UNIVERSIDADE FEDERAL DE CAMPINA GRANDE – UFCG

CENTRO DE CIÊNCIAS JURÍDICAS E SOCIAIS – CCJS

UNIDADE ACADÊMICA DE DIREITO

BÁRBARA BIRNEY SILVA DANTAS

A INEFICÁCIA DA LEI 12.737/2012 EM FACE DO AVANÇO DA CRIMINALIDADE DE INFORMÁTICA

SOUSA

2014

BÁRBARA BIRNEY SILVA DANTAS

A INEFICÁCIA DA LEI 12.737/2012 EM FACE DO AVANÇO DA CRIMINALIDADE DE INFORMÁTICA

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande, como exigência parcial para obtenção do título de Bacharel em Ciências Jurídicas e Sociais.

Orientador: Ms. Iarley Pereira de Sousa.

SOUSA

2014

BÁRBARA BIRNEY SILVA DANTAS

A INEFICÁCIA DA LEI 12.737/2012 EM FACE DO AVANÇO DA CRIMINALIDADE DE INFORMÁTICA

Trabalho de conclusão de Curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande, como exigência parcial para obtenção do título de Bacharel em Ciências Jurídicas e Sociais.

Aprovado em ____/____/____

_____
Orientador

_____
Primeiro Examinador

_____
Segundo Examinador

SOUSA

2014

Aos meus pais, Geraldo Birney e Márcia Dilene, que sempre me dedicaram seu amor, fé e companhia, vibrando junto comigo em todas as vitórias e me concedendo diariamente seu bem-vindo apoio em todos os momentos de minha vida.

AGRADECIMENTOS

A Deus, por me fazer forte e determinada na busca dos meus sonhos, por me presentear com a saúde e a sorte de concluir mais uma etapa de vida, por me dar a honra de fazer parte de uma família maravilhosa e por ter posto em minha vida amigos, cuja simples existência basta para me fazer feliz.

Aos meus pais, que trabalharam durante todos esses anos e não pouparam esforços para investir no que fosse necessário ao meu crescimento pessoal e profissional, e principalmente, me ensinaram o significado de amor incondicional.

A João Paulo de Sousa Pereira, por ter sido meu refúgio, me apaziguado com sua paz de espírito, positividade e principalmente, por ter construído comigo um amor memorável.

A todos os meus amigos, a família que eu escolhi, que eu tanto amo e que com cada gesto de carinho, atenção e bons conselhos se tornaram parte de mim.

À família CCAA Sousa e a todos os meus alunos, que me agraciaram com a mágica de ensinar, aprender e amar o trabalho pelo seu próprio valor.

A Dr. José Cirilo Fernandes Neto e toda a equipe do seu escritório que me ofereceu a oportunidade de tomar conhecimento sobre o real mundo da advocacia.

A todos os funcionários da 8ª Vara da Justiça Federal da Paraíba, que me acompanharam e me auxiliaram no desempenho da importante função de Juíza Conciliadora.

Aos professores do CCJS, CERS e CEJUS, especialmente meu orientador Ms. Iarley Pereira de Sousa, que contribuíram para a minha formação com sua paciência, vasto conhecimento e exemplo de vida.

Aos meus colegas com quem dividi as salas, as dúvidas e as experiências do Curso de Direito.

Aos membros do Karatê Askasa, companheiros na busca do equilíbrio material e espiritual.

Por fim a todos os demais, que expressamente ou em silêncio torceram por meu sucesso, me presentearam com um sorriso sincero, uma palavra amiga ou um ato de bondade.

"Há muito tempo que o meu axioma é de que as pequenas coisas são infinitamente as mais importantes."

(Sir Arthur Conan Doyle)

RESUMO

O presente trabalho se propõe a analisar o panorama da criminalidade informática no Brasil e o respectivo tratamento legal aplicado, tendo por objetivo geral averiguar a necessidade de revisão da lei 12.737/2012, para torná-la eficaz dentro do ordenamento jurídico brasileiro. É inegável que o avanço tecnológico permitiu a integração do Brasil ao mundo globalizado em diversos aspectos. A maior bandeira da globalização e do avanço tecnológico está fincada na Internet. Porém, pelas próprias características do meio, vislumbra-se também um terreno novo e convidativo para a prática de delitos e fraudes que, como sabido, não ocorrem só no Brasil. Como decorrência, assiste-se de imediato o relevante impacto das novas tecnologias nas regulamentações jurídicas, em especial no Direito Penal. A análise acerca da criação de leis penais que envolvem tecnologia da informação, mais precisamente a Lei 12.737/2012 deve ser feita com extrema cautela, especialmente quanto à finalidade e eficácia. Assim, o problema que originou essa pesquisa é a criação legal que já entrou no ordenamento jurídico brasileiro em atraso. Para se chegar aos fins pretendidos por esse trabalho, utiliza-se a pesquisa de natureza aplicada, abordagem qualitativa, bibliográfica-documental e exploratória, bem como dos seguintes instrumentos: coleta de dados documental e análise de conteúdo, através de método de abordagem dedutivo e dos métodos de procedimento comparativo e estudo de caso. No primeiro capítulo conceituam-se os crimes informáticos e discorre-se sobre sua terminologia e classificação doutrinárias, bem como se trata dos seus sujeitos ativos e dos crimes mais comumente praticados. No segundo capítulo comenta-se a Lei 12.737/2012 e seus respectivos dispositivos legais, mostrando as consequências práticas da tipificação criminal nela presente. No terceiro capítulo utiliza-se o direito comparado, a fim de expor o tratamento da matéria nas legislações de outros países. Apresenta-se como hipótese a implementação da proporcionalidade entre a gravidade da sanção penal e o objeto tutelado pela norma incriminadora, bem como a modificação de condicionantes do objeto do tipo, que não confundam a configuração do crime, do contrário, torne sua expressão mais abrangente.

Palavras-chave: Crimes informáticos. Lei 12.737/2012. Ineficácia.

ABSTRACT

This study aims to analyze the landscape of cybercrime in Brazil and its legal treatment, with the overall objective to determine the need for revision of the law 12.737/2012 to make it effective within the Brazilian legal system. It is undeniable that technological advancement has enabled the integration of Brazil into the globalized world in many aspects. The larger flag of globalization and technological advance is stuck in the Internet. However, its characteristics also glimpses a new and inviting way to commit irregularities and fraud which, as known, occur not only in Brazil. As a result, we are witnessing the immediate material impact of new technologies on legal regulations, in particular the Criminal Law. The analysis about the creation of criminal laws involving information technology, specifically the Law 12.737/2012 should be taken with extreme caution, especially regarding the purpose and effectiveness. Thus, the problem that originated this research is the legal creation that has entered the Brazilian legal system to late. To get to the purposes intended by this work, we use the research of an applied nature, documentary literature and exploratory qualitative approach, as well as the following instruments: collecting data and document content analysis through deductive method of approach, and methods of procedure and comparative case study. The first chapter conceptualize computer crime and talks about his doctrinal terminology and classification, as well as the case of its subjects and crimes most commonly practiced. The second chapter talks about Law 12.737/2012 and its respective legal provisions, showing the practical consequences of this criminal typing it. The third chapter uses comparative law, in order to expose the treatment of the subject in the laws of other countries. Presents itself as the hypothesis the implementetion of proportionality between the seriousness of the criminal sanction and the object protected by the rule, as well as the modification of all constraints of the rule in order not to confuse the configuration of the crime, but become its expression most comprehensive.

Keywords: Computer Crimes. Law 12.737/12. Inefectiveness.

SUMÁRIO

1 INTRODUÇÃO 10

2 CRIMES INFORMÁTICOS: CONCEITO E FUNDAMENTAÇÃO LEGAL 13

2.1 Conceito e terminologia dos crimes informáticos 13

2.2 Classificação dos crimes informáticos segundo a doutrina. 15

2.3 SUJEITOS 17

2.3.1 Tipos de hackers/crackers 18

2.3.2 Engenharia Social 21

2.4 CRIMES EM ESPÉCIE 23

2.4.1 Crimes Impróprios de Informática 23

2.4.2 Crimes próprios de informática 26

3 ANÁLISE DOS DISPOSITIVOS LEGAIS DA LEI 12.737 DE 30 DE NOVEMBRO DE 2012 E SUAS CONSEQUENCIAS PRÁTICAS 30

4 OS CRIMES INFORMÁTICOS NO ORDENAMENTO JURÍDICO DE ESTADOS ESTRANGEIROS 39

4.1 Os crimes informáticos no ordenamento jurídico dos Estados Americanos 39

4.2 Os crimes informáticos no ordenamento jurídico dos Estados Europeus 42

5 CONSIDERAÇÕES FINAIS 54

REFERÊNCIAS 57

1 INTRODUÇÃO

O corrente trabalho visa investigar o tratamento legal da criminalidade informática no ordenamento jurídico brasileiro, tomando por base a Lei 12.737/2012, a qual foi criada tardiamente e passou a tratar de crimes informáticos com delonga em relação a outros países, necessitando, por esta razão, se atualizar para se tornar eficaz na prevenção contra esses crimes, através da implantação do equilíbrio entre pena e objeto amparado pela norma criminal e da alteração das condicionantes do tipo penal de maneira que não causem embaraços à identificação da conduta criminosa, e sim, amplie sua manifestação.

Atualmente, o mundo virtual vem crescendo vertiginosamente. Há uma grande massa de usuários que pagam suas contas, fazem suas compras e se comunicam online. O direito deve se adequar ao desenvolvimento social, elaborando novas normas que regulam as relações no ambiente virtual. Porém, é cediço que à medida que se desenvolve a Internet, também aumenta o seu uso indevido.

Os denominados criminosos cibernéticos se valem da engenharia social, incorrendo em crimes de pirataria informática, acesso indevido, sabotagem bancária, fraude, entre outros, agindo com extremo grau de especialização técnica para a prática de tais delitos, de modo que já existem até organizações criminosas voltadas ao planejamento e execução de atos ilícitos via Internet, inclusive em nível global.

De acordo com Alexandre Jean Daoun e Gisele Truzzi de Lima, a doutrina penal brasileira e os tribunais pátrios conceituam crimes informáticos como toda ação típica, antijurídica e culpável cometida através do processamento automático de dados ou mesmo contra sua transmissão[1].

Segundo Samuel César da Cruz Júnior, a proteção do meio cibernético está ligada as formas de ataque utilizadas, pois as práticas criminosas dependem do quanto o sistema atacado é vulnerável, tanto que a própria defesa do sistema só é eficiente se constantemente atualizada para combater as novas ameaças que continuamente surgem[2].

---

[1]DAOUN, Alexandre Jean; LIMA, Gisele Truzzi de. **Crimes Informáticos: O direito Penal na Era da Informação**. Disponível em: < http://www.truzzi.com.br/pdf/artigo-crimes-informativos-gisele-truzzi-alexandre-daoun.pdf> Acesso em: 12 ago. 2013.

[2]JÚNIOR, Samuel César da Cruz. **A segurança e defesa cibernética no brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. Disponível em: < http://www.ipea.gov.br/portal/images/stories/PDFs/TDs/td_1850.pdf> Acesso em: 13 ago. 2013.

A partir daí nota-se que, em se tratando de uma atividade criminosa que muda continuamente, se faz necessário perceber que a atuação legislativa deve se conter à sua função de pensar no todo, deixando a cabo da jurisprudência toda a questão conceitual inerente a esses crimes, não podendo correr o risco de utilizar-se de técnica de conceituação tão rígida e específica que esvazie o conteúdo da norma ou dificulte sua aplicação às situações fáticas.

Assim, ao passo que cresce a criminalidade no meio virtual, vários países passam a promulgar leis que declaram ilegais novas práticas, por exemplo, a pirataria informática; passam também a atualizar leis relativas a crimes tradicionais, como o vandalismo, para que tais delitos também sejam tipificados no ambiente eletrônico, com vistas, principalmente, à proteção da utilização da informação processada pelos computadores. A Europa, por exemplo, há cerca de vinte anos, já tipificou condutas de violação bancária ou de mensagens pessoais, além da difusão de vírus.

Nesse contexto, foi editada no Brasil a Lei 12.737/2012, conhecida como Lei Carolina Dieckmann. Esta foi sancionada pela Presidente Dilma Rousseff em 3 de dezembro de 2012, promovendo alterações no Decreto-Lei 2.848 de 7 de dezembro de 1940-Código Penal Brasileiro, tipificando os crimes ou delitos informáticos.

A previsão desses delitos encontra-se sob o título de crimes contra a pessoa, visando o combate a qualquer afronta a sua privacidade ou à inviolabilidade dos seus segredos. Porém a lei merece críticas em virtude da amplitude e confusão de seus dispositivos que geram interpretação subjetiva, podendo ser utilizada como moldura para condutas vulgares e com isso, respaldando os reais grandes infratores cibernéticos, o que ressalta sua ineficácia e porque não dizer, injustiça.

A referida lei estabelece penalidades ínfimas de detenção ou de multa para violação grave à dispositivo informático. E quando estabelece pena de reclusão para condutas ainda mais sérias, como obtenção de segredo industrial, o *quantum* se encontra entre seis meses e dois anos e multa. Ademais, a literalidade da lei gera confusão, devido à sua amplitude, deixando à margem da sua aplicação, condutas graves e enquadrando condutas vulgares. Tudo isso aponta para sua ineficácia no combate aos crimes informáticos, devido a sua falta de técnica e atraso, necessitando de revisão.

Diante disso, cumpre registrar a urgência da adaptação da legislação brasileira ao desenvolvimento da criminalidade informática em toda sua amplitude, viabilizando e

assegurando a disponibilidade, a integridade, a confidencialidade e a autenticidade dos ativos de informações, que são valores tangíveis e intangíveis, imprescindíveis aos interesses do Estado e da Sociedade.

Ante esse panorama, o primeiro capítulo desse trabalho cuida de conceituar os crimes informáticos e apresentar sua terminologia, além de exibir sua classificação doutrinária, seus sujeitos ativos e trazer uma amostra condutas criminosas rotineiramente praticadas no meio virtual. O segundo capítulo traz Lei 12.737/2012 e seus dispositivos, focalizando os efeitos reproduzidos por sua tipificação criminal. O terceiro capítulo aplica o direito comparado, demonstrando como as legislações de outros países abordam os crimes informáticos, concluindo pela ineficácia da lei brasileira na prevenção quanto a tais delitos.

Para se atingir a finalidade aspirada por esse trabalho, emprega-se a pesquisa de natureza aplicada, abordagem qualitativa, bibliográfica-documental e exploratória, bem como dos seguintes instrumentos: coleta de dados documental e análise de conteúdo, através de método de abordagem dedutivo e dos métodos de procedimento comparativo e estudo de caso.

2 CRIMES INFORMÁTICOS: CONCEITO E FUNDAMENTAÇÃO LEGAL

Historicamente, desde os anos 60, há referências aos crimes informáticos, pela imprensa mundial e brasileira[3], sendo esses entendidos, como condutas ilícitas praticadas por meio de sistemas de computação e banco de dados, principalmente fraudes, sabotagem, espionagem e uso ilegal de sistemas. Porém, a partir dos anos 80[4], vieram a surgir os casos de vírus, "cracker" e pirataria informática, iniciando-se, nesse momento, as discussões a respeito da criminalidade informática.

Atualmente, em virtude do imenso e rápido avanço tecnológico, principalmente com a criação da "internet", bem como da acessibilidade à tecnologia, torna-se mais fácil e comum para qualquer pessoa física ou jurídica praticar ou ser vítima da prática de crimes informáticos cujos elementos se verão adiante.

2.1 Conceito e terminologia dos crimes informáticos

Ainda não há uma definição global do que vem a ser "crime informático" nem ao menos se essa seria a terminologia correta, variando de doutrinador para doutrinador, a amplitude do conceito, bem como a nomenclatura. No entanto, em um contexto geral, pode-se definir crime informático como a conduta ilícita praticada por meio de sistemas computadorizados ou contra esses, na qual o conhecimento informático do sujeito ativo leva a obter sucesso na sua realização.

De acordo com Paiva citado por Aguiar[5]:

> Apesar da discrepância doutrinária, são denominadas de "crimes de informática" as condutas descritas em tipos penais realizadas através de computadores ou voltadas contra computadores, sistemas de informática ou os dados e as informações neles utilizados (armazenamento ou processamento).

[3] KOHN, Aaron M. **Computer Criminals**. The Journal of Criminal Law, Criminology and Police Science. Chicago: Police Science, v.60: p. 1-2. Disponível em: < http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=5562&context=jclc > Acesso em: 01 mar. 2014.

[4] ROCHA, Marcelo Cavalcante. **Cultura Hacker - Tenha Ética E Ganharás Respeito**. Disponível em: < http://blog.marcelocavalcante.net/blog/2008/04/15/cultura-hacker-tenha-etica-e-ganharas-respeito/> Acesso em: 10 mar. 2014.

[5] PAIVA, 2006 APUD AGUIAR, 2009. p. 17.

Já para Corrêa, crimes informáticos seriam: *"Todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar."* [6] Observa-se que, nesse caso, o autor preocupou-se com os crimes efetivados contra o computador em si e o acesso indevido aos dados nele processados.

No entanto, para Ferreira (apud HIKAWA, 2008, p. 20)[7] crime informático *"é toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão"*. Nota-se, portanto, que esse é um conceito mais abrangente que envolve o computador, tanto como alvo da conduta criminosa quanto como instrumento para sua prática, afigurando-se mais completo, diante do fato da informática permitir não somente a prática de crimes novos, como também potencializar a prática de crimes tradicionais, a exemplo do furto.

Ainda para Roque[8], crime de informática é *"toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material."*.

Tomando por base as definições acima apresentadas, pode-se considerar que não há delimitação cristalina do crime informático, porém, pode-se identificar um denominador comum: a presença de dados, que são o objeto material do crime, o hardware, que constitui a parte física do sistema e o software, que constitui a parte lógica do sistema.

Quanto à terminologia, também não há unanimidade, divergindo os autores sobre qual nomenclatura seria a mais correta a ser empregada. Segundo Ivette Senise Ferreira (apud MARTINS, 2012, p. 5) [9]:

> As várias possibilidades de ação criminosa na área da informática, assim entendida no seu sentido lato, abrangendo todas as tecnologias de informação, do processamento e da transmissão de dados, originaram uma forma de criminalidade que, apesar da diversidade de suas classificações, pode ser identificada pelo seu objeto ou pelos meios de atuação, os quais lhe fornecem um denominador comum, embora com diferentes denominações nos vários países ou nos diferentes autores.

---

[6]CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. Saraiva: São Paulo, 2000.p.43
[7]FERREIRA, 2000 APUD HIKAWA. p.20
[8]ROQUE, Sérgio Marcos. **Criminalidade Informática – Crimes e Criminosos do Computador**. 1 ed. São Paulo: ADPESP Cultural, 2007. p.25
[9]FERREIRA, 2000 APUD MARTINS. p.5

Há autores, como por exemplo, Wendt & Nogueira que se utilizam da terminologia "crimes cibernéticos" ou "cibercrimes"[10]. No entanto, o Direito é uma ordem positiva e ideológica, cuja relevância material está nos meios sociais e biológicos que valora, o que não significa permitir-lhe a convivência no mesmo plano das coisas concretas por ele reguladas, como é o caso do mundo eletrônico, visto que não há um direito com vigência "cibernética" ou "virtual", por essa razão revela-se mais coerente a denominação "crimes informáticos". Tal discussão se assemelha bastante as denominações "Direito Penal" e "Direito Criminal", porém na prática ambas se apresentam irrelevantes, expostas apenas como questionamentos acadêmicos.

2.2 Classificação dos crimes informáticos segundo a doutrina.

Os crimes informáticos podem ser classificados de maneira bastante diversa. Na esteira de Vianna[11] os crimes de Informática podem ser:

a) impróprios – quando o computador é usado como instrumento para a execução do crime, porém não há ofensa à inviolabilidade dos dados nele contidos. Exemplo: difamação por meio da Internet;

b) próprios – aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade dos dados ou informações. Exemplo: Art. 313-A, do CP, Inserção de Dados Falsos em Sistema de Informações;

c) mistos – aqueles em que a norma visa tutelar a inviolabilidade dos dados e bem jurídico de natureza diversa. Exemplo: Art. 69, da Lei nº 9.100/95, Acesso não autorizado a sistema computacional eleitoral.

Maria de La Luz Lima (2003 apud LIBERATI. p.9) [12] classifica os delitos informáticos em três categorias:

---

[10]WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p. 18

[11]VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**. Disponível em: < http://www.academia.edu/1911160/Fundamentos_de_Direito_Penal_Informatico_do_acesso_nao_autorizado_a_sistemas_computacionais> Acesso em: 01 mar. 2014.

[12]LIMA, 2003 APUD Liberati, p.9

- Os que utilizam a tecnologia eletrônica como método, ou seja, crimes nos quais os sujeitos ativos utilizam métodos eletrônicos para obtenção do resultado;
- Os que utilizam a tecnologia eletrônica como meio, ou seja, crimes cuja realização depende do computador como instrumento;
- Os que utilizam a tecnologia eletrônica como fim, ou seja, crimes contra o próprio computador ou seus dados com a finalidade de danificá-los.

Luís Flávio Gomes (apud ARAS, 2009, on-line) [13] divide os crimes informáticos em duas categorias:

a) Crimes praticados contra o computador, em sentido amplo;

b) Crimes praticados por meio de computador.

Nessa mesma esteira, Damásio Evangelista de Jesus (apud ARAS, 2009, on-line) classifica os crimes informáticos também em duas categorias: 1) Crimes informáticos puros ou próprios: aqueles praticados por meio de um computador onde o resultado da conduta se opera em meio eletrônico, sendo a informática o bem jurídico protegido; 2) Crimes informáticos impuros ou impróprios: aqueles em que o sistema computacional funciona como ferramenta para a prática de condutas lesivas ao bem jurídico já protegido, não relacionado com a informática, produzindo resultado naturalístico que ofendem o mundo real[14].

Emerson Wendt e Higor Vinícius Nogueira Jorge[15] optaram por uma classificação que subdivide as condutas indevidas praticadas por computador em:

- Ações prejudiciais atípicas, que são as condutas praticadas na/através da rede mundial de computadores que causam transtorno e/ou prejuízo à vítima, porém não há uma previsão penal para as mesmas;
- Crimes Cibernéticos, esses últimos subdividindo-se mais uma vez em:

a) Crimes cibernéticos abertos, que são aqueles que podem ser praticados de forma tradicional ou por intermédio de computadores;

b) Crimes exclusivamente cibernéticos, que somente podem ser praticados com a utilização de computadores ou de outros recursos tecnológicos que permitam o acesso à internet.

Costa[16] ainda classifica os crimes informáticos em três grupos:

[13]GOMES, APUD ARAS, 2009.
[14]JESUS, APUD ARAS, 2009.
[15]WENDT; JORGE, 2012,p.19, passim.

- Crimes de informática puros, aquele pelo qual o sujeito ativo utiliza-se de um computador com a finalidade de atacar outro computador ou sistema informático especificamente, na definição:

> São aqueles em que o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas. Tal conduta, infelizmente, é a mais impune, pois não permite sua tipificação, na maioria das vezes, em nenhuma lei específica que puna tais delitos.

- Crimes de informática mistos, que não visam o sistema de informática em si, mas dele se utilizam como ferramenta para o delito. Ou seja: "*São todas aquelas condutas em que o agente visa a um bem juridicamente protegido diverso da informática, porém, o sistema de informática é ferramenta imprescindível a sua consumação*"[17];
- Crimes de informática comum: atos em que o agente utiliza o sistema de informática para a prática de crimes comuns, porém os mesmos poderiam ser praticados por qualquer outo meio. Resumindo:

> São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta a perpetração de crime comum, tipificável, na lei penal, ou seja, a via eleita do sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta. Um exemplo que ilustra perfeitamente esse tipo de crime é o Estelionato (Artigo 171 do Código Penal).[18]

Portanto, percebe-se que a despeito de propostas diferentes de classificação dos crimes informáticos, a classificação mais aceita é a que apresenta duas categorias: a dos crimes cometidos utilizando os recursos informáticos como instrumento, cuja tipificação já se encontra prevista no ordenamento penal tradicional e a dos crimes que ofendem ao sistema informático em si, em sua parte lógica, material ou passagem de dados.

2.3 SUJEITOS

---

[16]COSTA. Marco Aurélio Rodrigues da. **Crimes de Informática**. Jus Navigandi. Teresina, ano 1, nº 12, maio de 1997. p. 29.
[17]Ibid., p. 29.
[18]Ibid., p. 30.

Com a evolução da tecnologia digital, principalmente da Internet e sua difusão por todas as classes sociais e faixas etárias, vem se discutindo na mídia a invasão dos hackers (ou crackers) no meio virtual, sendo, inclusive comum encontrar vítimas das condutas desses indivíduos. Diante do avanço na acessibilidade e da velocidade da transmissão de dados, o meio virtual já passou a fazer parte do dia-a-dia das pessoas, até mesmo na realização de tarefas simples que atualmente não mais exigem o deslocamento para sua realização, pois podem todas ser executadas on-line.

Antes de mais nada, é preciso discutir a má utilização dos termos "hacker" e "cracker", veiculada na mídia. O hacker é o termo utilizado para designar o indivíduo que apresenta um conhecimento em informática superior ao demais e disso se utiliza para auxiliar as outras pessoas, ao contrário do que se pensa e se difunde. O cracker, por sua vez, também possui um conhecimento tecnológico elevado, mas não o utiliza de forma positiva, visa causar prejuízo aos demais[19]. Assim os crackers são os que promovem invasões, furtos, fraudes, etc., os sujeitos ativos dos crimes informáticos e os hackers são os que atuam em sentido oposto a eles, ou seja, os que rastreiam os primeiros, procurando evitar os danos que suas ações causam.

Com relação ao sujeito passivo, todo aquele que seja usuário de qualquer tecnologia informática (notebook, computador, tablet, caixa eletrônico, smartphone, etc.), esteja conectado à internet ou não, pode ser vítima da ação de um cracker. Daí se presume que a relação entre o sujeito ativo e o sujeito passivo já se encontra negativamente desequilibrada, em virtude de existir amplitude no polo passivo. Praticamente o mundo inteiro é vítima em potencial, hoje, já o polo ativo mostra-se extremamente restrito, pois nem todos possuem o conhecimento necessário à prática de crimes informáticos. Vale ressaltar, ainda, que o acesso à informática num parâmetro mundial ainda pode ser considerado desigual, o que contribui também para o desequilíbrio acima citado.

Nesse contexto, a realidade da prática de crimes informáticos é a de um ciclo vicioso, pois à medida que as pessoas forem se adaptando melhor à internet e, consequentemente, não serem tão facilmente enganadas, os crackers irão criar novas maneiras de fraudes e golpes, sendo cada vez mais necessário o estudo a fim de se desenvolver maior segurança na transmissão de dados.

2.3.1 Tipos de hackers/crackers

[19]VIANNA, Túlio Lima. **Dos Crimes Por Computador**. Disponível em: < https://www.academia.edu/1911164/Dos_crimes_por_computador > Acesso em: 09. mar. 2014.

Existem termos usados na informática para distinguir os tipos de sujeitos que atuam em seu meio, procurando diferenciá-los com vistas à promoção de uma melhoria na segurança da informação. São os seguintes:

- White Hats: São os hackers "verdadeiros", os que procuram solucionar falhas nos sistemas de informática de maneira legal, sem ter em mente quaisquer privilégios para si mesmos. Eles ajudam o Estado ou a empresa para que trabalhem a se manterem seguros contra crimes informáticos[20].

- Black Hats: São os crackers, pessoas que possuem um bom entendimento sobre sistemas operacionais, redes e programação e investigam suas falhas para delas tirar proveito próprio. Tais sujeitos invadem sistemas, desenvolvem seus próprios softwares, a fim de instalar vulnerabilidades e com isso derrubar servidores, obter informações sigilosas e modificar dados. Geralmente trabalham sozinhos[21].

- Gray Hats: São o resultado da junção entre os dois primeiros, pois não é possível saber se sua atuação se dá de maneira positiva ou negativa. São sujeitos mercenários e sem ética definida que procuram lucrar com os seus conhecimentos, prestando tanto serviços lícitos, quanto ilícitos em troca de dinheiro. Em regra, invadem computadores de maneira "sutil", sem causar vandalismo ou destruição[22].

- Prheakers: É o hacker especialista em telefonia (móvel e/ou fixa). Geralmente, já foram empregados de companhias telefônicas e, por alguma ou algumas razões, tentam prejudicar essas empresas. Sua atuação se dá na invasão das empresas de telefonia, podendo ligar ou desligar telefones, realizar ligações internacionais sem pagamento de taxas, através da invasão aos servidores internacionais, por exemplo[23].

[20] FILHO, Glenio Leitão Marques. Hackers e Crackers na internet: as duas faces da moeda. Revista Eletrônica Temática, Ano 6, nº 01, janeiro de 2010. Disponível em: <http://www.insite.pro.br/2010/Janeiro/hackers_crackers_internet.pdf > Acesso em: 7 de out. de 2013.
[21] Ibid.
[22] Ibid.
[23] Ibid.

- Skript Kiddies: São crackers sem experiência, pessoas que não possuem um conhecimento tão elevado, mas que por diversas razões, seja fama, seja lucro, seja desenvolver seu conhecimento, tentam atuar como ou se passar por hackers. Na maioria dos casos são adolescentes que entendem de informática e procuram alvos fáceis, eles procuram falhas pela internet até que encontrem uma máquina vulnerável e passam a monitorá-la. Suas ações são previsíveis, logo se torna mais fácil proteger-se contra elas[24].

- Lammers: São os que possuem um conhecimento ainda menor que os anteriores. São indivíduos que "brincam" de ser crackers, utilizando-se de programas pré-fabricados para crackear computadores, cuja linguagem de programação, eles geralmente não conhecem ou não entendem. São pessoas que apenas buscam se autoafirmar, desenvolvendo essa atividade[25].

- Newbies: São os novatos, os aprendizes que querem se tornar futuros hackers. Tais sujeitos procuram se aperfeiçoar obtendo novas informações, estão sempre questionando. Não se confundem com os Lammers, pois visam ao aprendizado e não à promoção pessoal[26].

- Defacers: São os crackers cuja atuação é voltada para a alteração de sites na Internet. Podem ser especialistas, ou Skript Kiddies, utilizando programas pré-prontos para tal. Na maior parte dos casos, são pessoas jovens que possuem tempo avantajado para pesquisar sites com falhas na segurança e disso se aproveitam para modificar a página principal do site inserindo uma mensagem por ele criada, assim sua finalidade são seus poucos minutos de fama (pois basta pouco tempo para o administrador corrigir o problema) tal e qual aquele indivíduo que pixa prédios, em um paralelo com o mundo não virtual[27].

- Carders: São os crackers especialistas em fraudar boletos bancários e cartões de crédito. Sua ação se dá com base na invasão de sites de comércio eletrônico, criação/clonagem de falsos sites comerciais e na infecção de máquinas alheias com programas que registram senhas ou monitoram todas as atividades do computador com a finalidade de obter as

[24] FILHO, 2010, passim.
[25] Ibid.
[26] Ibid.
[27] Ibid.

senhas para si. Dessa maneira, esses usam as informações colhidas a seu favor ou as vendem, podendo até efetivar desvio de grande quantidade de dinheiro[28].

- Warez: São os piratas, ou seja, sujeitos que jogam na internet produtos com direitos autorais, desconsiderando as licenças que proíbem cópias não autorizadas e promovendo seu comércio ilegal. Assim, eles difundem filmes, jogos, programas, softwares, etc. sem qualquer custo. Não se confundem com os "piratas de rua" que entregam um produto em troca de um preço, porém contribuem para sua ação[29].

A partir do estudo desses indivíduos e suas principais características observa-se que não há um consenso sobre o que os movem, suas ações vão desde a busca do aprendizado ou status até a espionagem industrial e a própria maldade.

2.3.2 Engenharia Social

Vale discorrer sobre a engenharia social, que é um método de ataque, no qual o criminoso faz uso da persuasão, abusando da inocência ou ignorância do usuário, para obter informações que podem ser usadas na obtenção de acesso não autorizado a computadores ou dados, ou seja, é uma reunião de técnicas muito utilizada pelos sujeitos ativos dos crimes cibernéticos para enganar suas vítimas, evidenciando assim, que não apenas o vasto conhecimento informático é necessário para a prática de boa parte desses crimes, como também é preciso ter certa sensibilidade a respeito da vulnerabilidade do sujeito passivo.

Logo, enquanto alguns crimes informáticos se valem de vulnerabilidades instaladas pelos próprios criminosos em computadores alheios, redes ou servidores, outros se valem da ingenuidade, displicência ou falta de conscientização do usuário do computador sobre as ameaças que lhe possam afetar.

Segundo Emerson Wendt e Higor Vinícius Nogueira Jorge[30]:

> Uma característica deste tipo de ação é que não possui procedimentos definidos sendo utilizado, trata-se principalmente da criatividade do autor destas ações e da sua capacidade de persuadir a vítima a oferecer as informações desejadas.

[28] FILHO, 2010, passim.
[29] Ibid.
[30] WENDT; JORGE, 2012, p.21,passim.

No entanto, é possível distinguir as técnicas mais utilizadas, veja-se:

- Ancoragem: ocorre quando o criminoso usa imagens de empresas conhecidas, bancos, órgãos públicos, etc. para dar confiabilidade aos seus atos[31]. Por exemplo, o usuário recebe um e-mail de um departamento de seu banco, afirmando que o serviço de acesso à conta bancária via internet possui algum problema e que é preciso executar determinado aplicativo em anexo para corrigi-lo. O usuário desavisado assim o faz sem ter noção de que, na realidade, a execução desse aplicativo gera uma tela falsa semelhante àquela que ele está habituado a usar para acessar sua conta bancária, porém a partir do momento em que o mesmo digitar sua senha esta será enviada ao criminoso.

- Efeito Saliência: é a utilização de algum assunto recente na mídia para atrair a atenção do usuário e fazê-lo executar determinado procedimento.[32] Por exemplo a não rara divulgação de fotos exclusivas do casamento de artistas conhecidos em um "link" no qual o usuário clica e sem saber instala um vírus no seu computador.

- Apelo emocional: os criminosos visam manipular as emoções dos usuários para que forneçam as informações que desejam. Assim se valem do medo, da simpatia, da curiosidade ou da ganância.[33] Por exemplo, o clássico golpe em que afirmam que o usuário ganhou grande quantia em dinheiro e para que o valor possa ser recebido ele deverá fornecer certas informações, ou realizar determinada transação em dinheiro a título de garantia.

Como foi explanado, tais ações não seguem regras, podendo incluir de condutas relativamente simples como uma ligação para o usuário se passando por suporte técnico do provedor de Internet e dessa maneira, conseguindo sua senha para se utilizar da sua conta na efetivação de outros crimes, até condutas que exigem conhecimento sobre programação, a exemplo do caso de um e-mail que o usuário recebe, afirmando estar o seu computador infectado com alguma ameaça e sugerindo que para solver o problema, o usuário instale uma ferramenta de determinado site, sendo a real função desta ferramenta, o monitoramento do computador da vítima.

[31] WENDT; JORGE, 2012, p. 23, passim.
[32] Ibid p., 23.
[33] Ibid p., 23.

Por tudo isso, percebe-se que na implementação da engenharia social, a vítima tem uma maior participação, ela é induzida a seguir certos comandos que cominarão no seu próprio prejuízo. Porém, há de se esclarecer que a engenharia social constitui uma via de mão dupla, pois também pode ser utilizada no âmbito da investigação criminal, para que faça o seu efeito inverso, ou seja, a consecução de informações sobre os próprios criminosos, inclusive através da infiltração policial.

2.4 CRIMES EM ESPÉCIE

Diante do que foi apresentado, indispensável é a citação dos crimes informáticos comumente praticados e suas facetas.

2.4.1 Crimes Impróprios de Informática

Como já explanado, nessa categoria o computador constitui mero instrumento da prática da conduta criminosa, a seguir vide exemplos.

a) Furto/Roubo de dados ou informações

Os dados presentes no computador são bens intangíveis, porém suscetíveis de subtração, tendo-se tornado recorrente tal prática com a difusão dos dispositivos móveis, como pen drives e HD's externos. Assim, o namorado ciumento que subtrai o diário virtual da namorada ou o indivíduo que invade uma empresa e sob violência ou grave ameaça, solicita dados presentes em seu sistema, se enquadram nos artigos 155 e 157 do Código Penal[34].

b) Crimes Contra a Honra

Estão previstos: a Calúnia, a Difamação e a Injúria, nos artigos 138, 139 e 140 do Código Penal, respectivamente[35]. O primeiro constitui a imputação de fato falso à vítima,

[34]BRASIL. Decreto-lei nº 2.848 de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm.> Acesso em: 07 mar. 2014. Arts. 155 e 157
[35] Ibid., Arts. 138, 139 e 140.

sendo esse fato definido como crime. O segundo é a imputação de fatos falsos à vítima que ofendam à sua reputação. Por fim, o terceiro é o gesto ou palavra ultrajante que vai de encontro ao sentimento de dignidade da vítima ou seu decoro, muitas vezes incluindo elemento racial, incorrendo na qualificadora do § 3º do artigo 140, acima referido, na qual a honra da vítima é ofendida com palavras, gestos, ou termos referentes à raça.

Tais condutas comumente eram praticadas de forma oral, entretanto, a utilização das redes sociais as tornou uma nefasta realidade virtual, pois os indivíduos que a elas recorrem, confiam no anonimato que a rede social oferece, na falta de controle, a dificuldade de remoção dessas ofensas da rede e no agravamento do resultado de sua conduta. Seu crime não mais será presenciado por uma parcela da população presente quando de sua realização e sim, pelo mundo inteiro.

c) Pedofilia

Trata-se da prática de conduta sexual envolvendo criança ou adolescente proibida por lei. Tanto o Código Penal, ao presumir a violência nos crimes contra a liberdade sexual cuja vítima possui menos que 14 anos (artigo 224)[36], quanto o Estatuto da Criança e do adolescente (Lei 8.069/90), que pune a divulgação de material pornográfico no qual se encontrem crianças ou adolescentes, protegendo os últimos de pessoas que apresentam o desvio sexual da pedofilia[37].

Nota-se que não são raros os casos em que em que pedófilos trocam entre si material com pornografia infantil via internet ou dispositivos móveis, o que não exige um conhecimento superior em informática, mas apenas coisas consideradas simplórias atualmente, como e-mails, redes sociais e pen drives.

d) Dano

Encontra-se previsto no artigo 163 do Código Penal[38], como sendo a conduta de destruir, deteriorar ou inutilizar coisa alheia. Assim o bem jurídico que o Direito visa tutelar é o patrimônio, seja um bem unitário ou conjunto de bens de valor econômico, de utilidade do

[36]BRASIL. Decreto-lei nº 2.848 de 7 de dezembro de 1940.,Art. 224, passim.
[37]Ibid. Art. 240.
[38]Ibid. Art.163.

seu proprietário ou até mesmo de valor sentimental, desde que tais valores sejam significativos para a vítima e o criminoso disso tenha conhecimento.

Os dados armazenados e processados no meio informático entram no conceito de "coisa". São bens, que podem ter valor para o seu usuário. Nesse sentido Túlio Lima Vianna[39] assevera:

> O crime de dano previsto no art. 163 do CP brasileiro é perfeitamente aplicável à tutela dos dados informáticos, sendo completamente prescindível a criação de um novo tipo penal para tal fim. Trata-se de interpretação extensiva da palavra "coisa", elemento objetivo do tipo penal.
> A proteção patrimonial dos dados não se limita ao seu valor econômico, pois a *intentio legis* é proteger todo o patrimônio da vítima, compreendido não só como tutela de valores econômicos, mas também do valor utilidade e do valor afetivo que porventura tenha a coisa.

e) Racismo

Racismo é qualquer tratamento que discrimine a condição humana, a moral e a estima de alguém ou até mesmo de várias pessoas, tomando por base a cor da pele, a origem étnica, seu sexo, sua condição econômica, entre outros. A Lei nº 7.716/2009 em seu artigo 20 tipifica a ocorrência de preconceito racial como praticar, induzir ou incitar a discriminação ou o preconceito de raça, cor, etnia, religião ou procedência nacional[40]. De forma semelhante ao que ocorre nos crimes contra a honra, são facilmente publicáveis na Internet vídeos, imagens ou textos ofensivos que se enquadrem nesse dispositivo, ou seja, a internet se tornou uma nova ferramenta. Em virtude disso, a despeito de todo o repúdio que há em relação ao racismo, se torna dificultoso o seu combate.

f) Estelionato

Previsto no Art. 177 do Código Penal, o estelionato é a consecução de vantagem ilícita por meio fraudulento[41]. No campo da Internet, o sujeito ativo utiliza-se de homepages, sites, chats, e-mails, etc. para induzir a vítima a erro, valendo-se de qualquer ardil ou artifício. É o

[39] VIANNA, Túlio Lima**. Do delito do dano e sua aplicação ao direito penal informático**. Revista dos Tribunais, São Paulo, a. 92, v.807, p. 491, janeiro de 2003.
[40]BRASIL. Lei nº 7.716, de 18 de fevereiro de 2009. Art. 20. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l7716.htm> Acesso em: 07 mar. 2014.
[41] BRASIL. Decreto-lei nº 2.848 de 7 de dezembro de 1940. Art. 177. passim.

exemplo dos e-mails que pedem para as pessoas se recadastrarem na Receita Federal ou Tribunal Superior Eleitoral, sob pena de cancelamento do seu CPF ou título eleitoral. Dessa forma, as vítimas enviam seus dados que, posteriormente, serão utilizados pelo remetente em compras, financiamentos ou falsificações ilegais.

2.4.2 Crimes próprios de informática

Conforme já transcrito, são os crimes que tem por objeto a informática em si, não constituindo o computador apenas um instrumento de sua prática e sim a destinação de sua ação. A seguir vide as condutas criminosas gerais que causam a prática dos crimes informáticos em menor amplitude.

a) Disseminação de Vírus em Geral

Tal e qual o vírus biológico, os vírus de computadores são programas que possuem um hospedeiro, se multiplicam e procuram permanecer ocultos, ou seja, são softwares que mudam a estrutura de uma outra programação de forma nociva, levando à destruição ou alteração de dados.

Existem diversos tipos de vírus, dentre eles:

- O vírus de boot, que se fixa nos programas de inicialização do sistema e cuja infecção ocorre geralmente através de um dispositivo móvel conectado ao computador desligado, sendo ativado quando ligá-lo[42];
- O vírus time bomb, cujo criador escolhe determinada data para seu efeito ser ativado[43];
- O worm, que reside na memória do computador e se auto multiplica sem qualquer ação por parte do usuário, consumindo os recursos da máquina e prejudicando seu desempenho[44];
- Os botnets, que possibilitam ao seu difusor controlar o computador da vítima à distância[45];

[42]WENDT; JORGE, 2012, p 23, passim.
[43]Ibid., p 24.
[44]Ibid., p 24.
[45]Ibid., p 25.

- O deface, que desconfigura sites ou perfis de redes sociais, geralmente inserindo a informação desejada pelo criminoso, seja ela relativa a convicção política ou religiosa, entre outras[46];
- O cavalo de tróia, que possui códigos maliciosos geradores de perda e roubo de dados[47];
- O keylloger, que captura tudo o que é digitado no teclado do usuário[48];
- O Hijacker, que direciona o usuário para páginas da internet diferentes das que o mesmo pretendia acessar, geralmente abrindo nesse mesmo instante pop-ups fraudulentas ou pornográficas[49];
- O rootkit, que são programas ocultos no computador e contaminam tarefas, e processos, gerando inclusive as famosas mensagens de erro[50];
- O sniffer, que intercepta todos os dados do usuário transmitidos pela internet[51] e;
- O backdoor, que ao ser instalado no computador deixa-o vulnerável a quaisquer outras ameaças[52].

A mera difusão de vírus no ordenamento jurídico brasileiro ainda é conduta atípica, sendo punido o criminoso, pela consequência patrimonial que se encaixa no crime de dano do art. 163 do Código Penal[53].

A Lei 12.737/12 inclui no Código Penal o art. 154-A que trata da instalação de vulnerabilidades, no entanto, a condiciona à obtenção de vantagem ilícita para se configurar o crime[54]. A tipificação da difusão viral é extremamente importante para promover a segurança na internet, pois a partir da disseminação do vírus se depreendem todos os demais crimes.

b) Cyberterrorismo

Diferentemente das ações terroristas comuns, o terrorismo no meio virtual exige conhecimentos especiais de informática, pois visa primordialmente atacar sites governamentais, causando pânico no meio tecnológico.

---

[46]WENDT; JORGE, 2012, p. 26, passim.
[47]Ibid., p 29.
[48]Ibid., p 30.
[49]Ibid., p. 32.
[50]Ibid., p. 32.
[51]Ibid., p.34.
[52]Ibid., p.37.
[53]BRASIL. Decreto-lei nº 2.848 de 7 de dezembro de 1940, Art. 163, passim
[54]BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 07 mar. 2014. Art. 154-A.

O hacker ou o grupo de hackers descontentes com o sistema político vigente utiliza-se dos sites governamentais, bem como de outros comumente utilizados para difundir seus ideais, seja por meio de vídeos com mensagens terroristas, seja para o planejamento de ações específicas.

No Brasil, forte exemplo é ação do grupo Anonymous[55], que por meio das redes sociais e de invasão a sites do governo exultou a participação dos brasileiros em protestos ocorridos em todo país contra a corrupção, cominando na ocupação do Congresso Nacional em 17 de junho de 2013.[56]

c) Interceptação Informática

A Constituição Federal de 1988, em seu artigo 5º, inciso XII protege a inviolabilidade da correspondência, comunicações telegráficas e telefônicas e dados[57].

Como extensão desse dispositivo, a Lei 9.296/96 prevê em seu artigo 1º, parágrafo único[58]:

> Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
>
> Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

No entanto, nesse caso, a conduta criminosa fica limitada à intenção da lei, ou seja, a obtenção de provas para fins processuais e/ou policiais, assim, caso a conduta não se enquadre nessa situação, será aplicada a Lei 6.538/78, que prevê os crimes de violação à correspondência[59].

---

[55]ANONYMOUS. **Sobre Anonymous**. Disponível em: < http://www.anonymousbrasil.com/sobre-anonymous> Acesso em 07 mar. 2014.

[56]VALENTE et al. (2013).Vídeo mostra momento da invasão do teto do Congresso Nacional. **Folha de São Paulo**, São Paulo, 17 jun, 2013. Disponível em: < http://www1.folha.uol.com.br/multimidia/videocasts/2013/06/1296762-video-mostra-momento-da-invasao-do-teto-do-congresso-nacional.shtml> Acesso em: 10 mar. 2014.

[57]BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF, Senado,1998. Art. 5º, XII.

[58]BRASIL. Lei nº 9.296 de 24 de julho de 1996. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9296.htm> Acesso em: 07 de mar. de 2014.

[59]BRASIL. Lei nº 6.538 de 22 de junho de 1978. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L6538.htm> Acesso em: 07 de mar. de 2014.

Até o presente momento, se tratou dos conceitos, termos e classificações relativas aos crimes informáticos, como forma de tornar clara a sua complexidade, cotidianidade e consequentemente, a importância do seu estudo e prevenção. No capítulo seguinte se fará um comparativo entre os crimes informáticos previstos e não previstos na legislação nacional, com o que se encontra tipificado na lei 12.737/2012, fazendo uma análise crítica da previsão legal brasileira e suas consequências práticas.

3 ANÁLISE DOS DISPOSITIVOS LEGAIS DA LEI 12.737 DE 30 DE NOVEMBRO DE 2012 E SUAS CONSEQUENCIAS PRÁTICAS

No contexto da evolução informática do mundo globalizado, o Brasil, já com evidente atraso, criou a Lei 12.373/2012, conhecida como Lei Carolina Dieckmann. Esta lei recebeu o apelido da famosa atriz da Rede Globo de Televisão, diante do fato de terem sido copiadas do seu computador pessoal e divulgadas na Internet, várias fotos íntimas em maio de 2011, causando grande escândalo na mídia brasileira.[60]

A referida lei, originada do Projeto de Lei 2793/2011, apresentado em 29 de novembro desse mesmo ano, pelo Deputado Paulo Teixeira (PT-SP), tramitou rapidamente no Congresso Nacional e foi sancionada em 03 de dezembro de 2012 pela presidente Dilma Rouseff e publicada no Diário Oficial da União no mesmo dia.[61]

Em consequência da sua entrada em vigor, foi alterado o Código Penal Brasileiro, e incluída a tipificação criminal dos delitos informáticos[62].

---

[60]POETA, Patrícia (2012). 'Sensação de faca no peito', diz Carolina Dieckmann sobre fotos. **Jornal Nacional**, Rio de Janeiro, 14 maio 2012. Disponível em: < http://g1.globo.com/jornal-nacional/noticia/2012/05/sensacao-de-faca-no-peito-diz-carolina-dieckmann-sobre-fotos.html > Acesso em: 11. Mar. 2014.

[61]AGUIARI, Vinícius (2012). Dilma sanciona Lei Carolina Dieckmann. **Abril**, São Paulo, 3 dez. 2012. Disponível em: < http://info.abril.com.br/noticias/internet/dilma-sanciona-lei-carolina-dieckmann-03122012-27.shl > Acesso em: 11 mar. 2014.

[62]Art. 2o O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

"Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

A principal modificação que essa lei trouxe, foi a inserção do Art.154-A, sob o título dos crimes contra a pessoa, visando à proteção da inviolabilidade dos seus segredos. O crime de invasão de dispositivo informático, desde logo, merece críticas, pois a redação do seu artigo, além de ineficiente, tornou o mesmo extremamente abrangente. Observa-se o trecho: *"Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança".*[63] Subtende-se que todas as condutas mais comuns praticadas via informática estariam submetidas a esse dispositivo, em virtude de, por exemplo, um vírus ser uma invasão, a pichação virtual ser uma invasão, ou seja, praticamente todos os crimes informáticos próprios terem por base, falhas na segurança.

Com isso, é de se observar que o usuário inexperiente não estaria amparado pela proteção legal, pois se o dispositivo exige quebra indevida na segurança, não é considerada invasão quando a conduta do sujeito ativo tiver por alvo computador desprotegido e sem qualquer medida adicional de segurança, como por exemplo, antivírus ou senha de usuário, atribuindo, assim, a maior responsabilidade de evitar a ocorrência de danos sobre seu equipamento ao próprio usuário do dispositivo informático e não ao Estado.

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."

"Ação penal

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

Art. 3o Os arts. 266 e 298 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266. .....

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

§ 2o Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública." (NR)

"Falsificação de documento particular

Art. 298. .....

Falsificação de cartão

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

Art. 4o Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

[63] BRASIL. Lei nº 12.737, de 30 de novembro de 2012, Art. 154-A, passim.

A própria defesa do criminoso informático seria facilitada, pois bastaria a prova de que o usuário não tomava todos os cuidados protetivos em relação ao seu dispositivo informático para desconfigurar o crime. Tal prova é facilmente apresentável para quem entende de sistemas de programação ou até mesmo quem tem acesso a informações privilegiadas, como os empregados de provedoras de serviço de internet, visto que a maioria das pessoas é leiga quanto ao assunto e de forma inocente deixam seu computador vulnerável.

Bem como, nessa mesma linha, não seria configurado o crime, se a invasão se desse por pessoa que tem acesso ao computador da vítima, conhecendo suas senhas e os locais onde se situam suas pastas. Por exemplo, mãe desconfia que seu filho possui material pornográfico infantil no seu notebook e vasculha todas as suas pastas, descobrindo que efetivamente há esse material ou que o filho gravou sua própria atividade sexual com pessoas diferentes. Nesse caso, não haveria violação de mecanismo de segurança, pois nenhuma barreira foi imposta à pessoa que invadiu a privacidade de outrem.

Por último, tal trecho deixa espaço para o enquadramento dos white hats,ou seja, aqueles hackers contratados que testam a segurança de sistemas de informação.

Ademais, o termo “indevida” que se exige a respeito da violação de mecanismo de segurança torna a questão amplamente subjetiva, o que geraria um grande debate judicial dentro das salas de audiências sobre se houve justo motivo ou não para a violação, e assim, olvidando a real intenção da lei que é proteger a privacidade do usuário. Para que surjam dúvidas nesse sentido basta imaginar a seguinte situação: namorado desconfia que esteja sendo traído e invade o diário eletrônico da namorada à procura de qualquer menção a relações com outras pessoas. Para o namorado seu motivo é justo, ele procura manter sua honra intacta, para a namorada seus segredos mais íntimos foram expostos a pessoa não autorizada.

Finalmente, a lei pune apenas o sujeito ativo do crime, aquele que pratica as ações expressas nos verbos do texto legal, mas não pune quem compartilha os dados ou informações violados, tornando a proteção à privacidade mais uma questão de sorte do que de eficaz tratamento legal, visto que a partir do momento em que os dados são divulgados por meio da Internet, entenda-se para o mundo inteiro, dificilmente serão retirados em virtude da agilidade com que já foram passados adiante. Grande exemplo brasileiro se encontra na ação judicial movida pela apresentadora Xuxa Meneghel contra a empresa Google, no qual a autora requeria a remoção da busca de conteúdos relacionados ao seu passado no qual posou em fotos sensuais e estrelou o filme “Amor estranho amor” em que faz uma cena erótica com um

adolescente. A autora não obteve êxito, pois em sua defesa a empresa Google afirmou que de nada serviria remover os resultados se o conteúdo em questão ainda permanece em blogs, sites e páginas do gênero, ou seja, o conteúdo ainda vaga pela internet, sendo o Google apenas um mecanismo de busca, uma ferramenta desenvolvida para facilitar a localização de conteúdo na internet, logo, não seria racional limitar os resultados, pois se esse fosse o caso, a ferramenta perderia sua eficiência[64].

Portanto, a primeiro momento, já se evidenciam indícios de falta de técnica na criação da lei que, além de não abarcar de forma global e indistinta o objetivo para o qual foi criada, exige muito dos usuários de um país onde a tecnologia pode ser considerada ainda recente.

Até tal momento, pode se pensar em praticidade, economia e até mesmo inteligência da lei ao prever tudo em apenas um dispositivo. No entanto, tal artigo peca estabelecendo as seguintes condicionantes *"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[65]".* Ora, a lei estabeleceu os motivos da prática dessa conduta, levando a crer que somente se configura o crime pela existência desses mesmos motivos na prática, o que gera dificuldades na hora da instrução probatória, pois a perícia pode detectar que o dispositivo foi invadido, mas não pode informar exatamente qual foi a finalidade da invasão.

Voltando ao exemplo do namorado ciumento que verifica o diário eletrônico de sua namorada, a conduta do mesmo se resume a mera leitura sem autorização da escritora, não houve obtenção de dados, pois o dito namorado poderia não salvar qualquer página, destruir ou adulterar os dados, e nem tampouco modificar a escrita ou excluir o próprio arquivo. Nesse caso, apesar de não autorizado, não se configuraria o crime, pois a conduta não atendeu a todas as condicionantes que a Lei estabelece.

Fazendo um paralelo com o crime de violação de domicílio (art. 150 CP), o Código Penal afirma ser crime *"entrar ou permanecer, clandestina ou astuciosamente, ou contra a vontade expressa ou tácita de quem de direito, em casa alheia ou em suas dependências"*[66]. Como se percebe, o bem da vida é a inviolabilidade da casa, a liberdade individual. O dispositivo cita "entrar" e "permanecer", como ações suficientes para a prática do crime, não exigindo em adição qualquer outro ilícito ou intenção, o que é mais lógico, no entanto a lei em

[64]AGUIARI, Vinícius (2012). Xuxa perde ação contra Google. **Abril**, São Paulo, 27 jul. 2012. Disponível em: < http://info.abril.com.br/noticias/internet/xuxa-perde-acao-contra-google-27062012-12.shl > Acesso em: 11 mar. 2014.
[65]BRASIL. Lei nº 12.737, de 30 de novembro de 2012, Art. 154-A, passim.
[66]BRASIL. Decreto-lei nº 2.848 de 7 de dezembro de 1940, Art. 150, passim.

questão não considera como crime a mera invasão presumidamente indevida, estabelecendo assim dificuldades à proteção da privacidade ou à inviolabilidade dos segredos das pessoas, que é, ou deveria ser, sua razão de ser.

Outra questão referente ao dispositivo que mais uma vez cai na subjetividade é a exigência da autorização tácita, tornando muito tênue a linha entre a prática do crime e a atipicidade. Até que ponto se estende a autorização de pessoa que nada exprimiu sobre sua vontade, ou condições? Levando em consideração o hábito de utilizar o computador alheio, facilmente qualquer pessoa da família ou amigo mais íntimo poderia cometer crime e escapar às punições da lei alegando autorização tácita.

Ou seja, ao tentar imprimir certa abrangência, a Lei terminou por deixar muitas falhas que podem excluir da apreciação judiciária, a prática de crimes sérios. A invasão em si ao dispositivo informático alheio já deveria importar em crime, pois a conduta acima referida se mostra errônea independentemente de qualquer intenção, tornando-se desnecessárias as condicionantes e os intentos estabelecidos pelo legislador para a configuração do delito.

Quanto à parte final do dispositivo referente à instalação de vulnerabilidades para obter vantagem ilícita, surge o seguinte questionamento: não seria a vulnerabilidade uma falha, uma fraqueza que viria com o próprio sistema? O termo "instalar" utilizado para algo inerente ao sistema tornou a redação legislativa confusa. No entanto, pode-se considerar previsto na legislação brasileira o crime de difusão viral. Pode-se imaginar que nem todos os tipos de vírus seriam abarcados pela lei em virtude da obtenção de vantagem ilícita que se exige como objetivo de sua instalação. No entanto, é de se observar que todo vírus tem um denominador comum, que é justamente a utilidade ou o proveito que não é devido ao agente, logo, a vantagem ilícita faz parte da própria difusão viral, sendo desnecessário incluir essa condicionante. Entretanto, sua inclusão no texto legal não obteve grande influência na configuração do crime, diferentemente dos outros casos acima citados.

Passando a discussão a respeito das agravantes e atenuantes previstas nos parágrafos do Art. 154-A inserido pela lei trabalhada, observa-se que ao prever a conduta de oferecer, distribuir, vender ou difundir dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput[67], o legislador quis tipificar a "pirataria informática". Entende-se por pirataria informática a prática da reprodução ilegal de um programa de computador, sem a autorização expressa do titular da obra ou sem a devida

[67]BRASIL. Lei nº 12.737, de 30 de novembro de 2012, Art. 154-A, passim.

licença de uso, bem como a revenda ou utilização de cópias não autorizadas do programa, o que já é bastante rotineiro dentre internautas que passam para a rede, jogos, filmes, softwares entre outros. Nesse ponto a colocação legislativa foi feliz, porém inócua, porque se pode dizer que a pirataria informática já se tornou um costume *contra legem*, já que naturalmente as pessoas não vão optar por gastar seu dinheiro, tendo a possibilidade de conseguir o exato produto desejado de graça. As licenças perdem a importância nesse momento, pois de toda maneira, o programa pirata é útil e funcional, prevalecendo, logicamente, a economia. Exemplo disso é download de cd's e dvd's a que quase todos os usuários assíduos da internet dão preferência.

Do aumento de pena previsto no parágrafo segundo[68] no caso de ocorrência de prejuízo econômico, a Lei torna evidente que tal e qual para o estelionato só é preciso a vantagem ilícita e não a comprovação do prejuízo em si, sendo esse um ponto positivo, em relação ao todo. Apesar disso, um terço da pena máxima, qual seja, um ano, aumentaria a pena já suficientemente baixa, em no máximo quatro meses.

O parágrafo terceiro do primeiro artigo da Lei traz a previsão de pena de reclusão de seis meses a dois anos, 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[69]. Embora seja uma pena um pouco mais alta do que o previsto anteriormente, ainda se afigura ínfima, em razão da invasão para a aquisição de segredos comerciais e industriais ser praticada principalmente no plano internacional, onde o poderio econômico é expressivo em grande escala.

Vale questionar como o Brasil poderia impor sua soberania e sua Lei, a um espião estrangeiro e qual seria a efetividade dessa lei, se no país de origem do criminoso a tecnologia é superior e o tratamento legal é bem mais especializado, ou seja, o tema em epígrafe envolve questões de soberania nacional, tanto em seu aspecto de discussão jurídica como na proteção do Brasil da espionagem de outros países, o que já é uma realidade. Nos estados estrangeiros as leis que tratam de crimes informáticos são mais graves. Partindo desse ponto, o Brasil seria um verdadeiro "paraíso" para o criminoso estrangeiro, pois se o mesmo está acostumado a infringir uma lei severa e, por vezes, escapar à sua punição, o país se tornaria um alvo fácil e

[68] BRASIL. Lei nº 12.737, de 30 de novembro de 2012, Art. 154-A, § 2º passim.
[69] Ibid., Art. 154-A, § 3º.

preferencial para a prática desses crimes, devido à sensação de impunidade a que a despreparada lei nacional, de certa forma, presta auxílio.

Merece atenção também a modificação dos artigos 266 e 298 do Código Penal, passando a vigorar redação que trata do caso de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.[70] Este dispositivo é extremamente aberto, já que a lei não precisou ao certo o que seria esse serviço de utilidade pública, se seria apenas o sistema que serve ao processo eletrônico, ou se redes sociais, a exemplo do Facebook estariam compreendidas, gerando na prática, novamente subjetividade e possibilidade de qualquer serviço atacado se intitular como de utilidade pública, confundindo mais uma vez a aplicação da lei que na verdade deve direcionar sua previsão para qualquer serviço, e não só os de utilidade pública. Ao não proceder de tal maneira, e levando em consideração a dicotomia público-privado que se estuda no direito, a Lei pode ter deixado de lado ataques a sites de organizações privadas, inclusive instituições bancárias, ficando estes enquadrados no crime de dano, cuja punição é ainda menor do que a prevista no dispositivo em referência, gerando grande injustiça, pois independentemente da natureza do serviço interrompido ou perturbado, poderia ocorrer igual ou maior prejuízo.

Há também a previsão que equipara cartões de crédito e débito a documento particular, buscando evitar a clonagem de cartões. No geral, a clonagem é fruto das falhas no serviço das operadoras de cartão, inclusive sendo estas responsabilizadas, devendo ressarcir o que foi gasto ou desviado pelo cartão clonado, tanto nas comprar comuns, quanto nas compras on-line. Com a presente tipificação criminal, aquele que porventura utilizar aparelhos embutidos nos caixas eletrônicos para ler e copiar as informações da faixa magnética do cartão para uso arbitrário sem autorização do dono do cartão sofrerá punição. Nesse ponto, a lei possui certa serventia.

Necessário é também comentar a previsão do Art. 154-B inserido pela Lei, que afirma somente se proceder mediante representação, os crimes do artigo anterior, salvo se cometidos 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[71].

A ação penal pública condicionada à representação depende da vontade da vítima para que se instaure o inquérito policial ou se ofereça a denúncia, constituindo uma faculdade, o poder de decidir se o Estado investigará e processará o criminoso ou não, sendo inclusive

[70]BRASIL. Lei nº 12.737, de 30 de novembro de 2012, Arts. 266 e 298, passim.
[71]Ibid., Art. 154-B.

retratável até o oferecimento da denúncia. O fundamento da ação condicionada é a preservação da intimidade da vítima e furto ao constrangimento da persecução penal. A partir daí, surge uma discussão que tem por base o fato da vítima raramente saber de quem é a autoria do crime informático, o que não lhe gera longínqua vontade de preservar o criminoso de sua punição, bem como o fato de que a ocorrência do crime já afrontou sua intimidade, logo deixar o processo penal de lado só lhe acarretaria prejuízo. Portanto não há motivo para que nesses crimes, a ação penal seja condicionada, não há razão para qualquer distinção. Do contrário, assim como é para a Administração Pública em geral, tais crimes devem ser de ação penal incondicionada, o que até estimularia o desenvolvimento de estudos informáticos que facilitariam a identificação dos crimes e criminosos, ainda tão deficiente no país.

Veja-se exemplo semelhante ao que originou a própria Lei: artista famosa tem seu computador "hackeado" e fotos íntimas divulgadas na Internet. Por ser uma pessoa pública, sua honra e sua intimidade foram gravemente feridas. As únicas razões para que tal pessoa não tivesse desejo de punição seria o fato da mesma querer ter essas fotos divulgadas e isso não passar de um escândalo para retomar a fama ou o sujeito ativo ser do seu convívio, um amigo ou parente. Porém só haverá condições de se descobrir a autoria após a instauração do inquérito, a partir desse momento a exposição e a afronta a sua intimidade já restaram mais do que consolidadas. Há quem possa imaginar que se a partir do inquérito viesse a se descobrir que o autor do crime era pessoa íntima, estaria justificada a vontade da vítima de se retratar e não mais prosseguir com a persecução penal.

Porém, o prejuízo para a mesma seria enorme, sua imagem já foi divulgada pelo mundo inteiro, seu constrangimento é patente, devendo o Estado Democrático de Direito se preocupar com a proteção devida a essa situação e não com o subjetivismo da vítima. A finalidade da lei é proteger a privacidade, e caso assim não o faça, haverá desmoralização do legislador, e estímulo da prática de tais condutas para criminosos que confiam e se valem do apreço que as vítimas lhes têm.

Por fim, é preciso tratar da quantidade ínfima de penalidade atribuída aos crimes previstos na lei em questão.

Para o crime de invasão de dispositivo móvel é aplicada a pena de três meses a um ano de detenção e multa. Enquadra-se no mesmo delito quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da invasão de computadores ou outro dispositivo informático. A pena será aumentada de um sexto a um terço se a invasão resultar em prejuízo econômico; e de um terço à metade se o crime for

praticado contra Presidente da República, governadores e prefeitos; Presidente do Supremo Tribunal Federal; Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal[72].

As penas possuem baixo grau de sanção, gerando a possibilidade dos benefícios da suspensão condicional do processo e o processamento nos Juizados Especiais, nos quais, dependendo de certos requisitos, como não possuir antecedentes ou a pena maior do crime em questão não ultrapassa dois anos, o réu terá direito a prestar serviços ou pagar cestas básicas ao invés de ser preso. Em suma, não se trata de uma punição, pois não há discussão do mérito da ação, o que, mais uma vez, contribui para ineficiência do combate ao crime cibernético. Na prática será muito difícil ocorrer a prisão de alguém por esse crime, pois além da dificuldade de investigação dos fatos pela despreparada polícia brasileira, a maioria dos criminosos informáticos sempre desenvolveram suas condutas no mesmo meio, qual seja, o virtual, iniciando com pequenos crimes informáticos e prosseguindo com crimes mais ousados, de tal modo que tornaram-se especialistas, raramente deixando rastros de suas condutas. Logo, dificilmente o sujeito ativo do Art. 154-A terá antecedentes criminais registrados, consequentemente, no máximo, irá cumprir alguma pena alternativa. Todavia, se a pena máxima dos crimes previstos na Lei 12.373/12 fosse maior, seria conferida ao juiz maior flexibilidade, para em virtude da gravidade do crime, efetivamente, expedir um mandado de prisão para o criminoso informático.

Como visto, o presente capítulo tratou da lei 12.737/2012 e explanou seus pontos positivos e negativos e também as consequências dessa previsão na prática dos crimes informáticos no Brasil, evidenciando que existem diversas falhas na Lei passíveis de retificação. A partir da exposição de tais falhas legislativas, o capítulo seguinte faz uso do direito comparado como forma de auxiliar a técnica brasileira, através da exibição do tratamento legal da matéria em outros países e que pontos positivos desse tratamento o Brasil poderia adotar.

[72]BRASIL. Lei nº 12.737, de 30 de novembro de 2012, Art. 154-A, passim.

4 OS CRIMES INFORMÁTICOS NO ORDENAMENTO JURÍDICO DE ESTADOS ESTRANGEIROS

Nos crimes informáticos ocorrem violações de diversos bem jurídicos, pois o criminoso não só invade a esfera individual da vítima como também perturba a paz social. Para saber qual o bem jurídico afetado em específico é preciso analisar o objeto do tipo penal. Pode-se dizer que em geral a informática como um todo é o bem jurídico tutelado, tal como o que dela decorrer ou nela estiver inserido, levando em consideração a sua importância atual. A informação toma a roupagem do bem que o crime atingir seja honra, patrimônio ou quaisquer outros. Todavia, por se tratar de uma área em constante desenvolvimento sempre surgirão novas questões que vão exigir novas soluções do direito. Nesse contexto, vários países, ao longo dos anos, procuraram adaptar suas legislações ao surgimento das novas tecnologias e acompanhá-las em paralelo de maneira que sua legislação possa abarcar condutas anteriormente inesperadas. O Brasil, como se pôde observar, apresenta legislação bastante recente sobre o assunto, fazendo-se necessário estudar, observar detalhadamente e seguir os antigos exemplos na busca da melhoria do tratamento da matéria no seu ordenamento jurídico.

4.1 Os crimes informáticos no ordenamento jurídico dos Estados Americanos

Iniciando a análise das legislações informáticas internacionais por caso semelhante ao que desencadeou a criação da Lei 12.737/2012, o hacker Christopher Chaney, em 2011, invadiu a conta de e-mail da celebridade Scarlett Johansson, divulgando fotos da mesma nua, o que resultou, ao final do processo, numa pena de dez anos de prisão aplicada pela justiça do Estado da Califórnia, nos Estados Unidos[73].

A lei americana, em especial o Ato de abuso e fraude computacional de 1986, trata dos crimes informáticos de forma geral, protegendo, no inciso 4 do § 1030 do Título 18, os computadores privados, condenando a até 5 anos de prisão mais multa, o hacker que

[73] ASSOCIATED PRESS (2012). Hacker que divulgou fotos de Scarlett Johansson é condenado a dez anos de prisão. **Folha de São Paulo**, São Paulo, 18 dez. 2012. Disponível em: < http://www1.folha.uol.com.br/tec/2012/12/1203080-hacker-que-divulgou-fotos-de-scarlett-johansson-e-condenado-a-dez-anos-de-prisao.shtml> Acesso em: 10 mar. 2014.

conseguir invadir computador alheio, e com a invasão, obter qualquer vantagem econômica[74], como os Estados possuem autonomia normativa, vários têm legislação independente. Observa-se a partir do primeiro exemplo, a grande diferença na quantidade da pena em relação à lei brasileira e ao tratamento da matéria, que nos Estados Unidos é considerada importante questão de segurança nacional, cuja legislação volta-se para a primordial proteção contra a espionagem econômica e de sistemas governamentais.

A legislação argentina, mais próxima da brasileira, prevê nos artigos 183 e 184 do Código Penal, reprimenda de quinze dias a um ano de prisão para aquele que altera, inutiliza ou destrói dados, documentos, programas ou sistemas de computador, ou vende, distribui, faz circular ou introduz em um sistema de computador, qualquer programa criado para causar danos, aumentando a pena de três meses a quatro anos se a ação for executada em sistemas de computador para a prestação de serviços de saúde, comunicações, fornecimento de energia ou de transporte ou outro serviço público[75]. O legislador argentino, como se vê, optou por apenas exprimir os núcleos do tipo sem citar qualquer condicionante em relação à intenção do agente, ou à quebra de segurança, presumindo o dolo do agente.

Vale citar a lei chilena nº 19.223/93[76] que trata de crimes informáticos:

---

[74]Fraud and related activity in connection with computers. §1030. (a) Whoever- (...) (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;(...) shall be punished as provided in subsection (c) of this section. (...) (c) The punishment for an offense under subsection (a) or (b) of this section is-(...) (3) (A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and (B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4),4 or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph.

[75]Articulo 183. - Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado. En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.(...). Articulo 184. - La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes: 1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;2. Producir infección o contagio en aves u otros animales domésticos; 3. Emplear substancias venenosas o corrosivas; 4. Cometer el delito en despoblado y en banda;5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos; 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

[76]Tipifica figuras penales relativas a la informatica. Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente Proyecto de Ley:

> Artigo 1 º - Quem maliciosamente destruir ou desativar um sistema de processamento de informação ou suas peças ou componentes, ou impedir , obstruir ou modificar o seu funcionamento deve sofrer a pena de prisão menor em seu grau médio ou máximo .
>
> Se, como resultado destes comportamentos se afetarem os dados contidos no sistema, se aplicará a pena prevista no parágrafo anterior, em seu grau máximo.
>
> Artigo 2 º - Quem, com a intenção de tomar, usar ou conhecer indevidamente a informação contida em um sistema de tratamento da mesma , o intercepte, interferira ou o acesse, é punido com pena de prisão nos seus limites mínimo e médio.
>
> Artigo 3 º - Quem maliciosamente alterar, danificar ou destruir os dados contidos em um sistema de processamento de dados, será punido com pena de prisão em seu grau médio.
>
> Artigo 4 º - Quem maliciosamente divulgar ou disseminar a informação contida em um sistema de informação, sofrerá a pena de prisão em seu grau médio. Se quem incorre nestes comportamentos é responsável pelo sistema de informação, a pena será aumentada de um grau. (tradução nossa).

Observa-se que de maneira simples, e em apenas quatro artigos o legislador chinelo preocupou-se com a proteção a sistemas de informação em geral, sejam públicos ou privados, e conseguiu abranger praticamente todas as condutas praticadas no meio virtual atualmente, quais sejam, o furto de quaisquer dados e sua divulgação, a destruição, alteração e danificação de dados, bem como toda forma de interceptação em sistemas de informação, exigindo como única condicionante o dolo e tendo como antecedente lógico a invasão aos sistemas informáticos, o que na prática facilita o ajustamento do criminoso à conduta.

Ademais, a lei chilena possui mais de vinte anos, o que deixa ainda mais claro o quanto o Brasil demorou a legislar sobre crimes informáticos, esvaziando o argumento de que

---

Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4°.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.".

Y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República. Santiago, 28 de Mayo de 1993.- ENRIQUE KRAUSS RUSQUE, Vicepresidente de la República.- Francisco Cumplido Cereceda, Ministro de Justicia. Lo que transcribo a Ud. para su conocimiento.- Saluda atentamente a Ud., Martita Worner Tapia, Subsecretario de Justicia.

o fato de ser um país latino emergente e com menos investimento em tecnologia, justificaria o atraso em que se encontra no tratamento da matéria.

O Código Criminal Canadense em sua seção 183 sob o título *"da invasão da privacidade"* protege todo tipo de interceptação nas comunicações privadas de maneira ampla e analítica, citando os meios pelas quais a conduta pode se dar, incluindo no rol, dispositivos informáticos em geral.[77]

4.2 Os crimes informáticos no ordenamento jurídico dos Estados Europeus

A Constituição Portuguesa prevê no seu artigo 35, inciso 4, a proibição de acesso a dados pessoais de terceiros[78], tendo inclusive lei de proteção específica aos dados pessoais estruturados em qualquer sistema e acessíveis segundo critérios determinados, quer seja um sistema centralizado, descentralizado ou repartido de modo funcional ou geográfico[79], bem como prevê no seu código penal, no artigo 193 a devassa por meio de informática, punindo com até dois anos de prisão mais multa quem criar, mantiver ou utilizar dados referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou a origem étnica[80], tornando bem abrangente o rol de condutas que poderiam se encaixar no presente artigo, o que demonstra a preocupação do legislador português com a privacidade dos cidadãos, procurando não desconsiderar qualquer conduta, independentemente do aspecto da vivência da vítima atingido com a prática dos crimes, em outras palavras, os núcleos do tipo foram desenvolvidos de forma a proteger múltiplos aspectos da privacidade do cidadão, não há preocupação da configuração de condicionantes, que afirmam com que finalidade o crime se deu, e sim qual efeito atingiu.

---

[77]Part VI. Invasion of privacy. Definitions. 183. In this Part, (...) "electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept a private communication, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing.

[78]PORTUGAL. Constituição (1976). Constituição da República Portuguesa. Disponível em< http://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx> Acesso em: 02 mar. 2014.

[79]PORTUGUAL. Lei nº 109 de 17 de Agosto de 1991. Disponível em: < http://www.wipo.int/wipolex/en/text.jsp?file_id=200065> Acesso em: 02 de mar. de 2014.

[80]PORTUGAL. Lei nº 59 de 4 de Setembro de 2007. Código Penal. Disponível em < http://www.hsph.harvard.edu/population/domesticviolence/portugal.penal.95.pdf> Acesso em: 02 mar. 2014.

Vigora ainda em Portugal, a Lei da Criminalidade Informática (Lei nº 109/91), que de forma técnica e com conceitos de informática descritos em seu artigo 2º[81], e adiante no capítulo II prevê os crimes de Falsidade informática, Danos relativo a dados ou programas informáticos, Sabotagem informática, Acesso ilegítimo, Intercepção ilegítima e Reprodução ilegítima de programa protegido[82], dentre os quais se destaca o dano relativo a dados ou programas informáticos, previsto no artigo 5º da lei, pelo qual quem, sem para tanto estar autorizado, e atuando com intenção de causar prejuízo a outrem ou de obter um beneficio ilegítimo para si ou para terceiros, apagar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis dados ou programas informáticos alheios ou, por qualquer forma, lhes afetar a capacidade de uso será punido com pena de prisão até três anos ou pena de multa[83], assim nesse ponto a lei portuguesa exige apenas a não autorização e a intenção de causar prejuízo de qualquer natureza, diferentemente da lei brasileira que exige "violação indevida a mecanismo de segurança" e traz os verbos "obter, adulterar ou destruir" como finalidade e não como núcleo, ou ações da conduta.

No crime de sabotagem informática o legislador português pune quem introduzir, alterar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir em sistema informático, atuando com intenção de entravar ou perturbar o funcionamento de um sistema informático ou de comunicação de dados à distancia[84], independentemente desse programa ou sistema ser utilizado no trato de informações públicas ou privadas, enquanto que a lei brasileira é mais restrita ao tratar apenas da interrupção, impedimento, ou dificuldade de restabelecimento de serviço telemático ou de informação de utilidade pública. Destaca-se, ainda, a diferenciação na gravidade das penas em relação à lei brasileira quando se considera que tal diploma normativo vigora desde 1991 e suas penas podem chegar até 10 anos de prisão, dependendo do crime e do caso concreto.

Na seção 8 do capítulo 24 do Código Penal Finlandês, aquele que, ilegalmente, através do uso dos meios de comunicação de massa, ou de outra forma, colocar à disposição de muitas pessoas a possibilidade de divulgação de informações, insinuações ou imagens da vida privada de outra pessoa, de modo que o ato seja propício a causar danos ou sofrimento, ou sujeitando a pessoa ao desprezo, deve ser condenado a uma multa ou pena de prisão de, no

[81]PORTUGUAL. Lei nº 109 de 17 de Agosto de 1991. Art. 2º. passim.
[82]Ibid., Arts. 4º, 5º, 6º, 7º, 8º, 9º.
[83]Ibid., Art. 5º.
[84]Ibid., Art. 6º.

máximo, dois anos.[85] Observa-se que nesse país a previsão é bem voltada para a privacidade e reputação pessoal, deixando espaço para o enquadramento do indivíduo que se utiliza da informática para atingir outrem, bastando a mera possibilidade da ocorrência do dano para a lei concluir pela punição.

Interessante é deter-se no Novo Código Penal Espanhol, que traz vários artigos ligados aos crimes informáticos, por exemplo, o artigo 197.1, primeiro do título que cuida dos delitos contra a intimidade, que afirma que aquele que, para descobrir os segredos ou violar a privacidade de outra pessoa, sem o seu consentimento, tomar posse de seus documentos, cartas, e-mails ou quaisquer outros documentos ou objetos pessoais ou interceptar suas telecomunicações ou usar dispositivos técnicos de escuta, transmissão, gravação ou reprodução de som ou imagem, ou outro sinal de comunicação, será punido com pena de prisão de um a quatro anos e multa de doze a vinte e quatro meses.[86] O código faz alusão específica aos que sem autorização, assumem o controle, usam ou modificam, em prejuízo de terceiros, dados reservados de caráter pessoal ou familiar registrados em ficheiros ou suportes de dados eletrônicos ou de tecnologia da informação, ou qualquer outro tipo de arquivo ou registro público ou privado, bem como alude também à alteração ou utilização em prejuízo do titular dos dados ou de terceiro, incorrendo nas mesmas penas anteriormente citadas.[87] No primeiro dispositivo a lei exige a finalidade de violar a privacidade e conseguir segredos, já no segundo caso o mero acesso ou controle desautorizado já justificam a punição. As penas, como nos demais casos das legislações internacionais também são de maior grau do que as da lei brasileira.

Adiante o Código Espanhol pune quem, por qualquer meio ou processo, e violando as medidas de segurança acessa de forma não autorizada dados ou software contido em um

---

[85]Chapter 24 - Offences against privacy, public peace and personal reputation (531/2000). (...). Section 8 – Dissemination of information violating personal privacy (531/2000) . (1) A person who unlawfully (1) through the use of the mass media, or (2) otherwise by making available to many persons disseminates information, an insinuation or an image of the private life of another person, so that the act is conducive to causing that person damage or suffering, or subjecting that person to contempt, shall be sentenced for dissemination of information violating personal privacy to a fine or to imprisonment for at most two years.

[86]Artículo 197.1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

[87]Artículo 197.2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

sistema de computador ou parte do mesmo ou permanecer dentro do mesmo contra a vontade de quem tem legítimo direito de excluir, com pena de prisão de seis meses a dois anos, o que sem dúvida, enquadra a difusão de vírus em quaisquer sistemas, sejam públicos ou privados, ou controle remoto dos mesmos, sendo causa de aumento de pena se essas condutas anteriormente citadas forem praticadas pelas pessoas responsáveis por arquivos, mídia de computador, eletrônica ou tecnologia da informação, arquivos ou registros, com a prisão imposta de três a cinco anos, e aumento extra em sua maior metade se os dados confidenciais forem difundidos, cedidos ou revelados[88], bem como quando os dados de caráter pessoal revelam ideologia, religião, crenças, saúde, origem racial ou vida sexual, ou a vítima for menor de idade ou incapaz[89]; e ainda com o adicional da aplicação da pena em maior grau se essas condutas se derem dentro de grupo ou organização criminosa[90], mostrando a atenção do legislador para casos específicos de discriminação fortemente comuns no meio virtual e a conexão que a criminalidade virtual possui com os demais tipos penais. Assim a lei espanhola trata da finalidade do agente e da violação à segurança separadamente, para que um ou outro não tornem dificultoso o enquadramento do criminoso informático, caso estejam no mesmo dispositivo como é o caso da lei brasileira.

O artigo 198 do mesmo código tipifica especificamente a conduta da autoridade ou agente da administração pública, que se valendo do seu cargo, pratica as condutas anteriores, sendo punido com as mesmas penas na metade superior e também com a de inabilitação absoluta por um período de seis a doze anos[91], o que é de fundamental importância na medida em que prevê a conduta de quem tem acesso privilegiado a informações valiosas, que podem ser utilizadas como vantagem, inclusive a nível governamental. Já a lei brasileira buscou proteger as autoridades, no entanto, se mostrou silente quanto à prática dos crimes por parte delas, o que, sem dúvida, expõe a risco e torna frágil a proteção dos dados privilegiados guardados pelos órgãos estatais.

---

[88]Artículo 197.5. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

[89]Artículo 197.6. I gualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

[90]Artículo 197.8. Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado.

[91]Artículo 198. La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

O artigo 200 do mesmo Código traz menção expressa da aplicação ao disposto anteriormente ao que descobrir, revelar ou ceder dados reservados de pessoas jurídicas sem o consentimento dos seus representantes[92].

Vale salientar que para os delitos descritos no artigo 198 a lei espanhola não exige queixa da vítima, quando a consecução do delito afete interesses gerais ou uma pluralidade de pessoas.

Outro importante aspecto que a lei espanhola prevê no artigo 212 do seu Código Penal é a responsabilidade solidária da pessoa física ou jurídica proprietária do meio informativo pelo qual se haja propagado calúnia ou injúria[93], ou seja, do provedor de acesso, o que certamente dificulta a ação dos criminosos informáticos, pois em geral tais empresas prestam serviço a uma grande quantidade de utilitários, o que gera uma maior preocupação em relação à segurança para que a empresa não sofra consequências, principalmente econômicas, da prática desses crimes.

Mais adiante, quando trata da fraude, no artigo 248, a lei espanhola pune os que, visando ao lucro e usando de alguma manipulação informática ou artifício semelhante, obtenha uma transferência não autorizada de qualquer ativo patrimonial em prejuízo de terceiro[94]; também aqueles que fabricarem, introduzirem, mantiverem ou facilitarem programas informáticos especificamente destinados a consecução de fraudes; e os que utilizam cartões de crédito ou débito ou cheques ou dados existentes em qualquer um deles, para fazer qualquer tipo de transação em prejuízo do titular ou por terceiro[95]. A pena aplicada será de seis meses a três anos se a quantia da fraude exceder a quatrocentos euros, podendo ser maior (de um a seis anos) de acordo com o caso concreto e se se tratar de especificidades

[92]Artículo 200. Lo dispuesto en este Capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código.
[93]Artículo 212. En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.
[94]Artículo 248.1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
[95]Artículo 248. 2. También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. c) Los que itilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

previstas na própria lei[96], o que previne a ação dos engenheiros sociais que comumente cometem fraudes, em grande parte bancárias, via internet.

A lei espanhola também protege expressamente as empresas, punindo com prisão de dois a quatro anos mais multa de doze a vinte e quatro meses, quem se utiliza de instrumento informático para descobrir segredo empresarial, aumentando a pena, caso se difundam, revelem ou cedam os segredos descobertos, bem como se o agente tinha obrigação contratual de guardar as informações ou as utiliza em seu próprio proveito[97].

Assim observa-se perfeitamente a divergência de tratamento da matéria na lei estrangeira e na lei brasileira, pois o legislador espanhol desceu a minúcias procurando não olvidar qualquer detalhe na execução dos delitos informáticos e na punição de seus agentes em todos os aspectos, bem como se mostrou conhecedor de uma melhor técnica de elaboração legislativa. Diferentemente da lei brasileira, amplificou a norma e a restringiu quando necessário e de forma correta, elevando as punições a tal nível de importância que na lei brasileira tais delitos seriam de ação penal pública incondicionada.

Na Itália, assim como e outros países europeus, há legislação avançada sobre crimes informáticos. O Código Penal Italiano, em seu artigo 615, prevê o envio de vírus, como a conduta do agente que difunde, comunica ou entrega um programa informático com o intuito de provocar danos nos dados, programas informáticos ou telemáticos de computadores alheios ou interrompa, total ou parcialmente, seu funcionamento[98], bastando o envio do vírus para a configuração do crime, independentemente da existência de dano material. Pune-se também aquele que difunde, ilegalmente, os códigos de acesso, palavras chaves ou outros meios idôneos de acessar um sistema de informática protegido por medida de segurança.

Portanto, observa-se que é comum nas legislações europeias haver uma previsão legal exclusiva e diferenciada para a pirataria de softwares, que é prática comum no Brasil e possui

---

[96]Artículo 249. Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años, si la cuantía de lo defraudado excediere de 400 euros. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los medios empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción.

[97]Artículo 278. 1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

[98]Art. 615 - Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico - Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire venti milioni.

certa relação com a violação à privacidade, pois boa parte dos hackers, em maioria os iniciantes, se utilizam de programas pirateados para iniciar a atividade de espionagem.

No Reino Unido, há o Ato do Mau Uso do Computador de 1990, prevendo o acesso não autorizado a material informático no caso do agente que, sabendo não estar autorizado para tal, faz com que um computador execute qualquer função com a intenção de garantir ou permitir o acesso a qualquer programa ou dados existentes em qualquer outro computador, tal como pune também o acesso desautorizado com a intenção de cometer ou facilitar a consecução de novas infrações e causar prejuízo[99].

Qualquer pessoa que se forneça ao auxílio dessas condutas também será punida. Logo é de se observar que a lei inglesa de forma simplificada exige apenas o dolo como configuração dos delitos expressos de forma breve, porém abrangente, tendo o diferencial de que a punição se estende em cadeia, na medida em que todos os que de alguma forma contribuíram para a consecução do crime, mesmo que de maneira indireta estão enquadrados na lei, o que gera uma forte coerção, ao contrário da lei brasileira que deixa a desejar quando se trata de responsabilizar tanto o provedor de acesso, quanto os que passam adiante as informações que são fruto dos crimes previstos na Lei 12.737/12.

No Código Penal Francês, há aumento de pena pros casos de tráfico de pessoas[100], corrupção de menores[101], difusão pornográfica[102], e estupro[103] quando o contato entre o agressor e a vítima se dá por meio informático.

---

[99]Unauthorised access to computer material. (1) A person is guilty of an offence if (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured; (b)the access he intends to secure, or to enable to be secured, is unauthorised; and (c) he knows at the time when he causes the computer to perform the function that that is the case.

[100]Artículo 225-4-2. La infracción prevista en el artículo 225-4-1 se castigará con diez años de prisión y multa de 1.500.000 euros, cuando se cometa: (...): 5º Cuando la persona haya sido puesta en contacto con el autor de los hechos gracias a la utilización de una red de telecomunicaciones para la difusión de mensajes destinados a un público indeterminado.

[101]Artículo 227-22. El hecho de favorecer o intentar favorecer la corrupción de un menor será castigado con cinco años de prisión y multa de 500.000 francos. Estas penas se elevarán a siete años de prisión y multa de 700.000 francos cuando el menor tenga menos de quince años o cuando el menor haya entrado en contacto con el autor de los hechos gracias a la utilización de una red de telecomunicaciones para la difusión de mensajes destinados a un público no determinado(...).

[102]Artículo 227-23. El hecho de tomar, grabar o transmitir la imagen o la representación de un menor con objeto de su difusión, cuando esta imagen o esta representación presenten un carácter pornográfico, será castigado con tres años de prisión y multa de 45.000 euros. El hecho de difundir una imagen o representación de ese tipo, por cualquier medio, de importarla o exportarla, o hacerla importar o exportar, será castigado con las mismas penas. Las penas se elevarán a cinco años de prisión y multa de 75.000 euros cuando, para la difusión de la imagen o de la representación de un menor destinada a un público indeterminado, se haya utilizado una red de telecomunicaciones. (...).

Vale citar o simplificado Ato do dano criminal de 1991 da Irlanda[104], que em sua seção 5, prevê:

> 5 – (1) "Acesso não autorizada de dados:.
> Aquele que, sem razão legal opera um computador :
> (a) no interior do Estado com a intenção de acessar quaisquer dados mantidos dentro ou fora do Estado, ou
> (b) fora do Estado com a intenção de acessar quaisquer dados guardados no interior do Estado, deve, caso acesse, ou não, os dados, ser culpado de um delito e será responsável a uma multa não superior a 500 £ ou prisão por um período não superior a 3 meses, ou ambos.
> A subseção (1) aplica-se à pessoa com a intenção de acessar quaisquer dados particulares, ou uma categoria de dados, ou dados mantidos por uma pessoa em particular."(tradução nossa).

Ou seja, a lei irlandesa pune a mera tentativa de invasão de quaisquer dados, sejam públicos ou privados, bastando somente a intenção do acesso desautorizado, por se tratar de uma questão principal de segurança nacional pelo que se observa do tratamento legal acima exposto. Tal lei não invoca condicionantes, é simples, prática e objetiva em sua redação e abrange todo tipo de violação e espionagem em todos os setores do Estado.

O Código Penal Alemão, em sua seção 15, § 202 "a" prevê a espionagem de dados punindo todo aquele que, contornando as medidas de proteção, obtém ilegalmente dados para si mesmo ou para outrem que a ele não foram destinados e foram especialmente protegidos contra acesso não autorizado, com pena de prisão não superior a três anos ou multa[105]. Nesse caso, a lei exige uma violação de segurança, mas não uma finalidade específica na conduta do agente, apenas que os dados não lhe digam respeito.

A seção 22, § 263 "a" do mesmo Código prevê a fraude informática como sendo o ato daquele que, com a intenção de obter para si ou para uma terceira pessoa um benefício material ilegal, causa dano à propriedade de outrem influenciando o resultado de uma

---

[103]Art. 222-24. La violación se castigará con veinte años de reclusión criminal: (...)8º Cuando la víctima se haya puesto en contacto con el autor de los hechos gracias a la utilización de una red de telecomunicaciones para la difusión de mensajes destinados a un público no determinado; (...).

[104]Unauthorised accessing of data.5—(1) A person who without lawful excuse operates a computer— (a) within the State with intent to access any data kept either within or outside the State, or (b) outside the State with intent to access any data kept within the State, shall, whether or not he accesses any data, be guilty of an offence and shall be liable on summary conviction to a fine not exceeding £500 or imprisonment for a term not exceeding 3 months or both. (2) Subsection (1) applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person.

[105]§202 a. Piratería informática. (1) Quien sin autorización se procure para sí o para otro datos que no estén destinados para él y que estén especialmente asegurados contra su acceso no autorizado, será castigado con pena privativa de la libertad hasta tres años o con multa. (...).

operação de processamento de dados por meio de configuração incorreta de um programa, ou uso de dados incorretos ou incompletos, ou uso não autorizado de dados ou outra influência não autorizada no curso do processamento, devendo ser condenado à prisão não superior a cinco anos ou multa. Pune-se todo aquele que prepara uma infração nesses termos, criando programas de computador cujo objetivo é cometer tal ato, ou adquiri-los para si mesmo ou para outrem, propõe à venda, mantém ou fornece para outrem, com prisão não superior a três anos ou multa[106].

Assim, facilmente se percebe o nível técnico do legislador alemão, que tipificou os dispositivos evidenciando os processos de phising e fraude eletrônica em sua íntegra e não olvidando também as invasões comuns, se assemelhando nesse ponto ao Código Espanhol e à Lei Inglesa em relação à punição estendida em cadeia para os fabricantes e difusores de programas que auxiliam a consecução do crime.

Mais adiante, na seção 27, § 303 "a", o Código Penal Alemão pune a violação de dados, nos casos de exclusão de forma ilegal, supressão, alteração ou inutilização, com pena não superior a dois anos e multa.[107] Finalmente o mesmo Código prevê a sabotagem informática como a conduta de interferir nas operações de processamento de dados que são de importância substancial para outrem, acessar ou transmitir dados com a intenção de causar dano, ou destruir, danificar, tornar inutilizáveis, remover ou alterar um sistema de processamento de dados ou um suporte de dados, sendo punido com pena de prisão não superior a três anos ou multa[108]. Logo, o país incluiu em sua legislação todas as principais ações nucleares que norteiam os crimes informáticos.

Portanto, é comum para a legislação europeia tratar os crimes informáticos com importância em nível de Estado soberano e exaustivamente legislar sobre os mais variados casos específicos que surgem. O legislador alemão, assim como os demais dos outros países europeus, como se pôde observar, tomou por base os procedimentos utilizados pelos

---

[106]§263 a. Estafa por computador . (1) Quien con el propósito, de procurarse para sí o para un tercero una ventaja patrimonial antijurídica, en la medida en que él perjudique el patrimonio de otro, por una estructuración incorrecta del programa, por la utilización de datos incorrectos o incompletos, por el empleo no autorizado de datos, o de otra manera por medio de la influencia no autorizada en el desarrollo del proceso, será castigado con pena privativa de la libertad hasta cinco años o con multa.(...).

[107]§ 303 a. Alteración de datos. (1) Quien borre, suprima, inutilice, o cambie antijurídicamente datos (§ 202 a, inciso 2), será castigado con pena privativa de la libertad hasta dos años o con multa. (...).

[108]§ 303b. Sabotaje de computadoras. (1) Quien perturba un procesamiento de datos que sea de importancia esencial para una empresa ajena, una industria ajena o una autoridad para 1. cometer un hecho según el § 303 a, inciso 1, o 2. destruir, dañar, inutilizar, eliminar o modificar un equipo de procesamiento de datos o un medio de datos será castigado con pena privativa de la libertad hasta cinco años o con multa. (...).

criminosos para a tipificação das condutas e quando não os conhece em específico, abrangem toda e qualquer invasão ou ofensa a dados e sistemas informáticos.

Afigura-se como solução à falta de técnica e ineficácia da Lei nº 12.737, seguir alguns exemplos das leis internacionais acima demonstradas, não como uma maneira de apenas atribuir ao Brasil algo que funciona em outro ordenamento, e sim de se promoverem as adaptações necessárias para que a lei possa efetivamente atingir sua finalidade.

Primeiramente, o legislador brasileiro poderia reduzir os objetos do tipo do artigo 154-A prevendo apenas a invasão de dispositivo conectado ou não à rede de computadores e a difusão de vírus, trazendo todas as condicionantes do tipo como a "finalidade de obter vantagem ilícita" ou "ou destruir dados ou informações" para a parte seguinte do dispositivo onde se prevê as causas de aumento de pena, pois assim toda e qualquer invasão seria punida, independentemente de quaisquer questões subjetivas[109]. O legislador deve deixar a cabo da jurisprudência, a definição de conceitos localizados num setor que muda constantemente, não sendo aconselhável engessar as tipificações, ou ao menos, a exemplo da lei portuguesa, destinar um artigo específico só para a conceituação no que tange à área informática.

A lei brasileira também poderia optar pela punição em cadeia, como ocorre na Espanha e Inglaterra, assim não apenas os responsáveis pela invasão seriam punidos, como também todo aquele que compartilha o conteúdo fruto da invasão ou de qualquer outra forma indireta participa do crime, pois ao coibir essa prática egoísta, porém comum no país, a lei determina a contenção geral e o respeito para com as vítimas que obtiveram sua intimidade violada por criminosos cibernéticos, tornando firme a convicção de que a vítima não é a culpada por não ter investido na segurança ou "facilitado" a ação, como muito se difunde, e sim que um crime dessa natureza é grave e não deve ser praticado sob nenhuma circunstância.

Nos casos do crime de difusão viral e pirataria de software, as legislações internacionais no geral, por uma questão de organização técnica, optaram por prevê-los independentemente em dispositivos separados para deixar mais clara e expressiva a proibição legislativa, exemplo que o legislador brasileiro também deve seguir. A lei ficaria mais cognoscível e tais crimes não dependeriam de uma interpretação como se estivessem subtendidos em outro dispositivo, o que inclusive contribui para melhorar a noção social do usuário de internet brasileiro que considera tais condutas "normais" ou com pouco grau de

[109]BRASIL. Lei nº 12.737, de 30 de novembro de 2012, Art. 154-A, passim.

significância, justamente porque o avanço da tecnologia do Brasil foi descompassada da legislação, o que comina na ineficácia da lei atual de tratamento tão desleixado.

A legislação internacional, tanto na Europa quanto em alguns países da América Latina, há muitos anos já previu os crimes informáticos e os revestiram, em sua maioria, da importância de um assunto de segurança nacional, quando não, priorizaram as vítimas que tiveram sua intimidade ou privacidade invadida, com o consolo de uma pena prisional, mais coercitiva e até mesmo retributiva, na medida em que aquele que infligiu a intimidade alheia excedeu do uso da sua liberdade, sendo agora dela privado.

Seguindo a tradição analítica do legislador brasileiro, os crimes de controle remoto de dispositivo informático, phising, clonagem e deface, rotineiramente praticados no Brasil, também merecem previsão específica.

O ataque a serviços deve ser direcionado tanto para serviços de utilidade pública quanto privada, aqui entra a questão da segurança nacional já exaustivamente citada anteriormente, o legislador deve inibir todo tipo de espionagem, seja das instituições do poder público, seja das empresas privadas, responsáveis por grande parte do lucro do país. Ao não proceder de tal maneira torna-se clara a tendenciosidade do legislador, que concedeu privilégio à área pública e a quem nela exerce função, tanto que instituiu aumento de pena quando o alvo dos crimes informáticos forem os chefes de poderes ou dirigentes máximos, mas nada tratou a respeito da possibilidade de ocorrer uma inversão e os criminosos informáticos se encontrarem em funções de alto escalão, bem como também não fez menção expressa à prática dessas condutas por parte de funcionários públicos e outros profissionais que tenham acesso privilegiado a informações importantíssimas. Nesse ponto é válido apontar a lei espanhola como um modelo a se seguir.

O legislador brasileiro parece não voltar-se para a administração bancária que possui falhas de segurança úteis aos criminosos diante da farta tecnologia à sua disposição. A título de exemplo prático, pode-se citar caso de furto a bancos nos quais os criminosos se valiam de aparelhos informáticos para obter acessos aos caixas.[110]

[110]SOUZA, Colombo de (2013). Integrante de quadrilha joinvilense de roubo a caixas eletrônicos é preso em Palhoça. **Notícias do Dia**, Joinville, 20 maio 2013. Disponível em: < http://www.ndonline.com.br/joinville/noticias/72549-integrante-de-quadrilha-joinvilense-de-roubo-a-caixas-eletronicos-e-preso-em-palhoca.html > Acesso em: 11 mar. 2014.

Por fim, é de se observar que em alguns países as penas são bem mais altas do que as previstas na Lei 12.737/12, o que se mostra uma modificação necessária na lei brasileira, pois os crimes informáticos por si só já imprimem dificuldade na captura do criminoso, pois o meio do qual se utilizam favorece o anonimato, e o próprio departamento policial brasileiro não possui divisão específica para cuidar desses assuntos no qual o bom uso da tecnologia iria combater o mal uso. Ademais, em sua maioria as leis estrangeiras possuem duas décadas e o Brasil só agora legislou de forma desatenta e por motivos midiáticos, desconsiderando a real necessidade e urgência de uma lei eficiente a respeito dos crimes informáticos.

Ressalta-se a existência de tese doutrinária que afirma que a eficiência da pena não se relaciona com sua severidade e sim com a sensação de impunidade, o que não depende da legislação em si, e sim da eficiência da atividade policial. Nesse sentido, a severidade da pena só influenciaria a consecução de crimes simples e não de crimes especializados, como é o caso dos crimes informáticos[111]. Todavia, fato é que desde o advento da Internet o mundo se tornou informatizado e em alguns países, como no caso do Brasil, os usuários não tiveram a maturidade de utilizar essa ferramenta com moderação, nem o legislador vislumbrou a possibilidade da mesma ser utilizada como arma para a prática de crimes com antecedência. De maneira que, atualmente, após sua consolidação, e com o exemplo das inúmeras condutas que podem se dar no meio virtual, é essencial que a lei procure frear os ímpetos dos criminosos informáticos, o que se dá apenas com um alto grau de coerção, pois já haviam se acostumando a impunidade, logo as penas relativas aos crimes informáticos não devem ser tão baixas, nem passíveis do oferecimento de benefícios legais e sim possibilitar a prisão exemplar, até que a educação avance ao ponto de alcançar a utilização do meio virtual de forma apropriada.

[111]SCHWARTZ, Richard D; ORLEANS, Sonya, "On Legal Sanctions**".** *In* Joel B. Grossman e Mary H. Grossman (eds.), **Law and Change in Modern America**, Pacific Palisades, Califórina, Goodyear Publishing Company, Inc., 1971, pp. 91-7, (Originariamente publicado em **University os Chicago Law Review 34** (1967), pp. 275-300.)

5 CONSIDERAÇÕES FINAIS

O presente trabalho propôs-se a abordar a análise dos tipos previstos na Lei 12.737/2012. O Objetivo principal do trabalho foi explorar a necessidade de revisão da lei supracitada, para torná-la eficaz dentro do ordenamento jurídico brasileiro. Os objetivos específicos constituem a revisão da quantificação da pena aplicada a cada tipo penal previsto na lei, do julgamento dos objetos dos tipos penais definidos e da comparação entre esses tipos penais expressos na lei e suas respectivas penas a outros tipos penais já definidos nos ordenamentos estrangeiros.

Como o Código Penal brasileiro foi elaborado em 1940, o legislador pátrio visou à proteção dos bens daquela época quando definiu os crimes. No entanto, atualmente várias mudanças ocorreram na sociedade, principalmente o avanço tecnológico e a informática, que já é parte do dia-a-dia dos brasileiros. A tecnologia da informação não é usada apenas para suas finalidades iniciais como também para a prática de crimes que lesam vários bens jurídicos.

Com o estudo conduzido neste trabalho observou-se que a evolução da informática deu nova roupagem e amplitude à criaminalidade, primordialmente na sua efetividade, pois sua execução foi simplificada, tanto para os crimes impróprios de informática, como visto, aqueles nos quais o dispositivo informático pode ou não ser um instrumento, quanto nos específicos ou próprios, ou seja, os que só podem ser necessariamente realizados por meio do dispositivo informático. Tal crescimento da utilização da informática obriga o Direito a se adaptar e enquadrar as condutas criminosas cometidas por meio dos sistemas informáticos.

Vislumbra-se assim, uma análise detalhada a respeito da ineficácia dos tipos previstos na supracitada lei no que tange à repressão da prática de condutas criminosas no meio informático, ante a falta de técnica legislativa voltada a finalidade primordial da previsão e a inobservância da proporcionalidade entre a gravidade da sanção penal e o objeto tutelado pela norma incriminadora, princípio de vital importância no ramo do direito penal.

No primeiro capítulo foi apresentada a conceituação e a terminologia dos crimes informáticos, em seguida de sua classificação doutrinária, sujeitos ativos e condutas mais comumente praticadas que se encaixam no conceito de crime. Restou demonstrado que os crimes informáticos, por mais comumente praticados que sejam, possuem um grau de

complexidade tanto no que se refere à sua prática, quanto à sua analise jurídica e tipificação, devido à necessidade de se conhecer as técnicas essenciais à sua prática, o que por si só exige do legislador conhecimento prático dos procedimentos, habilidade, atenção e também estratégia quando da elaboração das normas legais.

Já no segundo capítulo do presente trabalho, foi abordada a Lei 12.737/2012 e todos os dispositivos previstos em seu texto, pontuando-se os erros técnicos e de raciocínio do legislador brasileiro quando da sua confecção, ou seja, em que momento truncou demasiado o texto legal, em que momento foi muito abrangente a ponto de esvaziar o sentido da norma e em que momento deixou de observar atentamente à realidade da criminalidade informática brasileira.

Ainda no segundo capítulo, detalhou-se o tema através de exemplos e suposições de situações cotidianas relacionadas com os crimes informáticos que se submeteriam a aplicação da Lei 12.737/2012, suas consequências práticas e os pontos negativos gerados pela tipificação criminal na maneira pela qual se deu.

O último capítulo foi dedicado à abordagem a respeito do direito comparado, exibindo as legislações de outros países acerca da tipificação dos crimes informáticos, chamando atenção para sua antiguidade em relação à norma brasileira e também a sua técnica apurada, atenta à tecnologia e a ciência do quão rápido ela se desenvolve, tornando claro o quanto atrasado o Brasil se encontra no tratamento desses crimes e o quanto se faz urgente a necessidade de uma legislação melhorada, devido à insuficiência e ineficácia da norma atual.

Também no terceiro capítulo foram citadas como exemplo a se seguir algumas legislações americanas e europeias que com maestria souberam cuidar do tema com equilíbrio de maneira que nem a tipificação nem a pena aplicada fosse descomedida ou ínfima, o que se aplicado ao caso brasileiro tornaria a prevenção contra os crimes informáticos bem mais produtiva.

É de se compreender, portanto, que a criminalidade informática requer uma normatização ativa no sentido de coibir as condutas praticadas no meio virtual, implicando numa aplicação de pena eficiente e coercitiva. Além disso, deve-se facilitar a proibição que objetiva a previsão penal, tendo por base, precipuamente, o real grau de avanço tecnológico observado nas práticas criminosas.

Apresentaram-se como possíveis soluções, o aumento das penas para que se efetive maior coerção e prevenção quanto a prática de crimes informáticos, a diminuição de condicionantes do tipo para esclarecer a intenção legislativa e, principalmente, o tratamento legal, tendo em mente que a matéria de que se fala possui importância a nível nacional, envolvendo questões de segurança e não somente individuais, bem como a tutela de serviços não acobertados pela lei, melhor divisão dos tipos e explanação dos conceitos informáticos.

Dessa forma, através de uma pesquisa de natureza aplicada, abordagem qualitativa, bibliográfica-documental e exploratória, bem como da coleta de dados documental e análise de conteúdo, através de método de abordagem dedutivo e dos métodos de procedimento comparativo e estudo de caso, chegou-se à conclusão de que a Lei 12.737/2012 precisa ser retificada e aperfeiçoada para então reprimir o crime praticado no ambiente virtual de maneira hábil, principalmente no que concerne a mentalidade do legislador que ainda deixa evidente que esses crimes no ordenamento pátrio ainda de voltam para a esfera individual do ser humano, desconsiderado a importância que os mesmos têm em questões de Estado.

Diante desse panorama, todos os objetivos a que se destinou o presente trabalho científico foram alcançados, uma vez que se registrou a ineficácia da Lei 12.737/2012 e a urgência da adaptação da legislação brasileira ao desenvolvimento da criminalidade informática em toda sua amplitude, para que se viabilize e se assegure a disponibilidade, a integridade, a confidencialidade e a autenticidade dos ativos de informações que circulam no meio informático, os quais são valores tangíveis e intangíveis, imprescindíveis aos interesses do Estado e da Sociedade.

REFERÊNCIAS

AGUIAR, Daniel Pedrosa. **Estudo sobre crimes praticados na Internet com o uso de computador**. 105 f. 2009. Trabalho de Conclusão de Curso (Graduação em tecnologia em Informática): Centro Tecnológico da Zona Leste, Faculdade de Tecnologia da Zona Leste, São Paulo, 2009. Disponível em: < http://fateczl.edu.br/TCC/2009-2/tcc-16.pdf > Acesso em: 01 mar. 2014.

AGUIARI, Vinícius (2012). Dilma sanciona Lei Carolina Dieckmann. **Abril**, São Paulo, 3 dez. 2012. Disponível em: < http://info.abril.com.br/noticias/internet/dilma-sanciona-lei-carolina-dieckmann-03122012-27.shl > Acesso em: 11 mar. 2014.

_____, Vinícius (2012). Xuxa perde ação contra Google. **Abril**, São Paulo, 27 jul. 2012. Disponível em: < http://info.abril.com.br/noticias/internet/xuxa-perde-acao-contra-google-27062012-12.shl > Acesso em: 11 mar. 2014.

ALEMANHA. Lei de 13 de Novembro de 1998. Código Penal. Disponível em: <https://www.unifr.ch/ddp1/derechopenal/obrasjuridicas/oj_20080609_13.pdf> Acesso em: 01 mar. 2014. Tradução de: Cláudia López Dias.

ANONYMOUS. **Sobre Anonymous.** Disponível em: < http://www.anonymousbrasil.com/sobre-anonymous> Acesso em 07 de mar. de 2014.

ARAS. Vladimir. **Crimes de Informática – Uma nova criminalidade**. Disponível em: < http://www.informatica-juridica.com/trabajos/artigo_crimesinformaticos.asp>. Acesso em 26 abr. 2009.

ARGENTINA. Lei nº 11.179. Código Penal. Disponível em: < http://www.codigopenalonline.com.ar/> Acesso em 02 mar. 2014. Título original em Espanhol.

ASSOCIATED PRESS (2012). Hacker que divulgou fotos de Scarlett Johansson é condenado a dez anos de prisão. **Folha de São Paulo**, São Paulo, 18 dez. 2012. Disponível em: < http://www1.folha.uol.com.br/tec/2012/12/1203080-hacker-que-divulgou-fotos-de-scarlett-johansson-e-condenado-a-dez-anos-de-prisao.shtml> Acesso em: 10 mar. 2014.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF, Senado,1998.

BRASIL. Decreto-lei nº 2.848 de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm.> Acesso em: 07 mar. 2014.

_____. Lei nº 12.737, de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 07 mar. 2014.

_____. Lei nº 6.538 de 22 de junho de 1978. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L6538.htm> Acesso em: 07 mar. 2014.

_____. Lei nº 7.716, de 18 de fevereiro de 2009. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l7716.htm> Acesso em: 07 mar. 2014.

_____. Lei nº 8.069 de 13 de julho de 1990. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8069.htm> Acesso em: 07 mar. 2014.

_____. Lei nº 9.296 de 24 de julho de 1996. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9296.htm> Acesso em: 07 mar. 2014.

CANADÁ. Código Criminal de 1985. Disponível em: < http://laws-lois.justice.gc.ca/eng/acts/C-46/page-89.html#h-61> Acesso em: 02 mar. de 2014. Título original em inglês.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática: e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumem Júris, 2003.

CHILE. Lei nº 19.223 de 7 de junho de 1993. Disponível em: < http://www.leychile.cl/Navegar?idNorma=30590&r=1> Acesso em: 02 mar. 2014. Título original em espanhol.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. Saraiva: São Paulo, 2000.

COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática.** Jus Navigandi. Teresina, ano 1, nº 12, maio de 1997. Disponível em: <http://jus.com.br/artigos/1826/crimes-de-informatica/1> Acesso em: 2 out. 2013.

DAOUN, Alexandre Jean; LIMA, Gisele Truzzi de. **Crimes Informáticos: O direito Penal na Era da Informação**. Disponível em: < http://www.truzzi.com.br/pdf/artigo-crimes-informativos-gisele-truzzi-alexandre-daoun.pdf> Acesso em: 12 ago. 2013.

ESPANHA. Lei Orgânica nº 10 de 23 de novembro de 19995. Código Penal. Disponível em< http://www.ub.edu/dpenal/CP_vigente_2013_01_17.pdf> Acesso em: 02 de mar de 2014. Título original em espanhol.

ESTADOS UNIDOS DA AMÉRICA. Ato de abuso e fraude computacional. 1986. Código dos Estados Unidos. Disponível em: < http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section1030&num=0&edition=prelim> Acesso em: 02 mar. 2014. Título original em inglês.

FERREIRA, Ivete Senise . **A criminalidade informática**. In: Newton de Lucca; Adalberto Simão Filho. (Org.). Direito e Internet – aspectos jurídicos relevantes. Bauru: Edipro, 2000.

FILHO, Glenio Leitão Marques. **Hackers e Crackers na internet: as duas faces da moeda.** Revista Eletrônica Temática, Ano 6, nº 01, janeiro de 2010. Disponível em: <http://www.insite.pro.br/2010/Janeiro/hackers_crackers_internet.pdf > Acesso em: 7 de out. de 2013.

FINLÂNDIA. Código Criminal da Finlândia de 1894. Disponível em: < http://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf> Acesso em: 02 de mar. de 2014. Título original em inglês.

FRANÇA. Lei nº 495 de 12 de junho de 2003. Código Penal. Disponível em: < http://www.juareztavares.com/textos/codigofrances.pdf> Acesso em: 07 de mar. de 2014. Tradução de: Juarez Tavares.

FURLANETO NETO. Mário. GUIMARÃES. José Augusto Chaves**. Crimes na Internet: elementos para uma reflexão sobre a ética informacional.** Brasília: CEJ, 2003.

HIKAWA, Lígia Yumi. **Da Criminalidade Informática.** 2008. 72 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Faculdades Integradas Antônio Eufrásio de Toledo, Faculdade de Direito de Presidente Prudente, Presidente Prudente, 2008. Disponível em: < http://intertemas.unitoledo.br/revista/index.php/Juridica/article/viewFile/828/805> Acesso em: 01 de mar de 2014.

IRLANDA. Ato do Dano Criminal de 1991. Disponível em: < http://www.irishstatutebook.ie/1991/en/act/pub/0031/sec0005.html#sec5> Acesso em 02 de mar. de 2014. Título original em inglês.

ITÁLIA. Decreto nº 1398 de 13 de outubro de 1930. Código Penal Italiano. Disponível em: < http://www.juareztavares.com/textos/codigoitaliano.pdf> Acesso em: 02 de mar. de 2014. Título original em italiano.

JÚNIOR, Samuel César da Cruz. **A segurança e defesa cibernética no brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual.** Disponível em< http://www.ipea.gov.br/portal/images/stories/PDFs/TDs/td_1850.pdf> Acesso em: 13 ago. 2013.

KOHN, Aaron M. **Computer Criminals**. The Journal of Criminal Law, Criminology and Police Science. Chicago: Police Science, v.60: p. 1-2. Disponível em: < http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=5562&context=jclc > Acesso em: 01 mar. 2014.

LUCCA, Newton; SIMÃO FILHO, Adalberto. **Direito & Internet:** Aspectos Jurídicos Relevantes. 2. Ed. São Paulo:Quartier Latin, 2005.

MARTINS, Thiago de Souza. **Crimes Cibernéticos e a Impunidade Legal**. 2012. 41 f. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação): Unidade Universitária de Ciências Exatas e Tecnológicas, Universidade Estadual de Goiás, Anápolis, 2012. Disponível em: < http://www.unucet.ueg.br/biblioteca/arquivos/monografias/01-TC_-_THIAGO_DE_SOUZA_MARTINS.pdf> Acesso em: 01 mar. 2014.

PAIVA, Luciano Carneiro de. **A prova nos crimes de informática**. Aspectos técnicos e jurídicos. Dissertação.2006

POETA, Patrícia (2012). ‘Sensação de faca no peito’, diz Carolina Dieckmann sobre fotos. **Jornal Nacional**, Rio de Janeiro, 14 maio 2012. Disponível em: < http://g1.globo.com/jornal-nacional/noticia/2012/05/sensacao-de-faca-no-peito-diz-carolina-dieckmann-sobre-fotos.html > Acesso em: 11. Mar. 2014.

PORTUGAL. Constituição (1976). Constituição da República Portuguesa. Disponível em< http://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx> Acesso em: 02 mar. 2014.

PORTUGAL. Lei nº 109 de 17 de Agosto de 1991. Disponível em: < http://www.wipo.int/wipolex/en/text.jsp?file_id=200065> Acesso em: 02 mar. 2014.

_____. Lei nº 59 de 4 de Setembro de 2007. Código Penal. Disponível em: < http://www.hsph.harvard.edu/population/domesticviolence/portugal.penal.95.pdf> Acesso em: 02 mar. 2014.

REINO UNIDO. Ato do mau uso do computador de 1990. Disponível em: <http://www.legislation.gov.uk/ukpga/1990/18/contents> Acesso em 02 mar. 2014. Título original em inglês.

ROCHA, Marcelo Cavalcante**. Cultura Hacker: Tenha Ética E Ganharás Respeito.** Disponível em: < http://blog.marcelocavalcante.net/blog/2008/04/15/cultura-hacker-tenha-etica-e-ganharas-respeito/> Acesso em: 10 de mar. de 2014.

ROQUE, Sérgio Marcos. **Criminalidade Informática: Crimes e Criminosos do Computador**. 1 ed. São Paulo: ADPESP Cultural, 2007.

SCHWARTZ, Richard D; ORLEANS, Sonya. "On Legal Sanctions". *In:* Joel B. Grossman e Mary H. Grossman (eds.), **Law and Change in Modern America**, Pacific Palisades, Califórina, Goodyear Publishing Company, Inc., 1971, pp. 91-7, (Originariamente publicado em **University os Chicago Law Review 34** (1967), pp. 275-300.).

SOUZA, Colombo de (2013). Integrante de quadrilha joinvilense de roubo a caixas eletrônicos é preso em Palhoça. **Notícias do Dia**, Joinville, 20 maio 2013. Disponível em: < http://www.ndonline.com.br/joinville/noticias/72549-integrante-de-quadrilha-joinvilense-de-roubo-a-caixas-eletronicos-e-preso-em-palhoca.html > Acesso em: 11 mar. 2014.

VALENTE et al. (2013).Vídeo mostra momento da invasão do teto do Congresso Nacional. **Folha de São Paulo**, São Paulo, 17 jun. 2013. Disponível em: < http://www1.folha.uol.com.br/multimidia/videocasts/2013/06/1296762-video-mostra-momento-da-invasao-do-teto-do-congresso-nacional.shtml> Acesso em: 10 mar. 2014.

VIANNA, Túlio Lima. **Do delito do dano e sua aplicação ao direito penal informático**. Revista dos Tribunais, São Paulo, a. 92, v.807, janeiro de 2003.

_____, Túlio Lima. **Dos Crimes Por Computador**. Disponível em: < https://www.academia.edu/1911164/Dos_crimes_por_computador > Acesso em: 09 mar. de 2014.

_____, Túlio Lima. **Fundamentos de Direito Penal Informático**. Disponível em: < http://www.academia.edu/1911160/Fundamentos_de_Direito_Penal_Informatico_do_acesso_nao_autorizado_a_sistemas_computacionais> Acesso em: 01 mar. 2014.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012.