital, uma vez que a lei deve ser mais específica para abarcar mais possibilidades presentes no contexto da era digital, além de que, as penas devem ser repensadas. Sugere-se ainda a criação de uma polícia própria para o mundo virtual, com o intuito de mudar o pensamento de que a Internet é uma "terra sem lei e sem dono". Dessa forma, as condutas criminosas devem ser coibidas, mas é preciso remodelar o direito em si e não permitir que a epidemia do crime no mundo virtual continue em silêncio.[57]

A questão é que, a Lei n.º 12.737/2012, não deixa margem para imputar como criminosa a conduta de quem simplesmente invande um sistema informátivo. Para a legislação em comento, o dispositivo informático deverá estar protegido por sistema de segurança. E, entende-se que, não basta proteger o acesso com senhas. A lei somente pune a invasão a sistema que se considera sofisticado ou, no mínimo, bem elaborado. Isso leva-se à conclusão de que a Lei em análise não abrange os crimes cibernéticos com eficiência. A nossa legislação está a exigir que o titular faça sua própria segurança, não punindo invasores de sistema com proteção elementar. A lei deixa espaço para os criminosos atuarem com impunidade contra aqueles titulares mais vulnerários, ou seja, contra aqueles que estão mais sujeitos a sofrer danos sem possibilidade de instrumento legal de reparação dos seus prejuízos.

[57] Os crimes digitais sob a vertente do Código Penal. Brasileiro. Dayane Karla Barros de Farias Duarte; José Armando Ponte Dias Junior. Revista dos Tribunais Nordeste. Vol. 7/2014, p. p. 277 – 291/ Set - Out / 2014. Revista dos Tribunais Nordeste. Vol. 8/2014, p. 227 – 291/Nov - Dez / 2014. DTR\2014\21275.

4 – CONCLUSÃO

Para a conclusão do primeiro capítulo desta obra, foi importante destacar os itens a serem analisados nos demais capítulos, tais como: A) A problemática existente na lei 12.737/2012, em virtude de conter previsão de criminalização e punição de invasão apenas a aparelho informático que possua sistema de segurança, deixando sem amparo os demais aparelhos virtuais; B) A Justificativa deste trabalho científico como sendo, primordialmente, tipificar os possíveis delitos informáticos, sua evolução e suas espécies; C) A indagação de que: Diante dessa expansão da internet e a carência da lei 12.737/2012 é possivel em determinado crime cibernético o agente ficar impune?; D) A resposta, no sentido de que: A hipótese de invasão de aparelhos cibernéticos não protegidos com sistema sofisticado de segurança, causando prejuízos morais e/ou econômicos à vítima, não é considerada delito. O bem jurídico violado fica sem a tutela estatal; . E) A indicação do objetivo geral deste trabalho, que, no caso, é falar da criação do computador e da internet, dos crimes cibernéticos, evolução, espécies, casos concretos de vítimas de invasão virtual, legislação existente, notadamente a Lei n.º 12.737/2012 – Lei Carolina Dieckmann, do bem jurídico tutelado, apontamentos sobre consumação e tentativa, e a conclusão da análise do tema.

Quando da conclusão do segundo capítulo deste trabalho, importou especificar os crimes cibernéticos, que tiveram início a partir dos denominados "vírus", os quais ainda trazem transtornos para os usuários, pois agentes maliciosos viram na internet um meio fértil para suas ações delituosas, sendo o vírus de computador uma ferramenta que permite o acesso aos dados dos usuários. Importou, ainda, salientar que: os sistemas virtuais são cada vez mais utilizados, e mais vírus aparecem, causando sérios transtornos e prejuízos morais e/econômicos aos usuários; que a internet, como verdadeira revolução na informática, passou a servir para discurso de ódio, ações de pedofilia, de pornografia, de xenofobia, de homofobia, de discriminação contra negros, contra mulheres, contra nordestinos, além de outras intolerâncias criminosas. Tratou-se da evolução dos crimes cibernéticos, a qual teve seu início a partir da Guerra Fria entre os Estados Unidos e a Rússia, nos anos de 1960 e expandiu-se para as universidades, órgãos públicos, e, atualmente, é globalizada. Falou-se das espécies de crimes cibernéticos, tais como: *Trojan Horse* (Cavalo de Tróia); *phishing,* que, fazendo-se passar por terceiro, prejudica a vítima, com arquivos arquivos informáticos infectados por *softwares* daninhos, que capturam ou copiam dados; *Spywares,* que são programas espiões que enviam

informações do computador do usuário para desconhecidos na rede, além de outros tipos, uma grande quantidade, sempre em crescimento.

Por ocasião da conclusão do terceiro capítulo deste trabalho, foi importante adentrar no tratamento legislativo no Brasil dos crimes cibernéticos, falando sobre a proteção quando do uso da informática, tratada na Convenção de Budapeste, a qual o Brasil não assinou; ressaltando as iniciativas legislativas brasileiras, tais como: as leis sobre proteção da propriedade intelectual (Lei .º 7.646/87); Lei n.º 12.737/2012 – Lei Carolina Dieckmann, que trata sobre invasão de dados informáticos, telemáticos e outros aparelhos eletrônicos; Lei n.º 11.829/2008, sobre pornografia infantil; Lei n.º 12.965/2014 – Marco Civil da Internet, para garantir a privacidade dos usuários de empresas que atuam na *Web;* e, ainda, foi importante frisar que existe Projeto de Lei (494/2008) – Internet Legal, já aprovada no senado, para melhorar a proteção aos usuários de aparelhos virtuais. Foi importante, também, analisar o bem jurídico tutelado, sob o prima da privacidade e intimidade; Apontar a tipicidade dos crimes cibernéticos, como a conduta humana que se enquadra na descrição de crime contida na lei. Importante, ademais, foi importante verificar, no item consumação e tentativa, que os crimes cibernéticos seguem as especificações do *iter criminis,* ou seja pode haver preparação, execução, consumação e mera tentativa.

Neste quarto capítulo, chega-se á conclusão do tema enfrentado, no sentido de que a Lei n.º 12.737/2012, criada a partir do incidente de invasão da privacidade do conteúdo do e-mail da atriz Carolina Dieckamn, não proveu a legislação brasileira de um instrumento eficiente para desestimular os invasores de aparelhos eletrônicos alheios. Para entender o por que de não termos, ainda, uma legislação que criminalize eficazmente as invasões virtuais, aponta-se a ideia que se teve de punir apenas as invasões em aparelhos com sistema *top* de segurança dos dados virtuais sem autorização da vítima, sem tipificar a ação do agente oportunista que invada o aparelho informático de uma vítima desprevenida.

O legislador tem que atinar para o fato de que os crimes cibernéticos são cometidos por agentes que possuem habilidades avançadas no campo da informática, e atuam no exercício do mal, para causar dano econômico, para vingança com as próprias mãos, implantando ofensas e xingamentos à vítima, para difundir e arregimentar adeptos para compactuar com ideias racistas, sexistas, nazistas e outras intolerâncias criminosas, ou simplesmente como diversão, apenas para mostrar poder e, nesse caso, também, não deixa de praticar crime, pois essa "brincadeira" causa insegurança e desconforto ao usuário atingido pela invasão.

É imprescindível que Estado atente para a necessidade de reprimir, de forma eficaz e severa, a ação dos agentes que se especializam em praticar o terror virtual.

O legislador deve criminalizar toda invasão à dispositivo tecnológico, mesmo aquele que não possua um sistema *top* de segurança. No Direito Penal, por exemplo, é crime roubar ou furtar, a despeito do tipo de fechadura que possua a porta de acesso ao bem subtraído.

A Lei n.º 12.737/2012 – Lei Carolina Dieckmann -, não criminalizou invasões a aparelhos sem sistema de segurança. A lei em causa serve como ponto de partida nos muitos passos que o legislador deve dar para alcançar o ideal de segurança no meio virtual.

A invasão de computadores e dispositivos similares, com finalidades ilícitas, traz sérios prejuízos às pessoas físicas ou jurídicas. Daí porque, acredita-se que é carente a lei Carolina Dieckmann, por ter sido editada para aplacar o clamor público ante a divulgação do ilícito na mídia e por haver atingido uma pessoa pública. No item proteção aos usuários de aparelhos tecnológicos, deixou a desejar por não prever as situações de captação de dados cadastrais ou visuais de aparelhos eletrônicos sem sistema sofisticado de segurança.

O usuário de sistemas informáticos, de acordo com a Lei n.º 12.737/2012, pode vir a suportar sozinho, sem a tutela estatal para protegê-lo, quando da invasão de aparelho tecnológico que não possua sistema *top* de segurança, por agente muito esperto em informática, que venha a roubar os seus dados, para fins de extorsão ou desmoralização, levando-o a sofrer prejuízo econômico ou à desonra perante terceiros, num verdadeiro desrespeito à dignidade da pessoa humana. As leis brasileiras atuais, inclusive a Lei Carolina Dieckmann, não bastam para desacelerar o aumento desenfreando dos crimes cibernéticos no Brasil. A lei de que a sociedade está necessitando para fins de poder utilizar os meios tecnológicos sem tanto temor como ocorre atualmente, deve ser clara e severa, com penas adequadas aos crimes cibernéticos, a fim de desestimular os agentes maliciosos na prática do mal.

5 - REFERÊNCIAS

BONFIM, Edilson Mougenot. Direito penal, 2: parte especial. Edilson Mougenot Bonfim. 3.ª ed. – São Paulo: Saraiva, 2007, p. 99.

BRANDÃO, Cláudio. Curso de direito penal: parte geral – 2. ed. Cláudio Brandão – Rio de Janeiro: Forense, 2010, p. 125-128; 27-28; 67-68; 135-136; 128-129.

BRITO, Alexis Couto de. Execução penal. Alexis de Couto Brito. 3.ª ed. – São Paulo: Editora Revista dos Tribunais, 2013, p. 140.

BULOS, Uadi Lammêgo. Curso de direito constitucional. Uadi Lammêgo Bulos. São Paulo: Saraiva, 2007, p. 428-429; 403-404.

CUNHA JÚNIOR, Dirley. Curso de direito constitucional. Edições Podium: Bahia, 2008, p. 529.

PRADO, Luiz Regis. Direito penal econômico. Luiz Regis Prado. – 5.ª ed. – São Paulo: Editora Revista dos Tribunais, 2013, p. 116.

WENDT, Emerson. Crimes cibernéticos: ameaças e procedimentos de investigação. Emerson Wendt. 2.ª ed. – Rio de Janeiro: Brasport, 2013, p. 8-9; 18-19; 234.

IV ANUÁRIO BRASILEIRO DE DIREITO INTERNACIONAL. Jurisdição no Ciberespaço. Alexandre Atheniense. ANO IV. V. 2, 2013, p. 99 – 112.

BONIJURIS Revista. Delitos cibernéticos: implicações da lei 12.737/12. Wanderlei José dos Reis. ANO XXVII, fevereiro 2015, , n. 615, v. 27, n. 2, www.bonijuris.com.br **7**

DOUTRINAS ESSENCIAIS DE DIREITO CONSTITUCIONAL. O direito fundamental à privacidade e à intimidade no cenário brasileiro na perspectiva de um direito à proteção de dados pessoais. Andrey Felipe Lacerda Gonçalves; Monique Bertotti; Veyzon Campos Muniz. Vol. 8/2015 | p. 597 - 614 | ago / 2015.DTR\2015\11488

DUC IN ALTUM, Revista. Considerações sobre os requisitos da ação para a legítima defesa. Leonardo Siqueira. Caderno de direito, vol. 4, n.º 6, jul-dez, 2012, p. 244. Disponível em: file:///C:/Users/LCP/Downloads/170-596-1-PB%20(3).pdf. Acesso em 21.11.2015.

EXAME, Revista. Internet: cada marca no seu quarto. Marcio Orsolini. ANO 44. Edição 966, n.º 7, de 21.04.2010, p. 70.

REV. FAC. DIREITO UFMG, Belo Horizonte. Crimes cibernéticos: o descompasso do estado e a realidade. David Augusto Fernandes. . , n. 62, pp. 139 - 178, jan./jun. 2013.

RDC - Revista Científica Direitos Culturais. Revista Científica Direitos Culturais. Discurso de ódio na internet e multiculturalismo: uma questão de conflito entre liberdade de expressão versus dignidade da pessoa humana. Rosane Leal da Silva; Letícia Almeida de la Rue; Danielli Gadenz. – , v. 9 – n. 18 – Maio/Agosto/2014 – p. 129-151.

REVISTA BRASILEIRA DE CIÊNCIAS CRIMINAIS. O bem jurídico nos crimes informáticos. Spencer Toth Sydow. Vol. 113/2015 | p. 193 - 212 | Mar - Abr / 2015. DTR\2015\3604.

REVISTA DOS TRIBUNAIS NORDESTE . Os crimes digitais sob a vertente do Código Penal Brasileiro. Dayane Karla Barros De Farias Duarte; José Armando Ponte Dias Junior. Vol. 7/2014 | p. 277 – 291. Set - Out / 2014. Vol. 8/2014 | p. 227 - 291 | Nov - Dez / 2014.DTR\2014\21275.

SCIENTIFIC AMERICAN, Brasil. Nosso futuro transparente. Daniel C. Dennett; Deb Roy. ANO 13, n.º 155, abril/2015, p. 65; 67.

SOCIOLOGIA, Revista. Mídias sociais: rumo à democracia participativa?. ANO IV – Edição 37 – outubro/novembro/2011.

ÂMBITO JURÍDICO. O sigilo de dados no meio virtual. Maria dos Remédios Calado. Disponível em: http://www.ambito-jurídico.com.br/site/index.php?nlink=revistaartigosleitura&artigoid=9528. Acesso em 22.09.2015.

CULTURA DIGITAL. Marco civil da Internet entra em vigor. ANO 2014. Disponível em: http://culturadigital.br/marcocivil/. Acesso: 18.09.2015.

GLOBONEWS40. Sem fronteira. Jorge Pontual/10.09.15, 23:30h. ANO 2015.

INTERNET LEGAL. Senado aprova projeto que regula armazenamento de dados de usuários da internet. ANO 2015. Disponível em: http://www.internetlegal.com.br/2015/07/senado-aprova-projeto-que-regula-armazenamento-de-dados-de-usuários-da-internet/

JUSBRASIL. Disponível em: http://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lei-n-12737-12-art-154-a-do-codigo-penal. Acesso em 04.06.2015.

MARIACAROL. Crimes virtuais e segurança. Disponível em: <http://paraentender.com/internet/crimes-virtuais>. Acesso em 02.06.2015.

_____. _____. p. 10-11.

MILAGRE, José Antonio. Invasão de dispositivo com senha nem sempre é crime. Disponível em: http://www.conjur.com.br/2013-abr-01/jose-milagre-invasao-dispositivo-senha-nem-sempre-crime. Acesso em 24.08.2015.

NORTON BY SYMANTEC. O que é crime cibernético? ANO 1995-2015. Disponível em: <http://br.norton.com/cybercrime-definition>. Acesso em 02.06.2015.

PINHEIRO, Emeline Piva. Crimes virtuais: uma análise da criminalidade informática e da resposta estatal. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/ 29397-29415-1-PB.pdf. Acesso em 03.06.2015.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. ANO 2002.Revista Jus Navigandi, Teresina, ano 7, n. 58, 1 ago. 2002. Disponível em: <http://jus.com.br/artigos/3186/o-problema-na-tipificacao-penal-dos-crimes-virtuais>. Acesso em 03.06.2015.

SCOLANZI, Vinícius Barbosa. Bem jurídico e Direito Penal**.** Revista Jus Navigandi, Teresina, ano 17, n. 3129, 25 jan. 2012.< http://jus.com.br/artigos/20939>. Acesso em 02.06.2015.

UOL tv e famosos. Golpe envolvendo programa de xuxa expõe centenas de celulares no FACEBOOK. ANO 2015. <http://tvefamosos.uol.com.br/noticias/bbc/2015/09/23/golpe-envolvendo-programa-de-xuxa-expoe-centenas-de-celulares-no-facebook.htm>. Acesso em 23.09.2015.

_____._____. Abalada, mulher de Stênio Garcia fala sobre fotos íntimas vazadas: "Estou com vergonha". Disponível: http://entretenimento.r7.com/famosos-e-tv/abalada-mulher-de-stenio-garcia-fala-sobre-fotos-intimas-vazadas-estou-com-vergonha-30092015. Acesso em 1.º.10.2015.

_____._____. Olhar digital. Disponível em: http://olhardigital.uol.com.br/noticia/5-pontos-essenciais-para-entender-o-marco-civil-da-internet/41053. Acesso em 18.09.2015.

WIKIPEDIA. Crime informático. ANO 2013. Disponível em: <http://pt.wikipedia.org/wiki/Crime_inform%C3%A1tico>. Acesso em 02.06.2015.