UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE DIREITO

CURSO DE DIREITO

ISAAC RODRIGUES RAMOS NETO

A PRÁTICA DO *ETHICAL HACKING* PELOS TIMES DE RESPOSTA A INCIDENTES DE SEGURANÇA COMPUTACIONAL COMO CONDUTA DE LEGÍTIMA DEFESA

FORTALEZA

2013

ISAAC RODRIGUES RAMOS NETO

A PRÁTICA DO *ETHICAL HACKING* PELOS TIMES DE RESPOSTA A INCIDENTES DE SEGURANÇA COMPUTACIONAL COMO CONDUTA DE LEGÍTIMA DEFESA

Monografia apresentada ao Curso de Direito da Faculdade de Direito da Universidade Federal do Ceará, como requisito parcial para obtenção do Título de Bacharel em Direito.

Orientador: Prof. Dr. Nestor Eduardo Araruna Santiago.

FORTALEZA

2013

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Setorial da Faculdade de Direito

R175p Ramos Neto, Isaac Rodrigues.
A prática de ethical hacking pelos times de resposta a incidentes de segurança computacional como conduta de legítima defesa / Isaac Rodrigues Ramos Neto. – 2013.
68 f. : enc. il. ; 30 cm.

Monografia (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2013.
Área de Concentração: Direito Penal.
Orientação: Prof. Dr. Nestor Eduardo Araruna Santiago.

1. Crime por computador. 2. Legítima defesa (Direito). 3. Hackers. I. Santiago, Nestor Eduardo Araruna (orient.). II. Universidade Federal do Ceará – Graduação em Direito. III. Título.

CDD 343

ISAAC RODRIGUES RAMOS NETO

A PRÁTICA DO *ETHICAL HACKING* PELOS TIMES DE RESPOSTA A INCIDENTES DE SEGURANÇA COMPUTACIONAL COMO CONDUTA DE LEGÍTIMA DEFESA

Monografia apresentada ao Curso de Direito da Faculdade de Direito da Universidade Federal do Ceará, como requisito parcial para obtenção do Título de Bacharel em Direito.

Aprovada em: ____/____/_____

BANCA EXAMINADORA

_____

Prof. Dr. Nestor Eduardo Araruna Santiago (Orientador)

Universidade Federal do Ceará (UFC)

_____

Prof. Ms. Márcio Ferreira Rodrigues Pereira

Universidade Federal do Ceará (UFC)

_____

Prof. Ms. Raul Carneiro Nepomuceno

Universidade Federal do Ceará (UFC)

À memória de Isaac Rodrigues Ramos.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, Julgador dos impunes, Defensor dos esquecidos, por ter iluminado o meu caminho em toda essa árdua jornada, não me deixando titubear em nenhuma das escolhas feitas.

Aos meus pais, Rosilda e Sidney, pelo apoio incondicional, preciosas orientações e presença constante.

À minha irmã, Régia Maria, e ao meu cunhado, Marcelo, pela companhia e pelos infindos momentos de descontração.

À minha namorada, Juliana, por ter vivenciado comigo todos os detalhes deste trabalho e partilhado todos os momentos do meu dia-a-dia universitário, por ter me dado o apoio que necessitava nos momentos difíceis, todo carinho, respeito, por ter me tolerado nos momentos de estresse e por tornar minha vida cada dia mais feliz.

Ao meu amigo-irmão, Gustavo, pelas conversas, piadas, causos e auxílio nas incursões no mundo Além-Direito.

Aos colegas de Faculdade, em especial aos amigos Haylton, Joshua, Júlio César e Lai, pela alegria e bom convívio, tornando o ambiente acadêmico bem mais agradável.

Ao Núcleo de Estudos em Ciências Criminais (NECC) e a todos os seus membros pelo aprendizado, disposição e verdadeiro trabalho em equipe.

Ao meu orientador, Prof. Dr. Nestor Eduardo Araruna Santiago, pela condução nos primeiros e essenciais passos da minha formação acadêmica, pelas cobranças, exigências, confiança e por acreditar no potencial desta pesquisa.

Aos professores Márcio Ferreira Rodrigues Pereira e Raul Carneiro Nepomuceno por terem disponibilizado seu precioso tempo para participarem da banca examinadora deste trabalho de conclusão de curso.

A todos os meus professores, em especial aos professores Dimas Macedo, Francisco Luciano Lima Rodrigues, Júlio Carlos Sampaio Neto, Machidovel Trigueiro Filho, Marcos de Holanda, Maria Vital da Rocha, Tarin Cristino Frota Mont'Alverne e Yuri Cavalcante Magalhães, pelo vasto conhecimento compartilhado, inúmeras dúvidas esclarecidas, amizade e paciência.

A todos os meus supervisores de estágio e profissionais exemplares com quem tive a honra de trabalhar, pedindo, aqui, a devida vênia para suprimir os seus títulos, Alberto, Aldemy, Amós, André, Augustino, Cléber, Donato, Fabíola, Getúlio, Giovana, João Paulo,

Jorge, Larissa, Leilyanne, Mairton, Manu, Mariella, Raquel, Ruth, Sergiano, Silvinha, Tibério, e que humildemente ensinaram-me, direta ou indiretamente, valiosas lições tanto jurídicas quanto pessoais.

Por fim, aos colegas de estágio Amanda, Andrea, Antônio César, Júnior, Katerine, Lucas, Milena, Rafaela, Tayanne, Thiago, Vanessa, pela companhia descontraída e familiar durante as longas tardes e, algumas vezes, manhãs de labuta diária.

“O futuro está lá, olhando para trás, em nossa direção. Tentando entender a ficção em que nos transformamos.” (William Gibson)

RESUMO

Pesquisa sobre a possibilidade de configuração de legítima defesa diante da observância da prática do delito de invasão de dispositivo informático na modalidade qualificada, previsto no artigo 154-A, §§ 3º e 4º, do Código Penal. Analisa, inicialmente, a origem e as características da Sociedade da Informação e sua influência no surgimento de novos tipos penais. Apresenta a evolução da legislação brasileira quanto à tipificação daqueles considerados crimes eletrônicos. Expõe as principais características da modalidade qualificada do crime de invasão de dispositivo informático. Debate acerca da prática do *ethical hacking* pelos Times de Resposta a Incidentes de Segurança Computacional e se tal conduta amoldar-se-ia a excludente da legítima defesa. Utiliza a pesquisa doutrinária, legislativa e jurisprudencial. Recorre à internet como forma de complementação dos assuntos estudados. Espera demonstrar, ao final, que o *ethical hacking* poderá configurar hipótese de legítima defesa, desde que obedecidas às restrições destas, sendo o melhor caminho para reduzir os danos gerados pela invasão, pois, uma vez de posse da informação, o agente criminoso pode, fácil e rapidamente, gerar diversas cópias e espraiá-las pela internet, causando danos de improvável reparação.

Palavras-chave: Legítima defesa. Crimes eletrônicos. Invasão de dispositivo informático.

ABSTRACT

Research on the possibility of setting up self-defense against a computing device invasion in the qualified form under Article 154-A, §§ 3º and 4º, of the Brazilian Criminal Code. Initially analyzes the origin and characteristics of the Information Society and its influence on the emergence of new kinds of criminal conduct. Presents the evolution of Brazilian criminal law concerning the definition of electronic crimes. Exposes the main characteristics of the crime of computing device invasion in the qualified form. Debates about the practice of ethical hacking by Computer Security Incident Response Teams and if such conduct would conform to the legal definition of self-defense. Uses the doctrinal, legislative and judicial researches. Uses the internet as a way to complement the studied subjects. In the end, hopes to demonstrate that the ethical hacking can configure hypothesis of self-defense, since obeyed the imposed restrictions, and being the best way to reduce the damage caused by the invasion, because the invader can quickly and easily generate multiple copies of the archives and spread them over the internet once in possession of the information, causing a damage difficult to repair.

Keywords: Self-defense. Electronic crimes. Computing device invasion. Ethical hacking.

SUMÁRIO

1 INTRODUÇÃO

A Revolução Informacional, iniciada nas duas últimas décadas do século XX, caracteriza-se, segundo Castells, pela introdução da geração, do processamento e da transmissão de informações como fontes fundamentais de produtividade e poder por causa das novas condições tecnológicas surgidas nesse período[1], criando-se, assim, um novo paradigma.

Uma das diferenças entre a Revolução Informacional e as Revoluções Industriais dos séculos XVIII e XIX é a amplitude dos seus efeitos. Com os meios de comunicação bem mais avançados do que naquela época em razão da própria revolução, pode-se afirmar que, hoje, um grande número de países já adentrou a era da informação.

Não obstante tenha trazido grandes benefícios para as mais diversas áreas do conhecimento, por exemplo, a bioengenharia, a engenharia genética, a microeletrônica e as telecomunicações, a Revolução Informacional também acarretou um crescimento na ocorrência de crimes eletrônicos. Isso se deveu, especialmente, pela alteração do perfil do agente que comete tais tipos de delitos. O criminoso eletrônico, segundo Monteiro Neto, ostentava a qualidade de "exímio perito na operação de computadores e sistemas computacionais"[2], todavia, hoje, qualquer curioso usuário da internet pode aprender, por meio de diversos tutoriais disponibilizados na *web*, como realizar uma invasão[3]. Assim, considerando que há meios técnicos e jurídicos para identificar o infrator e puni-lo devidamente e que uma vez de posse da informação subtraída o invasor poderia facilmente espraiá-la pela internet, nascem alguns questionamentos: Seria possível reconhecer a legítima defesa, amparada pelo Direito Penal como causa excludente de ilicitude, diante da observância da prática desse delito? Em que situações específicas? Quais seriam seus limites?

O objetivo aqui trazido é o de analisar, à luz do direito penal brasileiro, a possibilidade de configuração de legítima defesa diante da observância da prática do delito de invasão de dispositivo informático em sua modalidade qualificada, tipificada no artigo 154-A, §§ 3º e 4º, do Código Penal. Perceber-se-á que toda a análise realizada é multidisciplinar, porque, se não o fosse, seria incompleta. Valer-se apenas do Direito para entender esse fenômeno seria uma atitude falha.

---

[1] CASTELLS, Manuel. **A Sociedade em Rede**. Vol. 1. 8ª ed. rev. e ampl. Tradução de Roneide Venâncio Majer e Klauss Brandini Gerhardt. – São Paulo: Paz e Terra, 2005, p. 65.

[2] MONTEIRO NETO, João Araújo. Crimes Informáticos: uma abordagem dinâmica ao direito penal informático. **Pensar**, Fortaleza, v. 8, 2003, p. 41. Disponível em: <http://hp.unifor.br/pdfs_notitia/1690.pdf>. Acesso em: 03 jul 2013.

[3] MONTEIRO NETO, *loc. cit.*

A pesquisa tem especial aspecto acadêmico, pois a discussão acerca da até então nomeada "legítima defesa digital" é incipiente, necessitando de análises aprofundadas.

Possui, ainda, relevante aspecto social visto tentar esclarecer se determinada conduta de proteção da informação poderá ser considerada legítima defesa ou não, extravasando seus limites.

Em um primeiro capítulo, intitulado "O Direito penal na sociedade da informação", mostra-se a forte influência da Sociedade da Informação na elaboração de novas leis incriminadoras. Apresentam-se, inicialmente, as origens e as principais características desse novo momento social. Após, são descritos alguns princípios gerais do Direito Penal a serem observados em tempos de necessárias mudanças legislativas. Relata-se a evolução da legislação penal brasileira quanto à tipificação dos delitos eletrônicos, apresentando-se, por último, a inovação trazida pela Lei n. 12.737, de 30 de novembro 2012, qual seja: o delito de invasão de dispositivo informático. Ao final, é apresentada uma tabela comparativa entre a Convenção de Budapeste, a atual legislação penal brasileira e o Anteprojeto do novo Código Penal.

O segundo capítulo trata-se de uma análise do delito de invasão de dispositivo informático em sua modalidade qualificada. São apresentados os bens jurídicos tutelados pelo tipo, bem como seus objetos materiais. Por fim, delineiam-se dois conceitos, o de invasão e o de dispositivo informático, alguns dos elementos estritamente necessários para a devida configuração do crime em apreço.

No terceiro e último capítulo, passa-se a enfrentar o tema efetivamente. Neste momento, será conceituado e analisado o *ethical hacking*, passando-se por todas as suas fases. Será observada também a atuação dos Times de Resposta a Incidentes de Segurança Computacional (CSIRT). Compara-se a atuação destes, quando enfrentam invasões, com a descrição de legítima defesa, prevista no artigo 25 do Código Penal. Finalmente, são demonstradas algumas situações específicas de excessos na prática do *ethical hacking*, descaracterizando-se, nesses casos, a configuração da legítima defesa.

Por fim, antes de serem apresentadas as referências que guiaram a escrita deste trabalho, serão realizadas breves considerações finais, apresentando dois possíveis cenários resultantes do reconhecimento desse novo caso de legítima defesa.

2 O DIREITO PENAL NA SOCIEDADE DA INFORMAÇÃO

Durante a Guerra Fria, no ano de 1969, foi desenvolvido, pelo Departamento de Defesa dos Estados Unidos da América, um sistema de intercomunicação entre os centros de pesquisas norte-americanos e suas bases militares. Tal sistema recebeu o nome de ARPANet, sigla para a expressão inglesa *Advanced Research Projects Agency Network*[4].

A ARPANet nasceu com uma finalidade bélica: alertar o Pentágono o mais rápido possível da possibilidade de um ataque, não os deixando vulneráveis. Ademais, a ARPANet possuía o objetivo de proteger as informações. Assim, uma vez destruída alguma base, as informações coletadas por elas estariam armazenadas na rede e não se perderiam. Anos mais tarde, a ARPANet passou a também ser utilizada por universidades que pesquisavam temáticas relacionadas à defesa nacional.

A ARPANet é considerada o ancestral da internet. Esta, por sua vez, veio a se popularizar com o desenvolvimento, por Tim Berners-Lee e Robert Cailliau, da *World Wide Web*, o tão conhecido "www", e a criação dos *browsers*, navegadores, que facilitaram a utilização da internet por usuários inexperientes. A Internet, segundo pesquisa relativa ao mês de junho de 2012, é utilizada por cerca de 2,4 bilhões de pessoas[5].

Assim, pouco a pouco, a ideia de ciberespaço cunhada por William Gibson, em sua obra *Neuromancer*, passou a se tornar realidade.

> Ciberespaço. Uma alucinação consensual vivenciada diariamente por bilhões de operadores autorizados, em todas as nações, por crianças que estão aprendendo conceitos matemáticos... uma representação gráfica de dados abstraídos dos bancos de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz alinhadas no não espaço da mente, aglomerados e constelações de dados. Como luzes da cidade, se afastando...[6]

O advento da internet reconfigurou a sociedade, agora comumente intitulada de "Sociedade da Informação".

Nessa nova fase, o fluxo de informação evoluiu tanto qualitativamente como quantitativamente. No aspecto qualitativo, observa-se a crescente velocidade dessas trocas. Em poucos milissegundos, dados são transferidos de um canto a outro do globo. No aspecto

---

[4] MATTELART, Armand. **Historia da Sociedade da Informação**. Traduzido por Nicolas Nyimi Campanario. – São Paulo: Edições Loyola, 2002, p. 62-63

[5] INTERNET WORLD STATS. **Internet Usage Statistics**. Disponível em: <http://www.internetworldstats.com/stats.htm>. Acesso em: 03 jul 2013.

[6] GIBSON, William. **Neuromancer**. Traduzido por Fábio Fernandes. 4ª ed. – São Paulo : Aleph, 2008, p. 77.

quantitativo, destaca-se o grande volume de trocas de informações. Costumou-se dizer que, hoje, um homem médio tem acesso, em um único dia, a informações que um indivíduo comum da Idade Média absorveria em uma vida. Pode-se facilmente, com simples toques, consultar informações sobre acontecimentos em diversos países, sendo, em alguns casos, transmitidas em tempo real, dando uma nova significação a ideia toyotista do *just in time*[7].

Entretanto, a Rede Mundial de Computadores não só trouxe vantagens para aqueles que dela se utilizam para aumentar seus conhecimentos. A evolução dessa tecnologia revelou grandes oportunidades para outros que, aproveitando-se do falso sentimento de anonimato, passaram a cometer crimes. Destacam-se, entre tais condutas, os crimes contra a honra, de preconceito e de divulgação e venda de pornografia infantil. Apesar da grande incidência e destaque desses delitos no meio digital, não se permite olvidar que, atualmente, duas novas preocupações surgiram: as condutas que afetam a segurança das informações e o alcance do Direito Penal sobre aquelas.

2.1 A nova Sociedade da Informação

São várias as nomenclaturas utilizadas para nomear essa nova fase da sociedade: Pós-Industrial, Virtual, Global, em Rede, do Conhecimento, da Aprendizagem, Informacional e, por último e mais comum, da Informação.[8]

Antes de se determinar um conceito para a Sociedade da Informação, é preciso esclarecer que, em todas as fases que antecederam esta, a informação e o conhecimento foram também molas propulsoras para o seu desenvolvimento[9]. Todavia, esses elementos, no momento atual, têm destaque e consequências nunca antes vistos, como será destacado adiante. Nessa linha, Castells prefere o complemento *informacional* ao *de informação*.

---

[7] CANONGIA, Claudia; MANDARINO JÚNIOR, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, Brasília, v. 14, n. 29, dez. 2009, p. 22. Disponível em: <http://www.cgee.org.br/parcerias/p29.php>. Acesso em: 03 jul 2013.

[8] GONZÁLEZ, Ignacio Siles. Cibernética y sociedad de la información: el retorno de un sueño eterno. **Signo y Pensamiento**, Bogotá, n. 50, jun. 2007, p. 86. Disponível em: <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-48232007000100007&lang=pt>. Acesso em: 03 jul 2013.

[9] MARTI, Yohannis; VEGA-ALMEIDA, Rosa Lidia. Sociedad de la información: Los mecanisnos reguladores en el contexto de una sociedad emergente. **Ciência da Informação**, Brasília, v. 34, n. 1, jan./abr. 2005, p. 38. Disponível em: <http://www.scielo.br.ez11.periodicos.capes.gov.br/pdf/ci/v34n1/a05v34n1.pdf>. Acesso em: 03 jul 2013.

> Gostaria de fazer uma distinção entre as noções de "sociedade da informação" e "sociedade informacional" com conseqüências similares para economia da informação e economia informacional. O termo sociedade da informação enfatiza o papel da informação na sociedade. Mas afirmo que informação, em seu sentido mais amplo, por exemplo, como comunicação de conhecimentos, foi crucial a todas as sociedade, inclusive à Europa medieval que era culturalmente estruturada e, até certo ponto, unificada pelo escolasticismo, ou seja, no geral uma infra-estrutura intelectual (ver Southern 1995). Ao contrário, o termo informacional indica o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico. Minha terminologia tenta estabelecer um paralelo com a distinção entre indústria e industrial.[10]

2.1.1 Conceito e características

A definição de Sociedade da Informação ainda permeia uma zona obscura, visto ainda haver alguns que defendem a sua não existência[11]. Entretanto, para aqueles que estão do lado oposto, é certo dizer que a Sociedade da Informação, ou qualquer outra denominação que porventura utilizem, é resultado de uma forte convergência da base tecnológica, podendo hoje quase tudo ser representado no formato digital[12].

O Livro Verde para a Sociedade da Informação em Portugal conceitua essa nova fase como sendo

> um modo de desenvolvimento social e económico em que a aquisição, armazenamento, processamento, valorização, transmissão, distribuição e disseminação de informação conducente à criação de conhecimento e à satisfação das necessidades dos cidadãos e das empresas, desempenham um papel central na actividade económica, na criação de riqueza, na definição da qualidade de vida dos cidadãos e das suas práticas culturais. A sociedade da informação corresponde, por conseguinte, a uma sociedade cujo funcionamento recorre crescentemente a redes digitais de informação. Esta alteração do domínio da actividade económica e dos factores determinantes do bem-estar social é resultante do desenvolvimento das novas tecnologias da informação, do audiovisual e das comunicações, com as suas

[10] CASTELLS, Manuel. **A Sociedade em Rede**. Vol. 1. 8ª ed. rev. e ampl. Tradução de Roneide Venâncio Majer e Klauss Brandini Gerhardt. – São Paulo: Paz e Terra, 2005, p. 64-65.
[11] GONZÁLEZ, Ignacio Siles. Cibernética y sociedad de la información: el retorno de un sueño eterno. **Signo y Pensamiento**, Bogotá, n. 50, jun. 2007, p. 87. Disponível em: <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-48232007000100007&lang=pt>. Acesso em: 03 jul 2013.
[12] BRASIL. **Sociedade da Informação no Brasil**: Livro Verde. Brasília : Ministério da Ciência e Tecnologia, 2000, p. 5. Disponível em <http://www.mct.gov.br/index.php/content/view/18878.html>. Acesso em: 03 jul 2013.

> importantes ramificações e impactos no trabalho, na educação, na ciência, na saúde, no lazer, nos transportes e no ambiente, entre outras.[13]

Infere-se desse conceito as cinco características basilares, elencadas por Castells: a informação como matéria-prima, a alta penetrabilidade dos efeitos das novas tecnologias, o predomínio da lógica de redes, a flexibilidade e a crescente convergência de tecnologia[14].

2.1.1.1 A informação como matéria-prima

A informação é considerada um ativo de valor, mais especificamente um bem intangível. Segundo Fontes, ela pode ser conceituada como resultado da transformação de dados, os quais, inicialmente, possuem pouco significado, em algo de valor[15].

Anteriormente, como assevera Castells, a informação era meramente utilizada para o desenvolvimento de novas tecnologias e seus aprimoramentos. Hoje, ocorre justamente o oposto: as tecnologias são desenvolvidas visando a auxiliar o homem no tratamento das próprias informações[16].

A informação, hoje, tem um papel tão importante que, no mês de junho de 2013, foi revelado, por Edward Snowden, um projeto norte-americano de monitoramento, denominado PRISM. Em suma, o projeto PRISM vigiava incessantemente ligações telefônicas, transações realizadas com cartão de crédito, trocas de e-mails, movimentações em redes sociais[17]. Outro exemplo foi a forte vigilância realizada pela Agência Brasileira de Inteligência (ABIn) nas redes sociais após o início das manifestações populares, conhecidas popularmente por "Revolta do Vinagre"[18].

---

[13] PORTUGAL. **Livro verde para a sociedade da informação em Portugal**. Lisboa: Ministério da Ciência e da Tecnologia, Missão para a Sociedade da Informação, 1997, p. 5. Disponível em <http://www2.ufp.pt/~lmbg/formacao/lvfinal.pdf>. Acesso em: 03 jul 2013.

[14] CASTELLS, Manuel. **A Sociedade em Rede**. Vol. 1. 8ª ed. rev. e ampl. Tradução de Roneide Venâncio Majer e Klauss Brandini Gerhardt. – São Paulo: Paz e Terra, 2005, p. 108-109.

[15] FONTES, Edison. **Segurança da Informação**: O usuário faz a diferença. – São Paulo : Saraiva, 2006, p. 2.

[16] CASTELLS, *op. cit.*, p. 108.

[17] KARASINSKI, Lucas. PRISM: entenda toda a polêmica sobre como os EUA controlam você. **Tecmundo**. Disponível em: <http://www.tecmundo.com.br/privacidade/40816-prism-entenda-toda-a-polemica-sobre-como-os-eua-controlam-voce.htm>. Acesso em: 03 jul 2013.

[18] Abin monta rede para monitoramento dos protestos. **O Povo**. Disponível em: <http://www.opovo.com.br/app/opovo/radar/2013/06/20/noticiasjornalradar,3077693/abin-monta-rede-para-monitoramento-dos-protestos.shtml>. Acesso em: 03 jul 2013.

A grande consequência dessa importância conferida às informações é justamente a necessidade do desenvolvimento de normas que busquem a assegurar sua proteção e devida utilização.

2.1.1.2 A alta penetrabilidade dos efeitos das novas tecnologias

Por alta penetrabilidade dos efeitos das novas tecnologias, deve-se entender que, como a informação faz parte das mais diversas atividades humanas, estas acabam sendo diretamente afetadas.

A implantação da estratégia de governo eletrônico em diversos países é uma forma de manifestação dessa característica, contribuindo, assim, para uma melhoria dos serviços públicos[19]. Hoje, pode-se facilmente, no Brasil, fazer a declaração de Imposto de Renda sem a necessidade de qualquer deslocamento. Os processos dos Juizados Especiais Federais tramitam em meio digital, não sendo necessários espaços físicos para acomodar pilhas e mais pilhas de autos. Consultas jurisprudenciais, antes feitas em livros de volumosos tomos, podem ser realizadas em sítios eletrônicos.

Portanto, a informação colabora para que os novos efeitos trazidos pelas recentes tecnologias espalhem-se na sociedade de modo rápido e eficaz.

2.1.1.3 O predomínio da lógica de redes

A lógica do funcionamento de redes tem como símbolo a internet. O seu advento fez com que dispositivos informáticos, que antes funcionavam de forma autônoma, evoluíssem para uma fase de "computação universal", podendo todos estar interconectados. Segundo Castells, "a lógica do funcionamento de redes [...] tornou-se aplicável a todos os tipos de atividades, a todos os contextos e a todos os locais que pudessem ser conectados

[19] MONTEIRO, Renato Leite. **Crimes eletrônicos**: uma análise econômica e constitucional. 2010. Dissertação (Mestrado em Direito) - Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2010, p. 32.

eletronicamente"[20]. Mattelart assevera que se está em "uma era em que processos políticos se tornaram globais"[21].

Castells afirma ainda que

> [...] quando as redes se difundem, seu crescimento se torna exponencial, pois as vantagens de estar na rede crescem exponencialmente, graças ao maior número de conexões, e o custo cresce em padrão linear. Além disso, a penalidade por estar fora da rede aumenta com o crescimento da rede em razão do número em declínio de oportunidades de alcançar outros elementos fora da rede.[22]

Com efeito, as alegações de Castells e Mattelart, hoje, são uma verdade incontestável. De posse de um *smartphone*, pode-se, por meio de redes *wireless*, a exemplo da 3G, realizar atividades profissionais, consultar e enviar e-mails, ler notícias, sendo a transmissão de voz apenas mais um serviço oferecido pelas operadoras. Em outros termos, vive-se conectado a um "meio ambiente global"[23].

2.1.1.4 A flexibilidade

A característica da flexibilidade revela a ideia de que as novas tecnologias podem ser facilmente modificadas, reorganizadas, reconfiguradas, favorecendo, assim, o seu desenvolvimento. E, ainda, caso não demonstre os efeitos desejados, tais processos podem ser revertidos[24].

Como consequência, tem-se um aumento crescente na quantidade de inovações tecnológicas, bem como em sua qualidade. É bastante comum, por exemplo, haver a utilização de programas, ainda em fase de testes, por potenciais usuários, a fim de que estes deem sua opinião acerca daqueles, podendo ser corrigido e aprimorado. Outro exemplo é o caso de distribuição de sistemas operacionais aos desenvolvedores de aplicativos, para que elaborem programas diversos com base naquele sistema.

---

[20] CASTELLS, Manuel. **A Sociedade em Rede**. Vol. 1. 8ª ed. rev. e ampl. Tradução de Roneide Venâncio Majer e Klauss Brandini Gerhardt. – São Paulo : Paz e Terra, 2005, p. 89.
[21] MATTELART, Armand. **Historia da Sociedade da Informação**. Traduzido por Nicolas Nyimi Campanario. – São Paulo : Edições Loyola, 2002, p. 100.
[22] CASTELLS, *op. cit.*, p. 108.
[23] *Ibid.*, p. 133.
[24] WERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ciência da Informação**, Brasília, v. 29, n. 2, maio/ago. 2000, p. 73-74. Disponível em: <http://www.scielo.br.ez11.periodicos.capes.gov.br/scielo.php?script=sci_arttext&pid=S0100-19652000000200009&lng=pt&nrm=iso&tlng=pt>. Acesso em: 03 jul 2013.

Nesse aspecto, a Sociedade da Informação traz uma possibilidade bem mais ampla de aproveitamento da criatividade humana.

2.1.1.5 A crescente convergência de tecnologia

A convergência de tecnologia representa a interdependência de diversos campos do conhecimento. Biologia, direito, eletrônica, engenharia, informática, medicina, telecomunicações, antes áreas tão distantes, estão cada vez mais próximas[25].

Nesse sentido, ensina Castells que

> A convergência tecnológica transforma-se em uma interdependência crescente entre as revoluções em biologia e microeletrônica, tanto em relação a materiais quanto a métodos. Assim, avanços decisivos em pesquisas biológicas, como a identificação dos genes humanos e segmentos do DNA humano só conseguem seguir adiante por causa do grande poder da informática.[26]

Essa crescente convergência, por exemplo, resultou na disseminação dos métodos de educação à distância, em especial o *e-learning*, e novos métodos de ensino, como o ensino híbrido[27]. É comum hoje se fazer cursos superiores e pós-graduações em quase sua totalidade *online*, por meio de aulas transmitidas ou não ao vivo, podendo, em determinados casos, assisti-las em seu próprio lar, necessitando apenas deslocar-se para a realização de algumas provas. A Organização Mundial da Propriedade Intelectual, por exemplo, conta com um centro de *e-learning*[28], no qual são disponibilizados diversos cursos, gratuitos ou pagos, realizados pela internet.

---

[25] WERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ciência da Informação**, Brasília, v. 29, n. 2, maio/ago. 2000, p. 74. Disponível em: <http://www.scielo.br.ez11.periodicos.capes.gov.br/scielo.php?script=sci_arttext&pid=S0100-19652000000200009&lng=pt&nrm=iso&tlng=pt>. Acesso em: 03 jul 2013.

[26] CASTELLS, Manuel. **A Sociedade em Rede**. Vol. 1. 8ª ed. rev. e ampl. Tradução de Roneide Venâncio Majer e Klauss Brandini Gerhardt. – São Paulo : Paz e Terra, 2005, p. 110.

[27] Cf. MOREIRA, Thiago Freire Feijão. **Série de Diálogos**: Tecnologia na Educação - Ensino Híbrido. Disponível em: <http://www.youtube.com/watch?v=MQpcqnXwnMY>. Acesso em: 03 jul 2013.

[28] *Cf*. ORGANIZAÇÃO MUNDIAL DA PROPRIEDADE INTELECTUAL. Sítio eletrônico do Centro de *e-learning*. Disponível em: <http://www.wipo.int/academy/pt/courses/distance_learning/catalog/welc.html>. Acesso em: 03 jul 2013.

2.2 Direito Penal e Sociedade da Informação

Diante das transformações acima destacadas, o Direito, como Ciência Social Aplicada, terá, necessariamente, de acompanhar tais mudanças, a fim de se adequar à atual realidade, bem como aos conflitos que dela surgirão. Todavia, há ramos do Direito não dotados de maleabilidade, sendo necessária a criação de novas leis, a exemplo do Direito Penal, a *ultima racio legis*.

Para esclarecer o porquê da elaboração de novas normas penais e da inaplicabilidade de algumas já existentes aos novos fatos, destacar-se-á adiante alguns princípios, que nortearão a aplicação e o desenvolvimento do Direito Penal diante do novo cenário social.

2.2.1 Princípios da legalidade e da reserva legal

Embora alguns autores conceituem de modo idêntico os princípios da legalidade e da reserva legal[29], tal posicionamento será aqui afastado, fazendo-se necessário observar as suas diferenças.

O princípio da legalidade está previsto no art. 5º, II, da Constituição Federal, dispondo que "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei". Já o princípio da reserva legal está previstos no art. 5º, XXXIX, da Constituição Federal, e art. 1º do Código Penal, os quais possuem o mesmo teor: "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal".

Nesse sentido, leciona Silva que

> A doutrina não raro confunde ou não distingue suficientemente o *princípio da legalidade* e o da *reserva de lei*. O primeiro significa a submissão e o respeito à lei, ou a atuação dentro da esfera estabelecida pelo legislador. O segundo consiste em estatuir que a regulamentação de determinadas matérias há de fazer-se necessariamente por lei formal. [...] Em verdade, o problema das relações entre os princípios da legalidade e da reserva de lei resolve-se com base no Direito Constitucional positivo, à vista do poder que a Constituição outorga ao Poder Legislativo. Quando essa outorga consiste no poder amplo e geral sobre qualquer

[29] PRADO, Luiz Régis. **Curso de direito penal brasileiro**, parte geral: arts. 1º a 120. 8ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2009, v. 1, p. 130. Nesse sentido, BITENCOURT, Cezar Roberto. **Tratado de Direito Penal** – Parte Geral, vol. 1. 14ª ed. rev., atual. e ampl. – São Paulo : Saraiva, 2009, p. 10.

> espécie de relações, como vimos antes, tem-se o princípio da legalidade. Quando a constituição reserva conteúdo específico, caso a caso, à lei, encontramo-nos diante do princípio da reserva legal.[30] (grifos originais).

O princípio da reserva legal, desse modo, estabelece que alguns temas deverão ser regidos por lei em sentido estrito, não sendo permitida, por exemplo, a utilização de medidas provisórias. Diferencia-se do princípio da legalidade, pois este trata da atuação pautada na lei, dentro de seus limites[31].

Como consequência dos dois princípios, tem-se o princípio da taxatividade e a vedação da aplicação da analogia *in malam partem*.

O princípio da taxatividade está pautado na expressão *nullum crimen, nulla poena sine praevia lege certa*. Esse princípio reforça a segurança jurídica, evitando surpresas indesejadas na aplicação da lei penal. Assim, na lição de Prado, o "seu fundamento político radica principalmente na função de garantia da liberdade do cidadão ante a intervenção estatal arbitrária, por meio da realização da certeza do direito"[32]. Tal princípio também é direcionado à atividade judicante, estabelecendo limites à função de julgar.

> Pela taxatividade, busca-se estabelecer as margens penais às quais está vinculado o julgador. Isso vale dizer: deve ele interpretar e aplicar a norma penal incriminadora nos limites estritos em que foi formulada, para satisfazer a exigência de garantia, evitando-se eventual abuso judicial.[33]

Quanto à aplicação da analogia *in malam partem*, entende-se que

> [...]completar o texto legal de maneira a estendê-lo para proibir o que a lei não proíbe, considerando antijurídico o que a lei justifica, ou reprovável o que ela não reprova ou, em geral, punível o que não é por ela penalizado, baseando a conclusão em que proíbe não justifica ou reprova condutas similares, este procedimento de interpretação é absolutamente vedado no campo da elaboração científico-jurídica do direito penal.[34]

Exemplo claro de aplicação da analogia a fim de prejudicar o réu, seria o caso de a conduta hoje prevista no artigo 154-A, § 3º, do CP, qual seja, invasão de dispositivo informático qualificada, ser enquadrada como furto simples (artigo 155, caput, do CP) ou furto qualificado pelo rompimento de obstáculo à subtração (artigo 155, §4º, I, do CP). Entretanto, tal raciocínio não poderia ser realizado, pois se estaria ampliando o conceito de

---

[30] SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 32ª ed. rev., atual. e ampl. – São Paulo : Malheiros, 2009, p. 422.
[31] SILVA, *loc. cit.*
[32] PRADO, Luiz Régis. **Curso de direito penal brasileiro**, parte geral: arts. 1º a 120. 8ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2009, v. 1, p. 131.
[33] *Ibidem*, p. 133.
[34] ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro**: parte geral. 6ª ed. rev. e atual. – São Paulo: Revista dos Tribunais, 2006, p. 151.

coisa móvel para abarcar o de arquivo digital, bem como o conceito de obstáculo, que traz uma ideia de construção física, para englobar o de sistema de segurança de dados.

2.2.2 Princípio da intervenção mínima

Por este princípio, deve-se entender o Direito Penal como *ultima ratio*, última solução a ser utilizada, devendo apenas cuidar daquelas situações que os demais ramos do Direito protegem de forma insuficiente, não se admitindo um caminho menos gravoso para sua proteção.

Nesse sentido, conforme ensina Bitencourt, o princípio da intervenção mínima preconiza que

> [...] a *criminalização* de uma conduta só se legitima se constituir meio necessário para a proteção de determinado bem jurídico. Se outras formas de sanção ou outros meios de controle social revelarem-se suficientes para a tutela desse bem, a sua criminalização é inadequada e não recomendável. Se para o restabelecimento da ordem jurídica violada forem suficientes medidas civis ou administrativas, são estas que devem ser empregas e não as penais.[35] (grifos originais)

Do conceito ora apresentado surgem outros três princípios: o da fragmentariedade, o da exclusiva proteção de bens jurídicos e o da adequação social.

O princípio da fragmentariedade está relacionado com o caráter subsidiário da proteção oferecida pelo Direito Penal. Está não é absoluta, e sim apenas relativa, pois um bem jurídico tutelado por uma lei penal também o é pelos demais campos do Direito[36].

Pelo princípio da exclusiva proteção de bens jurídicos, tem-se que "não há delito sem que haja lesão ou perigo de lesão a um bem jurídico determinado"[37].

Por fim, o princípio da adequação social garante que as condutas aceitas e toleradas na sociedade não sejam objeto de leis penais, justamente pela já citada característica de *ultima racio* que as revestem. Nos dizeres de Greco,

> [...] encontra-se o legislador, na qualidade de pesquisador e selecionador das condutas ofensivas aos bens jurídicos mais importantes e necessários ao convívio em sociedade, impedido de criar tipos penais incriminadores que proíbam condutas que

---

[35] BITENCOURT, Cezar Roberto. **Tratado de Direito Penal** – Parte Geral, vol. 1. 14ª ed. rev., atual. e ampl. – São Paulo : Saraiva, 2009, p. 13.
[36] PRADO, Luiz Régis. **Curso de direito penal brasileiro**, parte geral: arts. 1º a 120. 8ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2009, v. 1, p. 138.
[37] *Ibidem*, p. 136.

> já estejam perfeitamente aceitas e toleradas por essa mesma sociedade, pois, caso contrário, estaria, na verdade, compelindo a população a cometer crimes, uma vez que, estando a sociedade acostumada a praticar determinados comportamentos, não mudaria a sua normal maneira de ser pelo simples fato do surgimento de uma lei penal que não teve a sensibilidade suficiente para discernir condutas inadequadas socialmente daquelas outras que não são toleradas pela sociedade.[38]

Por exemplo, uma corrente minoritária indica que a comercialização de cópias não autorizadas de CDs e DVDs por vendedores ambulantes, popularmente conhecida por "pirataria", não mais causa estranheza à população, funcionando algumas vezes como difusora de cultura, garantindo o direito de acesso ao conhecimento, o direito à educação, o direito à igualdade e a função social da propriedade intelectual[39]. Nesse sentido, o voto do Desembargador Herbert Carneiro:

> Não se ignora a necessidade de efetivo combate à reprodução e comercialização de produtos falsificados. Todavia, sobre a questão, o Estado se vê longe de uma atuação coerente, e é tido por muitos como um dos maiores fomentadores da atividade classificada como ilícita.
> Artigos pirateados e contrabandeados são comercializados a todo instante, com aceitação de elevada parcela da sociedade, grande consumidora desses produtos, e, diga-se, pelo próprio Estado que, ao invés de coibir esse comércio, o incentiva, autorizando a abertura dos denominados "shoppings populares", cujos carros chefes são as mercadorias pirateadas.
> Diante desse quadro, traduz-se verdadeira incoerência punir penalmente o acusado, que expunha à venda, com intuito de lucro, DVD's falsificados, se os outros meios de repressão ainda não estão sendo utilizados com veemência. Nem se diga seja suficiente a atuação da Receita Federal e dos demais órgãos de fiscalização existentes.[40]

Todavia, tal conduta encontra-se tipificada no artigo 184, § 2º, do CP, por violar direito patrimonial decorrente dos direitos autorais. Tal posicionamento está pacificado no Superior Tribunal de Justiça, conforme voto do Ministro Marco Aurélio Belizze:

> É inaceitável, portanto, a aplicação do princípio da adequação social à hipótese, pois a prática rotineira da pirataria no país não tem o condão de impedir a incidência do tipo previsto no art. 184, § 2º, do Código Penal, diante da relevância jurídica da conduta.[41]

---

[38] GRECO, Rogério. **Direito Penal do Equilíbrio**: uma visão minimalista do Direito Penal. 5ª ed. – Niterói : Impetus, 2010, p. 83-84.

[39] MARTINS, Matheus Barcelos; PAZÓ, Cristina Grobério. Acesso ao conhecimento no âmbito digital em face dos direitos autorais. **Revista do Conselho da Justiça Federal**, Centro de Estudos Judiciários, Brasília, Ano XVI, nº 56, jan./abr. 2012, p. 83-84.

[40] BRASIL. Tribunal de Justiça de Minas Gerais. APELAÇÃO CRIMINAL - VIOLAÇÃO DE DIREITO AUTORAL - PRINCÍPIO DA ADEQUAÇÃO SOCIAL - CASO CONCRETO - ABSOLVIÇÃO DECRETADA - RECURSO PROVIDO. Apelação Criminal nº 1.0210.07.046952-8/001. Rel. Des. Doorgal Andrada. Publicado em: 16 jun. 2010.

[41] BRASIL. Superior Tribunal de Justiça. AGRAVO REGIMENTAL. RECURSO ESPECIAL. PENAL. VIOLAÇÃO DE DIREITO AUTORAL. REJEIÇÃO DA DENÚNCIA. PRINCÍPIO DA ADEQUAÇÃO SOCIAL QUE NÃO SE APLICA. AgRg no REsp 1356243/MS. Rel. Min. Marco Aurélio Belizze. Publicado em: DJe, 18 mar. 2013.

Diante dos princípios aqui elencados, conclui-se que a informação é um bem jurídico a ser tutelado pelo Direito Penal, principalmente numa era em que aquela é agraciada de tamanha importância, influenciando nas mais diversas relações.

2.2.3 Evolução legislativa no Brasil

Diante das restrições acima elencadas, tanto de elaboração legislativa como de interpretação do texto normativo penal, correto dizer que, com as mudanças comportamentais trazidas pelo advento da Sociedade da Informação, a legislação penal brasileira certamente sofreu alterações.

A primeira delas[42], a Lei n. 8.137, de 27 de dezembro de 1990, que define os crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências, prevê que

> Art. 2° Constitui crime da mesma natureza:
> I - fazer declaração falsa ou omitir declaração sobre rendas, bens ou fatos, ou empregar outra fraude, para eximir-se, total ou parcialmente, de pagamento de tributo;
> II - deixar de recolher, no prazo legal, valor de tributo ou de contribuição social, descontado ou cobrado, na qualidade de sujeito passivo de obrigação e que deveria recolher aos cofres públicos;
> III - exigir, pagar ou receber, para si ou para o contribuinte beneficiário, qualquer percentagem sobre a parcela dedutível ou deduzida de imposto ou de contribuição como incentivo fiscal;
> IV - deixar de aplicar, ou aplicar em desacordo com o estatuído, incentivo fiscal ou parcelas de imposto liberadas por órgão ou entidade de desenvolvimento;
> **V - utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública.**
> Pena - detenção, de 6 (seis) meses a 2 (dois) anos, e multa.[43] (grifos não originais)

Em 1996, a Lei n. 9.296 regulou o disposto no artigo 5º, XII, da Constituição Federal, e previu, em seu artigo 10, o crime de "interceptação de comunicações telefônicas, de

[42] MONTEIRO NETO, João Araújo. **Aspectos constitucionais e legais do crime eletrônico**. 2008. Dissertação (Mestrado em Direito) – Centro de Ciências Jurídicas, Universidade de Fortaleza, 2008, p. 119.
[43] BRASIL. Lei n. 8.137, de 27 de dezembro de 1990. Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8137.htm>. Acesso em: 03 jul 2013.

informática ou telemática, [...] sem autorização judicial ou com objetivos não autorizados em lei"[44].

Em 1997, houve a sanção da Lei n. 9.504, que dispõe sobre as normas aplicadas às eleições. Tal lei tornou-se necessária devido ao início da implantação, em 1996, da urna eletrônica, surgindo, assim, o voto eletrônico.

Em seu artigo 72, a supracitada lei prevê:

> Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos:
> **I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos;**
> **II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral;**
> III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.[45] (grifos não originais)

Percebe-se, nos incisos I e II, o surgimento da preocupação em proteger a integridade dos votos, os quais, agora, são informações armazenadas em sistema informatizado.

Em 1999, é apresentado o Projeto de Lei n. 84/1999, que tipificava as condutas de dano a dado ou programa de computador; acesso indevido ou não autorizado; alteração de senha ou mecanismo de acesso a programa de computador ou dados; obtenção indevida ou não autorizada de dado ou instrução de computador; violação de segredo armazenado em computador em computador, meio magnético, de natureza magnética, óptica ou similar; criação, desenvolvimento ou inserção em computador de dados ou programa de computador nocivos; e, por fim, veiculação de pornografia através de rede de computadores.[46]

Este projeto e suas posteriores alterações sofreram duras críticas, pois não houve participação efetiva de profissionais da ciência da computação e previram penas bastante rígidas para os delitos. Nesse sentido, Vianna sugere a substituição da pena de prisão por uma

---

[44] BRASIL. Lei n. 9.296, de 24 de julho de 1999. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 03 jul 2013.

[45] BRASIL. Lei n. 9.504, de 30 de setembro de 1997. Estabelece normas para as eleições. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9504.htm>. Acesso em: 03 jul 2013.

[46] BRASIL. Projeto de Lei nº 84, de 24 de fevereiro de 1999. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>. Acesso em: 03 jul 2013.

pena de prestação de serviços à comunidade[47], inovando ao colocar uma pena restritiva de direitos diretamente no preceito secundário de um tipo penal.

O PL n. 84/1999 foi convertido na singela Lei Ordinária n. 12.735, de 30 de novembro de 2012, que, em seu artigo 4º, previu que "os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado", e, em seu artigo 5º, alterou o disposto no artigo 20, § 3º, inciso II, da Lei 7.716/89, para acrescentar ao inciso a cessação de transmissões eletrônicas ou por qualquer outro meio de manifestações discriminatórias.

Ao reverso do projeto anteriormente analisado, o PL n. 2793/2011[48], conhecido popularmente por "Lei Carolina Dieckmann", apesar de apresentado tempos antes do caso de divulgação das fotos íntimas da atriz, teve uma maior participação de profissionais especializados, tentando-se evitar, assim, possíveis falhas técnicas.

O PL n. 2793/2011 foi convertido na Lei n. 12.737, de 30 de novembro de 2012, acrescentando ao Código Penal (CP) os artigos 154-A e 154-B. O primeiro tipifica a conduta de invasão de dispositivo informático, e o segundo estabelece que a ação será pública condicionada a representação, salvo o crime tenha sido praticado contra a Administração Pública. Acrescenta ao artigo 266 do CP a conduta de interromper, impedir ou dificultar o restabelecimento de serviço telemático ou de informação de utilidade pública. E, finalmente, equipara a documento particular os cartões de débito ou crédito, para fins de configuração da conduta típica de falsificação de documento particular (CP, artigo 298).

O último projeto em destaque é o PLS n. 236/2012, referente à reforma do CP. O novo CP tenta reunir é um único corpo legal tipos penais já previstos tanto no atual quanto em legislações extravagantes, ainda trazendo novos crimes. Importante ressaltar que, pelo novo texto legal, a prática de diversas condutas pela internet está devidamente tipificada. Destacam-se:

> Interceptação ilícita
> Art. 154. [...]
> Revelação ilícita [...]
> § 3º Aumenta-se a pena de um terço até a metade:

[47] VIANNA, Túlio Lima. **Fundamentos de direito penal informático**: do acesso não autorizado a sistemas computacionais. – Rio de Janeiro : Forense, 2003, p. 91.

[48] BRASIL. Projeto de Lei nº 2793, de 29 de novembro de 2011. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>. Acesso em: 03 jul 2013.

> I – se a divulgação ilícita for feita por meio da imprensa, rádio, televisão, **internet** ou qualquer outro meio que facilite a sua propagação; ou [...]
> Violação de direito autoral
> Art. 172. [...]
> Violação de direito autoral qualificada em primeiro grau
> § 2º Oferecer ao público, mediante cabo, fibra ótica, satélite, ondas, **internet**, sistema de informática ou qualquer outro que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente:
> Pena – prisão, de um a quatro anos. [...]
> Capítulo V
> Do racismo e dos crimes resultantes de preconceito e discriminação
> Art. 472. [...]
> VII – praticar, induzir ou incitar a discriminação ou preconceito, pela fabricação, comercialização, veiculação e distribuição de símbolos, emblemas, ornamentos, distintivos ou propaganda que a indiquem, inclusive pelo uso de meios de comunicação e **internet**. [...]
> Divulgação de cena de sexo
> Art. 495. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, **inclusive por meio de sistema de informática ou telemático**, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – prisão, de três a seis anos.
> § 1o Nas mesmas penas incorre quem: [...]
> II – assegura, por qualquer meio, o acesso por **rede de computadores** às fotografias, cenas ou imagens de que trata o caput deste artigo.
> Simulação de cena de sexo
> Art. 497. [...]
> Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga **por qualquer meio**, adquire, possui ou armazena o material produzido na forma do caput deste artigo[49]. (grifos não originais).

Concomitante ao início das discussões no Brasil acerca dos crimes digitais, o Conselho Europeu elaborou, em 2001, a Convenção sobre o Cibercrime[50], também conhecida por Convenção de Budapeste. O tratado entrou em vigor no dia 1º de julho de 2004 e foi assinado por 43 países, sendo quatro deles de fora do Conselho. Entretanto, foi apenas ratificado por 12[51]. A Convenção orienta os países a tipificarem uma série de condutas por ela previstas. Além disso, indica meios de cooperação judicial e normas de processo penal.

Apesar de o Brasil não ser signatário da Convenção, as condutas por ela elencadas já possuem, em sua maioria, previsão na legislação penal pátria. Destaca-se que o Projeto do

[49] BRASIL. Projeto de Lei do Senado nº 236, de 09 de julho de 2012. Reforma do Código Penal Brasileiro. Disponível em: <http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=106404>. Acesso em: 03 jul 2013.
[50] CONSELHO DA EUROPA. Convenção sobre o Cibercrime. Budapeste, 23 de novembro de 2001. Disponível em: <http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf>. Acesso em: 03 jul 2013.
[51] Dados disponíveis em: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=9/2/2006&CL=ENG>. Acesso em: 03 jul 2013.

Novo Código Penal cumpre o estabelecido naquela, conforme se pode observar pelo quadro a seguir.

Tabela 1 – Quadro comparativo entre a Convenção de Budapeste, a atual legislação penal brasileira e o Projeto do Novo Código Penal.

Convenção sobre o Cibercrime (ETS 185) e Protocolo adicional à Convenção sobre o Cibercrime (ETS 189)	**Legislação brasileira**	**Projeto do Novo Código Penal (PLS nº 236/2012)**
Art. 2º, ETS 185 - Acesso ilegítimo	Art. 154-A do CP	Art. 209
Art. 3º, ETS 185 - Interceptação ilegítima	-	Art. 154
Art. 4º, ETS 185 - Interferência em dados	Art. 313-A do CP; Art. 72, I, da Lei 9.504/97	Art. 273; Art. 333
Art. 5º, ETS 185 - Interferência em sistemas	Art. 313-B do CP; Art. 72, II, da Lei 9.504/97	Art. 170; Art. 210; Art. 274; Art. 333
Art. 6º, ETS 185 - Uso abusivo de dispositivos	-	Art. 209, § 1º; Art. 210, § 1º
Art. 7º, ETS 185 - Falsidade informática	Art. 313-A do CP; Art. 72, I, da Lei 9.504/97	Art. 273; Art. 333; Art. 334
Art. 8º, ETS 185 - Burla informática	Arts. 313-A e 313-B do CP; Art. 72, I e II, da Lei 9.504/97	Art. 170; Art. 210; Art. 273; Art. 274; Art. 333
Art. 9º, ETS 185 - Infrações relacionadas com pornografia infantil	Arts. 240 a 241-B da Lei 8.069/90	Arts. 494 a 496
Art. 10º, ETS 185 - Infrações relacionadas com a violação de direito de autor e dos direitos conexos	Art. 184 do CP	Arts. 172 a 174
Art. 3º, ETS 189 - Divulgação de material racista e xenófobo através de sistemas informáticos	Art. 20, § 2º, da Lei 7.716/89	Art. 472, VII
Art. 4º, ETS 189 - Ameaça racista e xenófoba motivada	Art. 147, do CP	Art. 146 c/c Art. 77, III, n
Art. 5º, ETS 189 - Ofensa racista e xenófoba motivada	Art. 140, § 3º, do CP	Art. 138, § 1º
Art. 6º, ETS 189 - Negação, minimização grosseira, aprovação ou justificação do genocídio ou crimes contra a humanidade	Art. 3º da Lei 2.889/56	Art. 459, parágrafo único

3 A INVASÃO DE DISPOSITIVO INFORMÁTICO QUALIFICADA

A conduta típica descrita no artigo 154-A, §3º, primeira parte, do Código Penal, foi primeiramente prevista na legislação norte-americana, em 1984, na Lei de Abuso e Fraude de Computadores (*Computer Fraud and Abuse Act*)[52], encontrando-se atualmente no Título 18, §1030a-2, do Código dos Estados Unidos[53]:

> 18 USC § 1030 - Fraudes e demais atividades relacionadas praticadas por meio de computadores
> (a) Quem—
> [...]
> (2) intencionalmente, acessar um computador sem autorização ou exceder os usos do acesso autorizado e assim obter—
> (A) informação contida em registro financeiro de uma instituição financeira, ou de uma operadora de cartão como definido na seção 1602 (n) do título 15, ou contida em arquivo de agência de informação de consumidores sobre o próprio consumidor, conforme definido na Lei do Acesso ao Crédito (15 U.S.C. 1681 et seq.);
> (B) informação de qualquer departamento ou agência dos Estados Unidos; ou
> (C) informação de qualquer computador protegido;[54] (tradução livre).

Em 2001, 17 anos após a sua primeira aparição, o crime encontrava-se previsto na Convenção de Budapeste, devendo os países signatários buscar os devidos meios para incorporar tal conduta em seu ordenamento jurídico.

> Artigo 2º - Acesso ilegítimo
> Cada parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático. As parte podem exigir que a infracção seja cometida com a violação de medidas de segurança, **com a intenção de obter dados informáticos** ou outra intenção ilegítima, ou que seja relacionada com um sistema informático conectado a outro sistema informático.[55] (grifos não originais)

---

[52] SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático**. Série Ciência do Direito Penal Contemporânea, vol. 4. – São Paulo : Revista dos Tribunais, 2003, p. 101.

[53] ESTADOS UNIDOS DA AMÉRICA. United States Code. Disponível em: <http://www.law.cornell.edu/uscode/text/18/1030?quicktabs_8=1#quicktabs-8>. Acesso em: 03 jul 2013.

[54] Texto original:
"18 USC § 1030 - Fraud and related activity in connection with computers
(a) Whoever—
[...]
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer;"

[55] CONSELHO DA EUROPA. Convenção sobre o Cibercrime. Budapeste, 23 de novembro de 2001. Disponível em: <http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf>. Acesso em: 03 jul 2013

Apenas em 2012, com a sanção da Lei n. 12.737, tal comportamento passou a ser encarado como delito no Brasil. Esta lei entrou em vigor no dia 2 de abril de 2013, acrescentando ao Código Penal Brasileiro o delito de invasão de dispositivo informático, artigo 154-A.

> 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;
> 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.[56] (grifos não originais)

Pelo novo tipo penal, observa-se que a mera invasão ainda não constitui uma conduta punível. *Hackers* que invadem sistemas apenas para testar seus conhecimentos e demonstrar suas capacidades, a fim de obter destaque em seu círculo de convivência, não serão abarcados pelo tipo penal, devido à ausência de dolo específico. O que se destaca é a tipificação da conduta daqueles que, conhecidos como *crackers*, obtêm informações privadas, sigilosas, por meio dessa invasão.

A modalidade qualificada, prevista no artigo 154-A, § 3º, primeira parte, do Código Penal, expressa o exaurimento da conduta designada no *caput*, em virtude de ser necessário para a configuração desta um especial fim de agir, qual seja "obter [...] dados ou informações sem autorização expressa ou tácita do titular do dispositivo".

---

[56] BRASIL. Decreto-Lei nº 2.848, de 07 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 03 jul 2013.

3.1 Bens jurídicos tutelados e sua dignidade constitucional

A punição da conduta ora analisada visa, primordialmente, à tutela da privacidade[57]. Assim, encontra-se inserida no Capítulo VI - Dos crimes contra a liberdade individual e na Seção IV - Dos crimes contra a inviolabilidade dos segredos.

Contudo, não só a privacidade é protegida. Deve-se levar em conta que a tipificação deste comportamento também assegura a proteção da propriedade e da livre concorrência, além do interesse da Administração Pública, caso a violação se dirija às pessoas designadas no parágrafo quinto.

3.1.1. Privacidade

A garantia da privacidade está prevista no artigo 5º, incisos X e XII, da Constituição Federal.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> X - **são invioláveis a intimidade, a vida privada**, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> [...]
> XII - **é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas**, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;[58] (grifos não originais)

[57] PRADO, Luiz Régis. **Curso de direito penal brasileiro**, parte especial: arts. 121 a 249. 11ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2012, v. 2, p. 407.
[58] BRASIL. Constituição (1988). Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 03 jul 2013.

Em razão do exposto no art. 5º, X, da CF, surge a necessidade de distinção entre privacidade e intimidade. Imaginando-se dois círculos concêntricos, a intimidade seria o círculo menor dentro de um maior chamado privacidade.

Na privacidade, estariam inclusos os fatos referentes, por exemplo, à profissão, aos relacionamentos gerais, às relações de consumo. Enquanto a intimidade abarcaria as relações com a família e os amigos mais próximos.[59]

Na lição de Mendes, Coelho e Branco, "no âmago do direito à privacidade está o controle de informações sobre si mesmo"[60]. E é justamente quando esse controle passa para as mãos de outras pessoas que o Direito Penal agirá. Com efeito, o célebre caso da atriz Carolina Dieckmann, responsável por agilizar a promulgação da lei que tipificou este delito informático, é um claro exemplo dessa violação, não obstante os demais casos não midiáticos, em que imagens são utilizadas sem a devida autorização de seus proprietários.

Conforme alerta Silva

> O intenso desenvolvimento de complexa rede de fichários eletrônicos, especialmente sobre dados pessoais, constitui poderosa ameaça à privacidade das pessoas. O amplo sistema de informações computadorizadas gera um processo de esquadrinhamento das pessoas, que ficam com sua individualidade inteiramente devassada. O perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento.[61]

Deve-se atentar que a forma qualificada do delito de invasão de dispositivo informático em nenhum momento exige que a obtenção das informações acarrete danos à vítima. A perda do domínio da privacidade por meio da invasão já é circunstância suficiente para a configuração do delito em sua modalidade simples.

Outro aspecto que surge a partir da privacidade é a garantia de sigilo das comunicações. Tal proteção, todavia, não é absoluta, havendo casos específicos em que é permitida a sua quebra.

A interpretação literal do texto do inciso XII retrocitado revela que apenas o sigilo das comunicações telefônicas poderia ser violado, obedecidas às restrições legais, mas tal significado não condiz com a realidade. É bastante comum nos crimes praticados pela internet, principalmente nos de divulgação de pornografia infantil, as ordens de quebra de sigilo telemático e de interceptação telemática de dados, instrumentos fundamentais para a

---

[59] MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 4. ed. rev. e atual. – São Paulo : Saraiva, 2009, p. 420.
[60] *Ibid.*, p. 422.
[61] SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 32ª ed. rev., atual. e ampl. – São Paulo : Malheiros, 2009, p. 209-210.

devida identificação do computador que difundiu tais arquivos e, por conseguinte, dos infratores. Sua aplicação está prevista no artigo 1º, parágrafo único, da Lei 9.296/96, que regulamenta aquele dispositivo constitucional:

> 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.[62]

3.1.2. Propriedade

A garantia do direito de propriedade está expressamente prevista no art. 5º, inciso XXII, da Constituição. Entende-se a propriedade como um instituto de múltiplas facetas, onde se incluem, por exemplo, a propriedade urbana, a propriedade rural e a propriedade intelectual. Como leciona Silva,

> A Constituição consagra a tese, que se desenvolveu especialmente na doutrina italiana, segundo a qual a propriedade não constitui uma instituição única, mas várias instituições diferenciadas, em correlação com os diversos tipos de bens e de titulares, de onde ser cabível falar não em propriedades, mas em *propriedades*.[63] (grifos originais)

A Constituição traz em sua literalidade, no art. 5º, incisos XXVII a XXIX, a proteção das diversas manifestações da propriedade intelectual, como os direitos autorais, as marcas e as patentes. Todavia, deve-se levar em conta que ela também garante a defesa do menor *quantum* constitutivo deste especial tipo de propriedade: a informação[64].

Ao se tipificar um delito como o ora analisado, em que há violação de segredos comerciais e industriais, de informações sigilosas, bem como de comunicações privadas, além de claramente proteger a privacidade como visto anteriormente, garante ainda a defesa do conteúdo destas, visto este ser, geralmente, o maior objetivo dos autores do delito.

---

[62] BRASIL. Lei n. 9.296, de 24 de julho de 1999. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 03 jul 2013.

[63] SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 32ª ed. rev., atual. e ampl. – São Paulo : Malheiros, 2009, p. 274.

[64] GRAU-KUNTZ, Karin. A quem pertence conhecimento e cultura? Uma reflexão sobre o discurso de legitimação do direito de autor. **Liinc em Revista**, Rio de Janeiro, v. 7, n. 2, set. 2011, p. 408. Disponível em: <http://revista.ibict.br/liinc/index.php/liinc/article/viewFile/437/324>. Acesso em: 03 jul 2013.

3.1.3. Livre concorrência

Um dos fundamentos do Estado Democrático de Direito trata-se da livre iniciativa, como previsto no artigo 1º, IV, da Constituição. Como manifestação da livre iniciativa, surge a livre concorrência, sendo esta um dos princípios da Ordem Econômica.

Em apertada síntese, pode-se indicar que, quanto à forma de participação do Estado nas atividades econômicas desenvolvidas em seu território, foram superadas as seguintes fases: o Estado Absolutista, em que havia forte intervenção estatal na economia; o Estado Liberal, em que havia o predomínio da máxima *laissez-faire, laissez-passer*, apresentando, assim, a plenitude da livre iniciativa, com intervenção mínima do Estado[65]; o Estado Keynesiano, que surgiu como forma de superar a Crise de 1929, influenciado pela Teoria Geral do Emprego, do Juro e do Dinheiro, de John Maynard Keynes, estimulando a demanda agregada e criação de empregos para aumentar o consumo e alavancar a economia mediante a política fiscal e a intervenção estatal[66].

Hoje, vive-se um misto de Estado neoliberal e Estado neo-keynesiano. Entretanto, destaca-se o importante papel de atuação estatal nesta nova fase mediante a regulamentação da economia, evitando eventuais abusos dentro do setor econômico e deste sobre os consumidores[67].

Assim, a Constituição, em seu artigo 173, § 4º, conclama que "A lei reprimirá o abuso do poder econômico que vise à dominação dos mercados, à eliminação da concorrência e ao aumento arbitrário dos lucros". A forma de abuso de poder que se pretende destacar é a concorrência desleal.

O Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio (TRIPS) de 1994, em seu artigo 39, indica a proteção dos segredos como forma de se evitar a concorrência desleal. Assim, dispõe que:

> 1. Ao assegurar proteção efetiva contra competição desleal, como disposto no Artigo 10 “bis” da Convenção de Paris (1967), os Membros protegerão informação confidencial de acordo com o parágrafo 2 abaixo, e informação submetida a Governos ou a Agências Governamentais, de acordo com o parágrafo 3 abaixo.
> 2. Pessoas físicas e jurídicas terão a possibilidade de evitar que informações legalmente sob seu controle seja divulgada, adquirida ou usada por terceiros, sem seu consentimento, de maneira contrária a práticas comerciais honestas, (10) desde que tal informação:

---

[65] FIGUEIREDO, Leonardo Vizeu. **Lições de direito econômico**. 4ª ed. – Rio de Janeiro : Forense, 2011, p. 38.
[66] BOARATI, Vanessa. **Economia para o direito**. Série noções de direito – Barueri : Manole, 2006, p. 32.
[67] FIGUEIREDO, *op. cit.*, p. 42-43.

> (a) seja secreta, no sentido de que não seja conhecida em geral nem facilmente acessível a pessoas de círculos que normalmente lidam com o tipo de informação em questão, seja como um todo, seja na configuração e montagem específicas de seus componentes;
> (b) tenha valor comercial por ser secreta; e
> (c) tenha sido objeto de precauções razoáveis, nas circunstâncias, pela pessoa legalmente em controle da informação, para mantê-la secreta.
> 3. Os Membros que exijam a apresentação de resultados de testes ou outros dados não divulgados, cuja elaboração envolva esforço considerável, como condição para aprovar a comercialização de produtos farmacêuticos ou de produtos agrícolas químicos que utilizem novas entidades químicas, protegerão esses dados contra seu uso comercial desleal. Ademais, os Membros adotarão providências para impedir que esses dados, sejam divulgados, exceto quando necessário para proteger o público, ou quando tenham sido adotadas medidas para assegurar que os dados sejam protegidos contra o uso comercial desleal.[68]

Com a finalidade de controlar a prática da concorrência desleal foi sancionada a Lei n. 12.529/2011, que estrutura o Sistema Brasileiro de Defesa da Concorrência, formado pelo Conselho Administrativo de Defesa Econômica (CADE) e pela Secretaria de Acompanhamento Econômico do Ministério da Fazenda. Esta lei, porém, elenca apenas infrações administrativas, indicando, em seu artigo 36, inciso I, que "Constituem infração da ordem econômica, independentemente de culpa, [...] limitar, falsear ou de qualquer forma prejudicar a livre concorrência ou a livre iniciativa".

Na esfera penal, alguns dos delitos que ofendem a livre concorrência estão previstos no rol de incisos do artigo 195 da Lei de Proteção à Propriedade Industrial, Lei n. 9.279/1996. Destacam-se aqueles mais importantes para o presente trabalho:

> Art. 195. Comete crime de concorrência desleal quem:
> [...]
> XI - divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;
> XII - divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude; ou
> [...][69]

Semelhante às disposições legais anteriormente elencadas, a modalidade qualificada do recente tipo penal também protege os segredos comerciais e industriais. A

---

[68] ORGANIZAÇÃO MUNDIAL DO COMÉRCIO. Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio. Marrakesh, 15 de abril de 1994. Disponível em: <http://www.itamaraty.gov.br/o-ministerio/conheca-o-ministerio/tecnologicos/cgc/solucao-de-controversias/mais-informacoes/texto-dos-acordos-da-omc-portugues/1.3-anexo-1c-acordo-sobre-aspectos-dos-direitos-de-propriedade-intelectual-relacionados-ao-comercio-trips/view>. Acesso em: 03 jul 2013.

[69] BRASIL. Lei n. 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9279.htm>. Acesso em: 03 jul 2013.

proteção trazida pela Lei n. 12.737/2011 é mais forte, embora seja mais específica. Agora, a mera obtenção do segredo já é considerada crime, desde que esta informação secreta esteja armazenada num dispositivo informático e seja acessada por meio de uma invasão, nos moldes descritos no artigo 154-A, *caput*, do Código Penal. Sua posterior divulgação é causa de aumento de pena da modalidade qualificada, conforme artigo 154-A, § 4º, do Código Penal.

3.2 Objeto material do delito

A modalidade qualificada do delito de invasão de dispositivo informático, quanto à obtenção de informações, elenca três objetos materiais: o conteúdo das comunicações eletrônicas privadas, os segredos comerciais e industriais e as informações sigilosas, assim definidas em lei.

3.2.1 Conteúdo de comunicações eletrônicas privadas

Por comunicação eletrônica entende-se toda troca de informações feita por meio eletrônico. Por exemplo, o envio de *e-mails*, a troca de mensagens em redes sociais, bem como por *Short Message Service* (SMS) e por aplicativos de *smartphones*, a exemplo do *WhatsApp*.

A dúvida que paira sobre essa definição atine a questão do uso do termo *privado*. Seria este apenas uma qualidade da troca de informações ou estar-se-ia referindo ao conteúdo destas?

Para Bitencourt,

> Quer nos parecer, que se refere a qualquer conteúdo e de qualquer comunicação eletrônica, independentemente de sua relevância ou natureza, desde que distinto das demais hipóteses elencadas, isto é, desde que não se refira a segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou a controle remoto não autorizado do dispositivo invadido. Pois estes outros conteúdos já estão nominados expressamente. Em outros termos, estamos sustentando que é indiferente a maior ou menor relevância do conteúdo da comunicação eletrônica violada, pois sua relevância está na violação em si, que retira a segurança individual de seus interesses, segredos, sigilos ou negócios; vulnera, enfim, totalmente a intimidade e a

> privacidade do titular desses interesses. Ademais, essa conclusão encontra respaldo na ausência de previsão similar a constante no final dos arts. 153 e 154, os quais exigem que da divulgação resulte em dano a outrem.[70]

Discorda-se da posição apresentada pelo citado autor. É certo que interceptar comunicações alheias é um comportamento repreensível, desde que não fundamentado nas hipóteses legais que permitem tais violações. Não se pode concluir, todavia, que toda interceptação do conteúdo dessas comunicações configurará a modalidade qualificada do delito do artigo 154-A do Código Penal, sob pena de ferir a razoabilidade.

Se com a invasão, o agente obteve apenas informações de domínio público, por exemplo, *links* referentes a notícias disponíveis em sítios eletrônicos de jornais de grande circulação, a modalidade qualificada não poderia estar configurada, e sim apenas a simples, visto a consumação da invasão e a presença do dolo específico.

Destarte, a utilização do termo *privado* para justificar uma conduta mais gravosa contra a vítima, salvo melhor juízo, deve estar se referindo à qualidade da informação trocada, e não apenas ao fato de tais mensagens não serem públicas.

3.2.2 Segredos comerciais ou industriais

São vários os sistemas de proteção da propriedade intelectual, a depender das suas manifestações. Assim, há regras específicas que protegem os direitos autorais, as patentes, as marcas, os desenhos industriais, as indicações geográficas, dentre outros. No Brasil, tem-se a Lei n. 9.279, de 14 de maio de 1996, que regula direitos e obrigações relativos à propriedade intelectual em geral, não abarcando os direitos autorais, e a Lei n. 9.610, de 19 de fevereiro de 1998, específica sobre estes.

Entretanto, não existe legislação específica para a proteção do segredo devido à própria natureza deste. Há apenas aquelas normas relacionadas à concorrência desleal, como observado no item 3.1.3. As outras formas de proteção exigem a publicidade, sendo esta característica totalmente contrária aos objetivos da guarda por meio do segredo. Nesse sentido, o posicionamento da Organização Mundial da Propriedade Intelectual (OMPI):

---

[70] BITENCOURT, Cezar Roberto. Invasão de dispositivo informático. **Atualidades do Direito.** Disponível em: <http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico/>. Acesso em: 03 jul 2013.

> A patente constitui o modo mais eficaz de se proteger uma invenção, mas, como já mencionei, os direitos relativos à patente são conferidos em troca da divulgação da tecnologia ao público pelo inventor. Outro modo eficaz de se obter proteção é manter a tecnologia em sigilo e apoiar-se no que denominamos segredo de fábrica, para manter as informações referentes à invenção confidenciais. A dificuldade desse método é que, desde que o produto é colocado no mercado e pode ser desmontado, os segredos podem ser desvendados por uma simples observação do produto, e a proteção a título de segredo de fábrica é perdida. [...] A proteção do segredo de fábrica ainda é, todavia, disponível, e pode se revelar muito útil, principalmente no que se refere ao know-how, quer dizer, o conhecimento técnico necessário à utilização mais eficaz possível de uma determinada tecnologia. E muitas vezes, a tecnologia propriamente dita não é protegida pela patente, porque é conhecida pelo técnico no assunto, mas o simples fato de manter o know-how em sigilo como segredo de fábrica, constitui uma maneira de proteger sua tecnologia.[71]

Agora, além das sanções cíveis, a obtenção desse segredo também será reprimida pela esfera penal, especificamente quando resultar de invasão de dispositivo informático. Como já se destacou, a legislação penal pátria já protegia a violação desses segredos. Entretanto, exigia para configuração do delito as condutas de, sem autorização, divulgar, explorar e utilizar tais informações, conforme artigo 195, incisos XI e XII, da retrocitada Lei n. 9.279/1996.

O tipo ainda garante a proteção dos segredos comerciais. Estes podem ser entendidos como os segredos do próprio negócio, algo que permeia a intimidade da empresa.

Durante a vigência da primeira parte do Código Comercial, este conceito abrangia apenas os livros empresariais, conforme os artigos 17 e 19.

> Art. 17 - Nenhuma autoridade, juízo ou tribunal, debaixo de pretexto algum, por mais especioso que seja, pode praticar ou ordenar alguma diligência para examinar se o comerciante arruma ou não devidamente seus livros de escrituração mercantil, ou neles tem cometido algum vício.
> Art. 19 - Todavia, o juiz ou Tribunal do Comércio, que conhecer de uma causa, poderá, a requerimento da parte, ou mesmo do ex officio, ordenar, na pendência da lide, que os livros, ou de qualquer ou de ambos os litigantes sejam examinados na presença do comerciante a quem pertencerem e debaixo de suas vistas, ou na de pessoa por ele nomeada, para deles se averiguar e extrair o tocante à questão.[72]

Hoje, estão inclusos, por exemplo, as listas de clientes, os custos operacionais e as decisões estratégicas, ou seja, informações que, caso se tornassem públicas, trariam forte vantagem para as empresas concorrentes[73].

---

[71] ORGANIZAÇÃO MUNDIAL DA PROPRIEDADE INTELECTUAL. Módulo 7: Patentes. **Curso Geral de Propriedade Intelectual**, 2011, p. 24.

[72] BRASIL. Lei n. 556, de 25 de junho de 1850. Código Comercial. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l0556-1850.htm>. Acesso em: 03 jul 2013.

[73] SANTOS, Márcio Fernando Candéo. O direito ao segredo: a violação da intimidade no âmbito dos direitos da personalidade. In: XVIII CONGRESSO NACIONAL DO CONPEDI, São Paulo, 2009. **Anais do XVIII Congresso Nacional do CONPEDI**, São Paulo, 2009, p. 5547. Disponível em:

3.2.3 Informações sigilosas, assim definidas em lei

Quanto às informações sigilosas, o tipo elenca uma norma penal em branco. O conceito deverá estar previsto em lei, não admitindo outros tipos de definições senão aquela descrita no dispositivo legal, evitando, assim, múltiplas interpretações e surpresas na aplicação da lei.

Haverá de ser lei em sentido estrito, inadmitindo-se, portanto, a "sua equiparação a resoluções, portarias, regulamentos etc. Em outros termos, estas não suprem a necessidade da definição legal"[74].

Prado alega que a "[...] complementação encontra-se no próprio Código Penal, que define quais são os segredos e informações invioláveis (seções II e IV do CP)"[75]. Todavia, a informação é equivocada. Em nenhum momento, o Código Penal apresenta tal conceituação.

Na realidade, o conceito de informação sigilosa pode ser encontrado no artigo 4º, inciso III, da Lei n. 12.527/2011, que regula procedimentos de acesso à informação a serem observados pela Administração Pública.

> Art. 4º Para os efeitos desta Lei, considera-se:
> I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
> II - documento: unidade de registro de informações, qualquer que seja o suporte ou formato;
> **III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;**
> IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;
> V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;
> VI - disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;
> VII - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;
> VIII - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;

<http://www.publicadireito.com.br/conpedi/manaus/arquivos/Anais/sao_paulo/2250.pdf>. Acesso em: 03 jul 2013.

[74] BITENCOURT, Cezar Roberto. Invasão de dispositivo informático. Disponível em: <http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico/>. Acesso em: 03 jul 2013.

[75] PRADO, Luiz Régis. **Curso de direito penal brasileiro**, parte especial: arts. 121 a 249. 11ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2012, v. 2, p. 412.

> IX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.[76] (grifos não originais)

O posicionamento aqui defendido é de que, ao prever os três objetos materiais destacados – conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais e informações sigilosas –, o Legislador direcionou cada um deles para um setor específico. Do contrário, poderia apenas ter utilizado o mesmo texto do *caput* em vez de destrinchá-lo. Assim, ao proteger as comunicações privadas, garantiria a privacidade no âmbito da pessoa física; ao proteger os segredos comerciais e industriais, defenderia a privacidade no âmbito das pessoas jurídicas de direito privado; e, ao proteger as informações sigilosas, estaria garantindo a privacidade de determinadas informações da Administração Pública direta e indireta. Desse modo, parece correto afirmar que o conceito de *informação sigilosa* é aquele trazido no supracitado inciso, visto ser direcionado à Administração.

3.3 Demais conceitos abordados pelo tipo

3.3.1 Invasão e violação de mecanismo de segurança

O termo invasão deve ser tido como sinônimo de acesso não autorizado ou, na terminologia inglesa, *hacking*[77].

Acesso, segundo Vianna, é entendido como

> a ação humana de ler, escrever ou processar dados armazenados em sistemas computacionais. Ler dados armazenados em um sistema computacional consiste em reinterpretá-los como informações humanamente inteligíveis[78].

Complementa o referido autor que

> Autorização é a legitimidade jurídica que alguém possui para acessar determinados dados em um sistema computacional. Sua validade decorre da propriedade dos

[76] BRASIL. Lei n. 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei n. 8.112, de 11 de dezembro de 1990; revoga a Lei n. 11.111, de 5 de maio de 2005, e dispositivos da Lei n. 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 03 jul 2013.
[77] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. – São Paulo : Saraiva, 2011, p. 64.
[78] VIANNA, Túlio Lima. **Fundamentos de direito penal informático**: do acesso não autorizado a sistemas computacionais. – Rio de Janeiro : Forense, 2003, p. 51.

> dados e o proprietário dos dados, evidentemente, terá sempre plenos poderes para acessá-los. Poderá ele também permitir que outras pessoas tenham acesso a esses dados, autorizando-os, geralmente através de uma senha.[79]

Assim, fica claro que para haver a configuração de um acesso não autorizado não necessariamente deverá ocorrer uma burla a um sistema de defesa. Entretanto, para a modalidade simples do delito de invasão de dispositivo informático, é necessária tal violação:

> 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: (grifos não originais)

Em razão disso, interpretações divergentes sobre o mesmo fato surgirão, senão vejamos. Se o agente tiver acesso à senha do proprietário do sistema sem que este tenha conhecimento e venha a se utilizar dela para obter informações privadas, sua conduta não se subsumirá àquela prevista na norma. A confusão é que, apesar de haver um acesso não autorizado, visto não existir qualquer permissão concedida pelo proprietário, não haverá a "violação indevida de mecanismo de segurança", pois o agente realizou um *logon* como se proprietário fosse, não havendo qualquer burla ao sistema em razão da utilização de dados verdadeiros. Em uma visão contrária, haveria uma violação de segurança, pois, ao se descobrir a senha do proprietário e utilizá-la para obter acesso ao dispositivo, estar-se-ia burlando o mecanismo de segurança.

Outro posicionamento conclui que o Legislador utilizou-se de uma redundância. Leciona Prado que:

> O próprio núcleo verbal *invadir* já encerra ideia de violação indevida. Aqui, todavia, destaca-se o elemento *mecanismo de segurança*, que pode ser *físico* como as portas, travas para teclados com chaves, ou *lógico*, tais como, o uso de nome de usuário e senhas, criptografas os dados etc. Essa menção – mecanismo de segurança – é, em princípio, desnecessária. Senão, veja-se. Nem todos os dispositivos informáticos têm mecanismo de segurança. A invasão pode ocorrer com ou sem mecanismo de segurança, visto que este último também tem vulnerabilidades. Assim, conforme o texto legal, pode ocorrer que se invada um dispositivo e se alegue que não dispunha ele de mecanismo de segurança. Haveria uma lacuna de punibilidade. Trata-se de crime de forma vinculada.[80] (grifos originais)

---

[79] VIANNA, Túlio Lima. **Fundamentos de direito penal informático**: do acesso não autorizado a sistemas computacionais. – Rio de Janeiro : Forense, 2003, p. 53-54.

[80] PRADO, Luiz Régis. **Curso de direito penal brasileiro**, parte especial: arts. 121 a 249. 11ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2012, v. 2, p. 408-409.

O método mais comum para se efetuar uma invasão é por meio de programas de código malicioso (*malwares*). *Malware* é um termo cunhado a partir da combinação das palavras *malicious* e *software* e pode ser definido como

> programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. [...] Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.[81]

São exemplos de *malwares* relacionados com a captura de informações: *backdoors*, *bots*, *botnets*, *spywares* e cavalos de troia (*trojan horses*).

Tabela 2 – Espécies e definições de *malwares*.

Espécie de *malware*	Definição
Backdoor	Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.
Bot	Programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente e, consequentemente, o sistema por ele infectado.
Botnet	Rede formada por centenas ou milhares de computadores controlados e que permite potencializar as ações danosas executadas pelos *bots*.
Spyware	Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.
Cavalo de Troia	Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Fonte: CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para a Internet**. Versão 4.0, de 04 de junho de 2012. Disponível em**:** <http://cartilha.cert.br/malware/>. Acesso em: 18 abr 2013.

Um método que pode facilitar a invasão chama-se ataque de negação de serviços ou *denial of service attack* (DoS *Attack* ou,simplesmente, DoS). Pode ser definido como ataques que objetivam impedir a utilização de determinados serviços por seus usuários

[81] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para a Internet**. Versão 4.0, de 04 de junho de 2012. Disponível em: <http://cartilha.cert.br/malware/>. Acesso em: 03 jul 2013.

legítimos[82]. Tal técnica é utilizada atualmente pelo grupo *Anonymous* para sobrecarregar *sites* e deixá-los fora do ar. Apesar de o DoS não ser voltado para invasões, pode ser utilizado como meio de enfraquecer os sistemas, facilitando a realização daquelas.

O aperfeiçoamento dessa técnica chama-se ataque distribuído de negação de serviço ou *distributed denial of service attack* (DDoS). Neste método, um computador-mestre comanda outros computadores, aqui denominados de "zumbis", sobrecarregando ainda mais os sistemas, deixando-os vulneráveis a outros ataques[83].

3.3.2 Dispositivo informático

O conceito de dispositivo informático é similar ao de sistema computacional. A Convenção de Budapeste sobre o Cibercrime, em seu artigo 1º, *a*, define sistema informático como "qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de um entre eles, desenvolve, em execução de um programa, o tratamento automatizado de dados"[84].

Vianna complementa, afirmando que

> é fácil perceber que tanto um simples computador doméstico como um sofisticado computador de grade porte são sistema computacionais formados por uma série de dispositivos físicos interconectados (processador, memória, disco rígido, etc.) comandados por uma série de dispositivos lógicos (BIOS, sistema operacional, programas utilitários).[85]

Outros exemplos de sistemas computacionais ou, como prefere o Legislador, dispositivos informáticos passíveis de ser alvo desse delito são: os *smartphones* e *tablets*, que permitem o acesso à internet em qualquer lugar em que haja cobertura da operadora para oferecer tal serviço; os caixas eletrônicos, que agilizam os serviços prestados pelos bancos; os dispositivos de memória externa, como *hard disks* externos e *flash drives*, estes representados

---

[82] SOFTWARE ENGINEERING INSITUTE. **Denial of Service Attacks**. Carnegie Mellon University. Disponível em: <http://www.cert.org/tech_tips/denial_of_service.html>. Acesso em: 03 jul 2013.
[83] KESAN, Jay P.; HAYES, Carol M. Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace. In: **Harvard Journal of Law & Technology**, Cambridge, Massachusetts, vol. 25, nº 2, Spring 2012, p. 430-431. Disponível em: <http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech415.pdf>. Acesso em: 03 jul 2013.
[84] CONSELHO DA EUROPA. Convenção sobre o Cibercrime. Budapeste, 23 de novembro de 2001. Disponível em: <http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf>. Acesso em: 03 jul 2013.
[85] VIANNA, Túlio Lima. **Fundamentos de direito penal informático**: do acesso não autorizado a sistemas computacionais. – Rio de Janeiro : Forense, 2003, p. 48.

pelos *pen drives* e cartões de memória; e os sistemas de gerenciamento de voo dos aviões[86]. Verifica-se, assim, a pluralidade de espécies de dispositivos informáticos existentes e a certeza de que este número tende a multiplicar-se.

[86] Hijacking airplanes with an Android phone. **Help Net Security**. Disponível em: <http://www.net-security.org/secworld.php?id=14733>. Acesso em: 03 jul 2013.

4 O *ETHICAL HACKING* PRATICADO PELOS TIMES DE RESPOSTA A INCIDENTES DE SEGURANÇA COMPUTACIONAL COMO CONDUTA DE LEGÍTIMA DEFESA

Com a sanção da Lei n. 12.737/2012, o ordenamento jurídico brasileiro foi presenteado com a tipificação do primeiro delito eminentemente eletrônico: a invasão de dispositivo informático (artigo 154-A do Código Penal).

Apesar dos defeitos destacados no capítulo anterior, essa tipificação representa o primeiro grande passo no sentido de combater os crimes eletrônicos no Brasil, que, paulatinamente, só aumentam o seu número de incidências.

Em alguns casos, o Poder Judiciário não conseguirá agir de forma efetiva e eficaz para recuperar os danos sofridos, especialmente no caso da modalidade qualificada daquele delito. Sabe-se que uma vez obtida a informação, se esta não for imediatamente recuperada, o agente criminoso poderá difundi-la rapidamente por toda a internet, impossibilitando, assim, qualquer justa reparação pelos prejuízos sofridos. Exemplos clássicos são os pedidos feitos a empresa Google para restringir os resultados de determinadas buscas, apesar de isso ser totalmente ineficaz para retirar as informações da rede.

Assim, como meio de enfrentar tais delitos, evitando prejuízos irreparáveis, levanta-se a possibilidade de configuração da legítima defesa em meio virtual.

4.1 Definição de *ethical hacking*

O *ethical hacking* pode ser entendido sob dois aspectos. Como ensina Crespo, "trata-se da utilização de conhecimentos técnicos específicos de agentes treinados para recuperar informações subtraídas ou copiadas de forma ilegítima, ou, ainda, defender-se de ataques"[87].

Assim, de um lado, o *ethical hacking* é definido como uma forma de prevenção, consistindo em uma série de testes de segurança nos quais os profissionais encarnam o personagem de agentes criminosos, a fim de identificar as possíveis falhas nos sistemas e,

[87] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. – São Paulo : Saraiva, 2011, p. 114.

assim, fortalecê-los.[88]

Por outro lado, o *ethical hacking* é conhecido pela ação de recuperação dos dados subtraídos, agindo o profissional de segurança com a mesma técnica do agente criminoso. É esta faceta que interessará ao presente trabalho, também denominada de *hacking back*.

O *hacking back* é um meio de resposta ativa contra a prática de invasões. São duas as suas principais modalidades[89]. A primeira trata-se de uma invasão com a finalidade de localizar o sistema computacional que originou os ataques e, consequentemente, os agentes envolvidos. A segunda envolve atacar a máquina de origem dos ataques, com a finalidade de suspender a ação invasiva, bem como, eventualmente, recuperar as informações obtidas de modo indevido.

Dois acontecimentos tornaram-se famosos nos Estados Unidos pela utilização desta técnica para combater delitos eletrônicos: o primeiro, um ataque eletrônico contra o Pentágono; e o segundo, contra o *site* da Organização Mundial do Comércio (OMC).

Em setembro de 1998, foi documentada, pela primeira vez, a utilização da técnica do *hacking back*. O Pentágono reagiu a um ataque de DoS, iniciado pela *Eletronic Disruption Theater*, uma organização hacktivista, utilizando-se de uma técnica ofensiva para interromper o funcionamento daqueles dispositivos de onde partiam as invasões[90].

A segunda reação documentada ocorreu em janeiro de 2000, durante uma reunião da OMC. O grupo *The Electrohippies Collective*, também conhecidos por *e-Hippies*, invadiram o *site* da OMC, utilizando ataques de DoS[91].

Na ocorrência de uma invasão, devem ser seguidos três passos na utilização do *hacking back*: identificar o causador da invasão por meio de sistemas de detecção (IDS[92]); em seguida, chegar ao dispositivo informático responsável pelos ataques (*traceback*); e, ao fim,

---

[88] KNIGHT, William. License to hack? - Ethical hacking. **Infosecurity**. Disponível em: <http://www.infosecurity-magazine.com/view/4611/license-to-hack-ethical-hacking/>. Acesso em: 12 mai 2013.

[89] DENNING, Dorothy E. The Ethics of Cyber Conflict. In: HIMMA, Kenneth Einar; TAVANI, Herman T. **The Handbook of Information and Computer Ethics**. Hoboken, New Jersey : Wiley, 2008. p. 422. Disponível em: <http://www.e-reading.su/bookreader.php/141465/The_Handbook_of_Information_and_Computer_Ethics.pdf#page=441>. Acesso em: 03 jul 2013.

[90] JAYASWAL, Vikas; YURCIK, William; DOSS, David. Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism? In: **IEEE 2002 International Symposium on Technology and Society (ISTAS'02)**: Social Implications of Information and Communication Technology. Proceedings. 2002. ISBN: 0-7803-7284-0, p. 381. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1013841>. Acesso em: 03 jul 2013.

[91] DENNING, *op. cit.*, p. 423.

[92] Acrônimo para *Intrusion Detection Systems*.

contra-atacar, seja para interromper o funcionamento daquele sistema, cessando a invasão, ou para recuperar informações obtidas ilegalmente.[93]

Os sistemas de identificação de intrusos (IDS) foram bastante desenvolvidos durante a primeira década do século XXI[94]. Os IDSs identificam padrões de invasão com a finalidade única de identificar com precisão sua origem. A grande dificuldade surge nos ataques de DDoS, visto ser originado de vários dispositivos distintos[95]. O *firewall* é o exemplo mais comum de IDS. Aqueles são programas utilizados para proteger um computador contra acessos não autorizados vindos da Internet[96] e conseguem gravar os endereços de IP dos dispositivos que se conectaram ou tentaram se conectar ao sistema invadido[97], facilitando, assim, o rastreamento dos pretensos invasores.

Superado o primeiro momento, a segunda fase, o *traceback,* é iniciada e poderá ser concluída em poucos segundos[98]. O grande risco do *traceback* é o fato de, em grande parte dos casos, o sistema de ataque principal ser responsável indiretamente pela invasão[99]. Atenta-se que a invasão de um dispositivo informático também poderá resultar no controle remoto deste. Esta conduta também se encontra tipificada na modalidade qualificada do delito de invasão de dispositivo informático (CP, art. 154-A, § 3º, segunda parte). Com o controle do sistema de terceiros, o agente criminoso poderá realizar outras invasões a partir dele. Destarte, surge a estrita necessidade de a técnica do *hacking back* ser utilizada apenas por especialistas da área de segurança da informação, pois um possível ataque ao computador que está apenas sendo manipulado, apesar de não configurar o delito do artigo 154-A, por ausência de dolo, não impossibilita a reparação civil pelos eventuais danos causados.

Por derradeiro, ao se identificar corretamente o sistema computacional que originou os ataques, tomam-se medidas de contra-ataque, que consistem na utilização dos mesmos métodos do invasor com o objetivo, todavia, de interromper aquela conduta e, sendo

---

[93] KESAN, Jay P.; HAYES, Carol M. Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace. In: **Harvard Journal of Law & Technology**, Cambridge, Massachusetts, vol. 25, nº 2, Spring 2012, p. 461. Disponível em: <http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech415.pdf>. Acesso em: 12 mai 2013. No mesmo sentido, PINHEIRO, Patrícia Peck. **Direito Digital**. 3ª ed. rev., atual. e ampl. – São Paulo : Saraiva, 2009, p. 241.

[94] *Ibid.*, p. 467.

[95] *Ibid.*, p. 468.

[96] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para a Internet**. Versão 4.0, de 04 de junho de 2012. Disponível em: <http://cartilha.cert.br/mecanismos/>. Acesso em: 03 jul 2013.

[97] JAYASWAL, Vikas; YURCIK, William; DOSS, David. Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism? In: **IEEE 2002 International Symposium on Technology and Society (ISTAS'02)**: Social Implications of Information and Communication Technology. Proceedings. 2002. ISBN: 0-7803-7284-0, p. 381. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1013841>. Acesso em: 03 jul 2013.

[98] KESAN; HAYES, *op. cit.*, p. 466-467.

[99] JAYASWAL; YURCIK; DOSS, *op. cit.*, p. 383.

o caso, recuperar informações perdidas. O tempo para a tomada dessas decisões deve ser o mais curto possível, facilitando a identificação do invasor e diminuindo as perdas econômicas[100].

4.2 Os Times de Resposta a Incidentes de Segurança Computacional

Com o número crescente de incidentes computacionais, conforme informações do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[101], surgiu a necessidade de aprimorar a segurança das empresas, agora, com o fim de proteger as suas informações e o bom desenvolvimento de suas atividades.

Surgiram, assim, os Times de Resposta a Incidentes de Segurança Computacional (CSIRT[102]), com o objetivo primordial de monitorar, "para que se possa pegar o infrator literalmente com a 'mão na máquina', quer ele seja de dentro, algum funcionário ou colaborador, quer seja de fora"[103]. Por ser um serviço de monitoramento constante, é necessário um funcionamento incessante, sendo os CSIRTs verdadeiros guardiões das redes.

O CSIRT também poderá ser um grupo *ad hoc*, formado exclusivamente para responder e avaliar incidentes específicos[104], desvirtuando-se, nesses casos, de sua natureza de monitoramento. Poderá prestar serviços para empresas, órgãos governamentais, organizações acadêmicas[105].

O primeiro CSIRT surgiu em 1988, após um fato conhecido por *The Morris Worm Incident*.[106]

---

[100] JAYASWAL, Vikas; YURCIK, William; DOSS, David. Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism? In: **IEEE 2002 International Symposium on Technology and Society (ISTAS'02)**: Social Implications of Information and Communication Technology. Proceedings. 2002. ISBN: 0-7803-7284-0, p. 380. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1013841>. Acesso em: 03 jul 2013.

[101] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA DO BRASIL. Estatísticas dos Incidentes Reportados ao CERT.br. Brasil, 2013. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 03 jul 2013.

[102] Acrônimo de *Computer Security Incident Response Teams*.

[103] PINHEIRO, Patrícia Peck. **Direito Digital**. 3ª ed. rev., atual. e ampl. – São Paulo : Saraiva, 2009, p. 241.

[104] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. – São Paulo : Saraiva, 2011, p. 113.

[105] Uma lista de CSIRTs brasileiros está disponível em: <http://www.cert.br/csirts/brazil/>. Acesso em: 03 jul 2013.

[106] PEIXOTO, Mário César Pintaudi. **Criando um CSIRT**: Computer Security Incident Response Team e entendendo seus desafios. – Rio de Janeiro : Brasport, 2008, p. 2.

> No dia 2 de Novembro de 1988 a Internet foi alvo de um software malicioso do tipo habitualmente designado por "worm". Este programa informático, criado por Robert Morris com o propósito de se auto-propagar através da rede, foi responsável pela contaminação de mais de 60,000 computadores, afectando negativamente e durante vários dias diversos serviços e a funcionalidade global da Internet. A rapidez de propagação e o consequente impacto do agora designado Morris Worm apanhou a então pequena comunidade Internet desprevenida. Da análise do incidente verificou-se que o que mais prejudicou o normal funcionamento da rede e serviços associados não foi o tempo necessário para encontrar um antídoto eficaz, mas sim a inexistência de uma estrutura organizada que permitisse informar a comunidade da existência do incidente, efectuar uma eficaz distribuição do antídoto e instruir os utilizadores sobre a sua aplicação. Como consequência imediata foi então criado um centro de coordenação de resposta a incidentes de segurança designado de CERT/CC.[107]

Esses times, também conhecidos por outras designações[108], atuam em três grandes classes de serviços: proativos, reativos e gerenciamento de qualidade[109]. Para este estudo, o mais importante são os reativos, em que estão inclusos: tratamento de incidentes; detecção e rastreamento de invasões; auditoria e preservação de evidências; análise de riscos; avaliação de produtos; e análise de vulnerabilidades.

A atuação do CSIRT no combate a incidentes pode ser resumida em seis grandes etapas: preparação, identificação, contenção, erradicação, recuperação e aprendizado[110].

A etapa de preparação é um momento de prevenção. Deverá, por exemplo, haver uma conscientização dos usuários sobre o manejo dos conteúdos de *e-mails* corporativos e privados e, principalmente, das informações restritas as quais têm acesso. Nesta fase, ocorrerão auditorias e buscas por vulnerabilidades[111], fortalecendo, assim, a segurança da rede.

As etapas de identificação, de contenção e de erradicação coincidem com as fases do *hacking back*. A fase de identificação coincide com o momento de utilizar os instrumentos necessários, os IDSs, para identificar devidamente o dispositivo do qual partiu a invasão, bem localizá-lo corretamente. As demais fases, contenção e erradicação, coincidem com o momento de contra-atacar e cessar as atividades do dispositivo invasor.

Por último, vêm as etapas de recuperação e de aprendizado. Esclarece-se, desde logo, que essa etapa de recuperação nada tem que ver com aquela recuperação de informações subtraídas. É um momento de evolução, em que o CSIRT irá recuperar-se dos danos

---

[107] SERVIÇO DE RESPOSTA A INCIDENTES DE SEGURANÇA INFORMÁTICA. Enquadramento. Disponível em: http://www.cert.pt/index.php/institucional/enquadramento-e-motivacao. Acesso em: 03 jul 2013.
[108] "*Computer Incidente Response Capability* (CIRC), *Computer Incident Response Team* (CIRT), *Incident Response Center* (IRC), *Incident Response Capability* (IRC), *Incident Response Team* (IRT), *Security Emergency Response Team* (SERT) *ou Security Incident Response Team* (SIRT)" (CRESPO. Op. cit., p. 113).
[109] PEIXOTO, Mário César Pintaudi. **Criando um CSIRT**: Computer Security Incident Response Team e entendendo seus desafios. – Rio de Janeiro : Brasport, 2008, p. 13.
[110] *Ibid.*, p. 36.
[111] *Ibid.*, p. 37.

eventualmente sofridos, ampliará e aperfeiçoará suas defesas, verificará se o sistema está operando corretamente e, finalmente, aprenderá com seus erros, tentando evitar novas falhas em situações futuras[112].

O CSIRT deverá manter laços com entidades de segurança governamentais e privadas, tanto nacionais quanto estrangeiras, a fim de que troquem conhecimento e apoio contra incidentes computacionais.[113]

4.3 Legítima defesa digital e *ethical hacking*

A legítima defesa está prevista no Direito Penal Brasileiro, no art. 23, II, do CP, como uma causa de excludente de ilicitude.

Quanto ao conceito de legítima defesa, o próprio CP, no art. 25, estabelece que age "em legítima defesa quem, usando moderadamente dos meios necessários, repele injusta agressão, atual ou iminente, a direito seu ou de outrem". Tal conceito de há muito foi pacificado.

Pode-se afirmar que a expressão "legítima defesa" trata-se de uma redundância, um pleonasmo. Na realidade, o termo "legítima" foi acrescentado pelo Direito Romano, pois as palavras "defesa" e "agressão" eram designadas pelo mesmo termo: o verbo *fendo*[114].

O conceito de legítima defesa sofreu abalos apenas durante a Idade Média, período no qual predominou os impérios da Igreja Católica. Segundo Fioretti, "o exercício da legítima defesa parecia um ato lesivo da caridade para com o próximo"[115].

A legítima defesa é considerada a mais antiga causa de exclusão de antijuridicidade. Surgiu após a vingança particular cair em desuso. Quando essa preocupação desapareceu e a defesa social passou a ser exercida pelo próprio Estado, surgiu a ideia de que alguém que sofre uma injusta agressão era colocado na estrita necessidade de defender-se,

---

[112] PEIXOTO, Mário César Pintaudi. **Criando um CSIRT**: Computer Security Incident Response Team e entendendo seus desafios. – Rio de Janeiro : Brasport, 2008, p. 43-44.
[113] *Ibid.*, p. 17.
[114] FIORETTI, Julio. **Legítima Defesa**: Estudo de Criminologia. Traduzido por Fernando Bragança. – Belo Horizonte : Líder, 2002, p. 21.
[115] *Ibid.*, p. 39.

todavia, neste caso, não deveria ser punido[116], desde que obedecesse aos limites impostos pela lei.

> O indivíduo que pratica qualquer ato em estado de legítima defesa representa um instrumento de defesa de que a sociedade se serve num momento de perigo iminente. Quando, ao contrário, o delito está consumado e o mal deixa de ser iminente, ela serve-se dos juízes.[117]

Em outros termos, "faz-se valer a máxima de que o Direito não tem que ceder ante o ilícito"[118].

4.3.1 Fundamento como excludente de ilicitude

Quanto ao fundamento da legítima defesa como excludente de ilicitude, pode-se destacar dois grandes posicionamentos.

O primeiro, adotado por Bitencourt e Prado, apresenta um duplo fundamento: individual e social.

O fundamento individual encontra-se na necessidade de proteger bens jurídicos ameaçados e/ou atingidos por uma injusta agressão. O fundamento social reside no fato de que, ao se repelir uma agressão ilegítima, estar-se-ia defendendo o próprio ordenamento jurídico.[119]

A segunda posição, defendida por Zaffaroni e Pierangeli, une os dois fundamentos anteriormente citados em um só. Indica que a legítima defesa mostra-se necessária à conservação da ordem jurídica e da garantia do pleno exercício dos direitos.

> O problema mais complexo da legítima defesa não é a sua natureza, mas seu fundamento. É definido pela necessidade de conservar a ordem jurídica e de garantir o exercício dos direitos. Conforme seja acentuado um ou outro dos aspectos deste duplo fundamento, se insistirá em seu conteúdo social ou individual. **Na realidade, o fundamento da legítima defesa é único, porque se baseia no princípio de que ninguém pode ser obrigado a suportar o injusto**. [...] O fundamento individual (defesa dos direitos ou dos bens jurídicos) e o fundamento social (defesa da ordem jurídica) não podem ser encontrados simultaneamente, porque a ordem jurídica tem

---

[116] FIORETTI, Julio. **Legítima Defesa**: Estudo de Criminologia. Traduzido por Fernando Bragança. – Belo Horizonte : Líder, 2002, p. 18.
[117] *Ibid.*, p. 16.
[118] PRADO, Luiz Régis. **Curso de direito penal brasileiro**, parte geral: arts. 1º a 120. 8ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2009, v. 1, p. 350.
[119] *Ibid.*, p. 351. No mesmo sentido, BITENCOURT, Cezar Roberto. **Tratado de Direito Penal** – Parte Geral, vol. 1. 14ª ed. rev., atual. e ampl. – São Paulo : Saraiva, 2009, p. 340.

> por objetivo a proteção dos bens jurídicos, e se, numa situação conflitiva extrema, não consegue lográ-lo, não pode recusar ao indivíduo o direito de prover a proteção dos bens por seus próprios meios.[120] (grifos não originais).

4.3.2 Requisitos necessários à configuração da legitima defesa

Como destacado anteriormente, a legítima defesa é conceituada no Código Penal Brasileiro como o uso moderado dos meios necessários, a fim de repelir uma agressão injusta, atual ou iminente, contra direito seu ou de terceiro.

Dessa definição, destacam-se três requisitos: que os meios utilizados na defesa sejam aqueles estritamente necessários e, concomitantemente, sejam utilizados de forma moderada; que a agressão deverá ser injusta; e que tal agressão seja atual ou iminente.

Por fim, o quarto e último requisito, de ordem subjetiva, trata-se do *animus defendendi*.

4.3.2.1 Injusta agressão a um bem jurídico

O termo *agressão* deve ser entendido como toda ação que tenha a finalidade de por em perigo ou gerar dano a um bem jurídico, podendo ser uma atitude violenta ou não[121]. Por exemplo, a conduta de invadir um dispositivo informático, viola um bem jurídico e não há violência.

> É irrelevante que a agressão não constitua um ilícito penal; deverá, contudo, constituir, necessariamente, um fato ilícito, caso contrário não seria *injusta*, pois, como destacava o Ministro Assis Toledo, a *ilicitude* na área penal não se limita à *ilicitude típica*, ou seja, à ilicitude do delito, sempre e necessariamente típica. Exemplo de *ilicitude atípica* pode ser encontrado na exigência de *ilicitude da agressão* - "agressão injusta" - na legítima defesa, que nada mais é do que *agressão ilícita*. A agressão autorizadora da reação defensiva, na legítima defesa, não necessita revestir-se da qualidade de *crime*, isto é, "não precisa ser um *ilícito penal*,

[120] ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro**: parte geral. 6ª ed. rev. e atual. – São Paulo: Revista dos Tribunais, 2006, p. 496.
[121] PRADO, Luiz Régis. **Curso de direito penal brasileiro**, parte geral: arts. 1º a 120. 8ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2009, v. 1, p. 351. No mesmo sentido, BITENCOURT, Cezar Roberto. **Tratado de Direito Penal** – Parte Geral, vol. 1. 14ª ed. rev., atual. e ampl. – São Paulo : Saraiva, 2009, p. 341.

> mas deverá ser , no mínimo, um *ato ilícito*, em sentido amplo, por não existir legítima defesa contra atos lícitos"[122] (grifos originais).

Deve-se ainda ter mente que agressão e defesa tratam-se de *condutas*[123]. Desse modo, aquele que se defende de um ataque de um cão, age em estado de necessidade, e não em legítima defesa. Observe-se, ainda, que a injustiça da agressão deverá estar relacionada a aspectos objetivos, nunca podendo estar relacionada com o seu autor. Surge, assim, a possibilidade de legítima defesa contra atitudes ilícitas praticadas por inimputáveis[124].

A definição de injusta agressão defendida pelos autores aqui destacados é bastante ampla, coincidindo o conceito de *injusto* com o de *ilícito*. Assim, se houver afronta a um bem tutelado pelo ordenamento jurídico, mesmo não havendo tipo específico para a proteção desse bem, a legítima defesa poderá ser invocada, desde que a conduta obedeça aos requisitos necessários para a configuração daquela.

Em razão de a legítima defesa tratar-se de repulsa à injusta agressão e dever ser uma conduta, não se pode admitir legítima defesa contra agressões culposas[125], devendo o ato agressivo ser consciente e voluntário, objetivando gerar danos aos bens jurídicos[126]. Outra consequência é a impossibilidade de ocorrer uma legítima defesa contra legítima defesa[127].

Outrossim, a legítima defesa não poderá atingir terceiros. Se assim ocorrer, aquele que supostamente agiu sob o manto dessa excludente terá agido de forma culposa ou em estado de necessidade[128].

Quanto ao bem jurídico protegido, leciona Zaffaroni e Pierangeli que

> A defesa "a direito de seu ou de outrem" abarca a possibilidade de defender legitimamente qualquer bem jurídico. O requisito da moderação da defesa não exclui a possibilidade de defesa de qualquer bem jurídico, apenas exigindo uma certa proporcionalidade entre a ação defensiva e a agressiva, quando tal seja possível, isto é, que o defensor deve utilizar o meio menos lesivo que tiver ao seu alcance.[129]

---

[122] BITENCOURT, Cezar Roberto. **Tratado de Direito Penal** – Parte Geral, vol. 1. 14ª ed. rev., atual. e ampl. – São Paulo : Saraiva, 2009, p. 341-342. Nesse sentido, GRECO, Rogério. **Curso de Direito Penal** (parte geral). 11 ed. Rio de Janeiro : Impetus, 2009, p. 341. Ainda no mesmo sentido, ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro**: parte geral. 6ª ed. rev. e atual. – São Paulo: Revista dos Tribunais, 2006, p. 498.

[123] ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro**: parte geral. 6ª ed. rev. e atual. – São Paulo: Revista dos Tribunais, 2006, p. 498.

[124] BITENCOURT, *op. cit.*, p. 342.

[125] ZAFFARONI; PIERANGELI, *op. cit.*, p. 498.

[126] PRADO, Luiz Régis. **Curso de direito penal brasileiro**, parte geral: arts. 1º a 120. 8ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2009, v. 1, p. 351.

[127] ZAFFARONI; PIERANGELI, *op. cit.*, p. 498.

[128] ZAFFARONI; PIERANGELI, *loc. cit.*

[129] *Ibid.*, p. 497-498.

E justificam,

> É sabido que a extensão da legítima defesa a todos os bens jurídicos é fruto do industrialismo, pois antes ela era reservada apenas a certos bens jurídicos (vida, integridade física, honestidade, etc.). Não se pode ignorar que esta extensão e generalização é resultado da necessidade de dar segurança à riqueza que se concentrava nas cidades, diante da ameaça representada pelas massas miseráveis, que também lá se concentravam, quando a acumulação de capital produtivo não era suficiente para assimilar a sua mão-de-obra.[130]

Verifica-se, portanto, que a legítima defesa é admitida contra a agressão a qualquer bem juridicamente protegido, especialmente, aqueles tutelados pelo Direito Penal. No delito analisado neste presente trabalho, verificou-se que a agressão será dirigida, especialmente, contra a inviolabilidade dos segredos, aspecto da privacidade, bem como contra a propriedade intelectual e a livre concorrência.

Crespo apresenta um posicionamento curioso:

> Outro entendimento seria no sentido de que nem sempre se falaria em legítima defesa, uma vez que, eventualmente, não se terá uma agressão, já que é possível programar computadores para que ajam de forma remota, obtendo-se por exemplo, um ataque DoS (*Denial of Service*). Nessa concepção, como as máquinas é que fariam os ataques, não se falaria em ação humana, o que inviabilizaria a aplicação do instituto da legítima defesa. Por outro lado, poder-se-ia pensar em ação sob a égide de outra excludente: o estado de necessidade, em que há, em vez de agressão, verdadeiro conflito entre interesses jurídicos, ou mesmo a tese de inexigibilidade de conduta diversa. Isto é, ante o reconhecimento de que não havia outro comportamento que fosse exigível por parte da vítima, exclui-se a sua culpabilidade, não havendo crime. [131]

Todavia, não assiste razão este entendimento, visto que o computador é programado pelo próprio homem. As ações daquele são reflexos das ordens deste, sendo impossível e inadequado querer criar uma identidade para a máquina.

4.3.2.2 Agressão atual ou iminente

Quanto ao tempo da injusta agressão, esta deverá ser atual ou iminente.

Por iminente, entende-se aquela conduta que está prestes a acontecer, não admitindo, portanto, delongas na repulsa[132]. Por atual, entende-se aquela agressão presente,

---

[130] ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro**: parte geral. 6ª ed. rev. e atual. – São Paulo: Revista dos Tribunais, 2006, p. 501.
[131] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. – São Paulo : Saraiva, 2011, p. 116.
[132] BITENCOURT, Cezar Roberto. **Tratado de Direito Penal** – Parte Geral, vol. 1. 14ª ed. rev., atual. e ampl. –

que, já iniciada, ainda não se concluiu[133] ou aquela que acabou de acontecer[134].

Assim, pode-se aferir que é pouco provável a configuração de legítima defesa em relação ao tipo penal em análise quando a vítima é um usuário comum, visto não possuir, em regra, aparato e conhecimentos técnicos para repelir a agressão no tempo adequado. Como destacado em ponto anterior, os times de resposta a incidentes de segurança computacional realizam um monitoramento 24 horas por dia e sete dias por semana das redes por eles protegidas, podendo, assim, responder tempestivamente às invasões e tentativas de invasão.

4.3.2.3 Uso moderado dos meios necessários

Quanto aos meios necessários, estes são entendidos como

> aqueles eficazes e suficientes para repelir a agressão. Para que esteja agasalhado pela excludente em estudo, o agente deve utilizar na repulsa da agressão, os meios necessários. Meios necessários são aqueles que causam o menor dano indispensável à defesa do direito. São aqueles meios de que o agente dispõe no momento em que repele a agressão. Meios necessários são aqueles encontrados à disposição do agente, no momento da agressão, e capazes de repeli-la e que, primordialmente, deve o sujeito agredido fazer uso do meio menos lesivo que encontrar.[135]

A valoração acerca de quais meios serão os necessários para a repulsa "deve ser sempre [...] *ex ante*, isto é, do ponto de vista do sujeito no momento em que se defende"[136].

O conceito de uso moderado leva em consideração o dano causado na ação. Assim, em nenhuma hipótese, a agressão infligida pela legítima defesa poderá ser maior que a própria agressão a qual ela combate[137].

> O sujeito que age em legítima defesa deve usar de moderação, ou seja, não exceder no emprego do meio necessário para repelir a agressão. A defesa deve ser sempre proporcional à agressão nos meios e na forma de que o reagente deve agir nos limites da defesa de seu direito ou de outrem, devendo evitar, sempre que possível, impor um mal desnecessário ao seu agressor, sob pena de desfigurar a presença da

---

São Paulo : Saraiva, 2009, p. 342.

[133] PRADO, Luiz Régis. **Curso de direito penal brasileiro**, parte geral: arts. 1º a 120. 8ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2009, v. 1, p. 352.

[134] GRECO, Rogério. **Curso de Direito Penal** (parte geral). 11 ed. Rio de Janeiro : Impetus, 2009, p. 350-352.

[135] RODRIGUES, Arlindo Peixoto Gomes. **A legítima defesa como causa excludente da responsabilidade civil**. – São Paulo : Ícone, 2008, p. 68.

[136] ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro**: parte geral. 6ª ed. rev. e atual. – São Paulo: Revista dos Tribunais, 2006, p. 501.

[137] BITENCOURT, Cezar Roberto. **Tratado de Direito Penal** – Parte Geral, vol. 1. 14ª ed. rev., atual. e ampl. – São Paulo : Saraiva, 2009, p. 343.

> excludente.[138]

Assim, surge a possibilidade de legítima defesa sucessiva, ou seja, uma legítima defesa contra outra excessiva[139]. Observa-se, aqui, a manifestação do Princípio da Proporcionalidade, ilustrado na clássica máxima de Jellinek de que "não se abatem pardais disparando canhões"[140].

> Na legítima defesa, a ponderação dos males só pode funcionar como "corretivo", isto é, como limite. A legítima defesa não pode contrariar o objetivo geral da ordem jurídica - a viabilização da coexistência - de maneira que, quando existe uma desproporção muito grande entre o mal que evita quem se defende e o que lhe quer causar quem o agride, porque o primeiro é ínfimo comparado com o segundo, a defesa deixa de ser legítima.[141]

Como concluído no item anterior, também se mostra difícil a configuração da legítima defesa em relação à invasão de dispositivo informático quando a vítima é um usuário comum, pois, normalmente, não possui conhecimentos técnico-profissionais para repelir a agressão de modo adequado, podendo agredir o próprio invasor.

4.3.2.4 Animus defendendi

O último elemento caracterizador da legítima defesa é o *animus defendendi*. Ao contrário dos demais requisitos de ordem objetiva, este possui caráter subjetivo. Como assevera Prado, o "agente deve ser portador do elemento subjetivo, consistente na ciência da agressão e no ânimo ou vontade (*animus defendi*) de atuar em defesa de direito seu ou de outrem"[142].

> Embora não se exija a *consciência da ilicitude*, é necessário que se tenha conhecimento da ação agressiva, além do propósito de defender-se. A legítima defesa deve ser *objetivamente necessária* e *subjetivamente orientada* pela vontade de defender-se.[143]

---

[138] RODRIGUES, Arlindo Peixoto Gomes. **A legítima defesa como causa excludente da responsabilidade civil**. – São Paulo : Ícone, 2008, p. 69.
[139] PRADO, Luiz Régis. **Curso de direito penal brasileiro**, parte geral: arts. 1º a 120. 8ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2009, v. 1, p. 352.
[140] JELLINEK, Georg Apud BONAVIDES, Paulo. **Curso de Direito Constitucional**. 15. ed. rev., atual. e ampl. – São Paulo : Malheiros, 2004, p. 402.
[141] ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro**: parte geral. 6ª ed. rev. e atual. – São Paulo: Revista dos Tribunais, 2006, p. 497.
[142] PRADO, *op. cit.*, p. 353.
[143] BITENCOURT, Cezar Roberto. **Tratado de Direito Penal** – Parte Geral, vol. 1. 14ª ed. rev., atual. e ampl. – São Paulo : Saraiva, 2009, p. 344.

Tal requisito trata-se de um verdadeiro divisor de águas entre a ação criminosa e a legítima defesa. É esse elemento que distingue os dois comportamentos. Complementa Bitencourt:

> O *elemento subjetivo* que compõe a estrutura do tipo penal assume transcendental importância na definição da conduta típica. É através da identificação do *animus agendi* que se consegue visualizar e qualificar a atividade comportamental de alguém; somente conhecendo e identificando a intenção – *vontade* e *consciência* – do agente poder-se-á classificar um comportamento como típico, correspondente a este ou aquele dispositivo legal, particularmente quando a figura típica exigir também o *especial fim* de agir [...]. [144] (grifos originais)

4.3.3 "Legítima defesa digital": novo conceito ou apenas um novo caso?

No Brasil, a *legítima defesa digital* surgiu, primeiramente, no Substitutivo ao PLS 76/2000, PLS 137/2000 e PLC 89/2003, apresentado pelo Senador Eduardo Azeredo, que definia "defesa digital" como a

> manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta à ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação.[145]

Todavia, essa definição foi duramente criticada, pois criava uma figura específica de defesa que muito se distanciava daquela respaldada no artigo 25 do Código Penal. Deixava claro, ainda, que o instituto só poderia ser utilizado por "agente técnico ou profissional habilitado". Foi finalmente retirada após avaliação feita pela Comissão de Constituição, Justiça e Cidadania (CCJC) do Senado Federal.

A prática do *ethical hacking*, em sua modalidade *hacking back*, pelos Times de Resposta a Incidentes de Segurança Computacional quando estão diante da prática do delito

---

[144] BITENCOURT, Cezar Roberto. **Tratado de Direito Penal** : Parte Especial – Dos crimes contra a pessoa, vol. 2. 9. ed. – São Paulo : Saraiva, 2009, p. 296.

[145] BRASIL. Substitutivo ao PLS 76/2000, PLS 137/2000 e PLC 89/2003, apresentado pelo Senador Eduardo Azeredo. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei n° 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei n° 9.296, de 24 de julho de 1996, o Decreto-Lei n° 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei n° 10.446, de 8 de maio de 2002, e a Lei n° 8.078, de 11 de setembro de 1990 (Código do Consumidor), para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e da outras providencias. Disponível em: <http://www.oab.org.br/pdf/substitutivoazeredo.pdf>. Acesso em: 03 jul 2013.

de obtenção de informações privadas por meio de invasão a dispositivos informáticos deverá ser considerada legítima defesa nos termos estabelecidos no próprio Código Penal.

A injusta agressão a um bem jurídico, o primeiro requisito, está configurada, pois o tipo penal previsto no art. 154-A, § 3º, do CP, protege, em especial, o "conteúdo das comunicações eletrônicas privadas, segredos comerciais ou industriais e informações sigilosas, assim definidas em lei".

A resposta atual ou iminente à agressão, o segundo requisito, está relacionada à atuação dos CSIRTs, visto que atuam monitorando incessantemente todas as atividades nas redes de computadores de determinada empresa ou órgão, protegendo, assim, todo o fluxo de informações.

O uso moderado dos meios necessários, o terceiro requisito, está claramente presente na técnica do *hacking back*, focada na cessação da invasão, bem como na recuperação das informações subtraídas.

O *animus defendendi*, o quarto requisito, deverá ser avaliado caso a caso. Todavia, aqui, presumir-se-á presente, pois se está analisando a conduta de um time formado por profissionais que atuam na área de segurança da informação.

Diante do exposto, não se pode dizer que a *legítima defesa digital* trata-se de um novo conceito. Ela é apenas um novo caso dentro da clássica previsão do Código Penal, nascida diante da necessidade de proteção das informações contra os novos agentes criminosos que se utilizam do meio ambiente virtual em suas empreitadas delituosas.

4.3.4 Excessos na prática do ethical hacking

O artigo 23, parágrafo único, do Código Penal, prevê que "o agente, em qualquer das hipóteses deste artigo, responderá pelo excesso doloso ou culposo".

Configura o excesso quando há "flagrante desproporção entre a ofensa e a agressão, quando o agente responde com um tiro a um tapa desferido pelo agressor e quando o agente mata uma criança porque esta adentrou ao seu pomar e apanhou algumas frutas"[146].

O excesso na prática do *ethical hacking* como legítima defesa pode ser verificado quando, por exemplo, na tentativa de recuperar os arquivos, informações além daquelas

[146] RODRIGUES, Arlindo Peixoto Gomes. **A legítima defesa como causa excludente da responsabilidade civil**. – São Paulo : Ícone, 2008, p. 69.

subtraídas são obtidas, podendo ser do próprio agressor ou de um usuário diverso que tenha seu computador controlado. Verifica-se nessas duas hipóteses, respectivamente, um uso imoderado e uma agressão contra terceiros.

É difícil dizer se tais excessos seriam puníveis na esfera penal, visto que tanto o delito de invasão de dispositivo informático quanto o crime de exercício arbitrário das próprias razões não preveem a modalidade culposa. Assim, para que houvesse a sanção penal nesses casos, o excesso deveria ser doloso, além de a conduta dever amoldar-se a todos os demais elementos previstos no art. 154-A, *caput*, do Código Penal.

5 CONCLUSÃO

Os efeitos de legalizar o *ethical hacking*, segundo Jayaswal, Yurcik e Doss, podem ser representados por dois extremos: um caminho para a devida proteção das informações ou uma trilha para um caótico cenário no melhor estilo "velho oeste"[147].

Embora a visão dos citados autores esteja embasada no Direito norte-americano, poderá ser aplicada à realidade brasileira. Como observado ao final do primeiro capítulo, o ordenamento jurídico pátrio conta com um tipo penal específico que pune as invasões de dispositivos informáticos, bem como a obtenção e a divulgação das informações em decorrência do ataque.

Assim, ao invés daqueles dois cenários serem originados a partir da legalização do *ethical hacking*, eles surgiriam, no Brasil, em razão de a prática do *ethical hacking*, em sua modalidade *hacking back*, ser reconhecida ou não como legítima defesa, obedecendo, portanto, todos os seus requisitos.

Na visão otimista, o *ethical hacking*, aqui considerado como meio de legítima defesa, representaria uma opção para a contenção dos efeitos das práticas criminosas em meio eletrônico, visto a redução dos danos sofridos pelas invasões ser seu principal objetivo.

Apesar de existirem outros recursos jurídicos capazes de punir o invasor, estes se mostram lentos devido à instantaneidade dos ataques eletrônicos, sendo uma resposta imediata no momento da invasão mais adequada para a devida proteção das informações. Lembrando, novamente, que uma vez de posse da informação, o agente criminoso pode, fácil e rapidamente, gerar diversas cópias e espraiá-las pela internet.

No contexto pessimista, o *ethical hacking*, aqui não considerado em nenhuma hipótese meio de legítima defesa, encorajaria a prática do vigilantismo em vez do uso de recursos jurídicos, criando-se, assim, um cenário de faroeste. As empresas contratariam outras que prestassem serviços de segurança de informação, a exemplo da *Wells Fargo Private Security*[148], fazendo estas o papel de verdadeiros pistoleiros.

Tais empresas praticariam o *ethical hacking* sem limites, pois o Poder Judiciário e a legislação penal apresentar-se-iam lentos, incapazes de solucionar plenamente os problemas

---

[147] JAYASWAL, Vikas; YURCIK, William; DOSS, David. Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism? In: **IEEE 2002 International Symposium on Technology and Society (ISTAS'02)**: Social Implications of Information and Communication Technology. Proceedings. 2002. ISBN: 0-7803-7284-0, p. 384. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1013841>. Acesso em: 03 jul 2013.

[148] Disponível em: <https://www.wellsfargo.com/privacy_security/online/protect>. Acesso em: 03 jul 2013.

advindos das invasões. O *ethical hacking*, longe dos parâmetros estabelecidos pela legítima defesa, seria, portanto, a medida mais eficaz para a contenção desses delitos. Sistemas invadidos e controlados remotamente por um sistema principal capaz de executar ações por meio daqueles poderiam ser considerados alvos, pois não haveria limites para o contra-ataque. As ferramentas de *ethical hacking* continuariam a se desenvolver e seriam utilizadas secretamente até que medidas legais e judiciais fossem implementadas. Com a ausência de fiscalização na realização do *ethical hacking* e o desenfreado número de ataques e contra-ataques, a integridade da internet restar-se-ia prejudicada.

É certo que alguns casos chegariam ao Poder Judiciário, mas seria uma quantidade mínima. Em outros, a própria vítima contrataria uma empresa de segurança capaz de rastrear o invasor e buscar fazer justiça com as próprias mãos, passando, agora, à verdadeira condição de criminosa, podendo sua conduta ser tipificada, a depender do caso, no crime de exercício arbitrária das próprias razões ou no próprio crime de invasão de dispositivo informático, agindo, assim, em concurso de agentes. Outra implicação desse péssimo cenário seria a proliferação de seguros contra invasões eletrônicas.

Diante do exposto, qual seria a solução mais adequada para a sociedade brasileira? Os futuros cenários de uso do *ethical hacking* variam da paz ao caos. Este trabalho posiciona-se no sentido de se construir uma postura ofensiva. Sendo hipótese de legítima defesa, dentro de todos aqueles requisitos exigidos pelo art. 25 do Código Penal, a indústria iria desenvolver aplicativos capazes de interromper tais ataques, chegando-se, talvez, ao ponto de os usuários domésticos serem capazes de evitar tais invasões. Verifica-se, por fim, que os obstáculos mais difíceis de serem transpostos e que envolvem diretamente o tema são aqueles de cunho social, em especial, a responsabilidade legal do invasor e daquele que age em excesso de legítima defesa.

REFERÊNCIAS

Abin monta rede para monitoramento dos protestos. **O Povo**. Disponível em: <http://www.opovo.com.br/app/opovo/radar/2013/06/20/noticiasjornalradar,3077693/abin-monta-rede-para-monitoramento-dos-protestos.shtml>. Acesso em: 03 jul 2013.

BITENCOURT, Cezar Roberto. Invasão de dispositivo informático. **Atualidades do Direito**. Disponível em: <http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico/>. Acesso em: 03 jul 2013.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**: Parte Especial – Dos crimes contra a pessoa, vol. 2. 9. ed. – São Paulo : Saraiva, 2009.

_____. **Tratado de Direito Penal**: Parte Geral, vol. 1. 14. ed. rev., atual. e ampl. – São Paulo : Saraiva, 2009.

BOARATI, Vanessa. **Economia para o direito**. Série noções de direito – Barueri : Manole, 2006.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 15. ed. rev., atual. e ampl. – São Paulo : Malheiros, 2004.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 03 jul 2013.

_____. Decreto-Lei n. 2.848, de 07 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 03 jul 2013.

_____. Lei n. 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei n. 8.112, de 11 de dezembro de 1990; revoga a Lei n. 11.111, de 5 de maio de 2005, e dispositivos da Lei n. 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 03 jul 2013.

_____. Lei n. 556, de 25 de junho de 1850. Código Comercial. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l0556-1850.htm>. Acesso em: 03 jul 2013.

_____. Lei n. 8.137, de 27 de dezembro de 1990. Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8137.htm>. Acesso em: 03 jul 2013.

_____. Lei n. 9.296, de 24 de julho de 1999. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 03 jul 2013.

_____. Lei n. 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9279.htm>. Acesso em: 03 jul 2013.

_____. Lei n. 9.504, de 30 de setembro de 1997. Estabelece normas para as eleições. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9504.htm>. Acesso em: 03 jul 2013.

_____. **Sociedade da Informação no Brasil**: Livro Verde. Brasília : Ministério da Ciência e Tecnologia, 2000. Disponível em <http://www.mct.gov.br/index.php/content/view/18878.html>. Acesso em: 03 jul 2013.

_____. Projeto de Lei do Senado n. 236, de 09 de julho de 2012. Reforma do Código Penal Brasileiro. Disponível em: <http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=106404>. Acesso em: 03 jul 2013.

_____. Projeto de Lei n. 2793, de 29 de novembro de 2011. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>. Acesso em: 03 jul 2013.

_____. Projeto de Lei n. 84, de 24 de fevereiro de 1999. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>. Acesso em: 03 jul 2013.

_____. Substitutivo ao PLS 76/2000, PLS 137/2000 e PLC 89/2003, apresentado pelo Senador Eduardo Azeredo. Altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei n. 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei n. 9.296, de 24 de julho de 1996, o Decreto-Lei n. 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei n. 10.446, de 8 de maio de 2002, e a Lei n. 8.078, de 11 de setembro de 1990 (Código do Consumidor), para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e da outras providencias. Disponível em: <http://www.oab.org.br/pdf/substitutivoazeredo.pdf>. Acesso em: 03 jul 2013.

_____. Superior Tribunal de Justiça. AGRAVO REGIMENTAL. RECURSO ESPECIAL. PENAL. VIOLAÇÃO DE DIREITO AUTORAL. REJEIÇÃO DA DENÚNCIA. PRINCÍPIO DA ADEQUAÇÃO SOCIAL QUE NÃO SE APLICA. AgRg no REsp 1356243/MS. Rel. Min. Marco Aurélio Belizze. Publicado em: DJe, 18 mar. 2013.

_____. Tribunal de Justiça de Minas Gerais. APELAÇÃO CRIMINAL - VIOLAÇÃO DE DIREITO AUTORAL - PRINCÍPIO DA ADEQUAÇÃO SOCIAL - CASO CONCRETO - ABSOLVIÇÃO DECRETADA - RECURSO PROVIDO. Apelação Criminal nº 1.0210.07.046952-8/001. Rel. Des. Doorgal Andrada. Publicado em: 16 jun. 2010.

CANONGIA, Claudia; MANDARINO JÚNIOR, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, Brasília, v. 14, n. 29, p. 21-46,

dez. 2009. Disponível em: <http://www.cgee.org.br/parcerias/p29.php>. Acesso em: 03 jul 2013.

CASTELLS, Manuel. **A Sociedade em Rede**. Vol. 1. 8ª ed. rev. e ampl. Tradução de Roneide Venâncio Majer e Klauss Brandini Gerhardt. – São Paulo: Paz e Terra, 2005.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA DO BRASIL. Estatísticas dos Incidentes Reportados ao CERT.br. Brasil, 2013. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 03 jul 2013.

_____. **Cartilha de Segurança para a Internet**. Versão 4.0, de 04 de junho de 2012. Disponível em: <http://cartilha.cert.br/>. Acesso em: 03 jul 2013.

CONSELHO DA EUROPA. Convenção sobre o Cibercrime. Budapeste, 23 de novembro de 2001. Disponível em: <http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf>. Acesso em: 03 jul 2013.

_____. Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Actos de Natureza Racista e Xenófoba praticados através de Sistemas Informáticos. Estrasburgo, 28 de janeiro de 2003. Disponível em: <http://dre.pt/pdf1sdip/2009/09/17900/0641506421.pdf>. Acesso em: 03 jul 2013.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. – São Paulo : Saraiva, 2011.

DENNING, Dorothy E. The Ethics of Cyber Conflict. In: HIMMA, Kenneth Einar; TAVANI, Herman T. **The Handbook of Information and Computer Ethics**. Hoboken, New Jersey : Wiley, 2008. p. 407-428. Disponível em: < http://www.e-reading.su/bookreader.php/141465/The_Handbook_of_Information_and_Computer_Ethics.pdf#page=441>. Acesso em: 03 jul 2013.

ESTADOS UNIDOS DA AMÉRICA. United States Code. Disponível em: <http://www.law.cornell.edu/uscode/text/18/1030?quicktabs_8=1#quicktabs-8>. Acesso em: 03 jul 2013.

FIGUEIREDO, Leonardo Vizeu. **Lições de direito econômico**. 4ª ed. – Rio de Janeiro : Forense, 2011.

FIORETTI, Julio. **Legítima Defesa**: Estudo de Criminologia. Traduzido por Fernando Bragança. – Belo Horizonte : Líder, 2002.

FONTES, Edison. **Segurança da Informação**: O usuário faz a diferença. – São Paulo : Saraiva, 2006.

GIBSON, William. **Neuromancer**. Traduzido por Fábio Fernandes. 4ª ed. – São Paulo : Aleph, 2008.

GONZÁLEZ, Ignacio Siles. Cibernética y sociedad de la información: el retorno de un sueño eterno. **Signo y Pensamiento**, Bogotá, n. 50, p. 84-99, jun. 2007. Disponível em: <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-48232007000100007&lang=pt>. Acesso em: 03 jul 2013.

GRAU-KUNTZ, Karin. A quem pertence conhecimento e cultura? Uma reflexão sobre o discurso de legitimação do direito de autor. **Liinc em Revista**, Rio de Janeiro, v. 7, n. 2, p. 405-415, set. 2011. Disponível em: <http://revista.ibict.br/liinc/index.php/liinc/article/viewFile/437/324>. Acesso em: 03 jul 2013.

GRECO, Rogério. **Curso de Direito Penal** (parte geral). 11 ed. Rio de Janeiro : Impetus, 2009.

GRECO, Rogério. **Direito Penal do Equilíbrio**: uma visão minimalista do Direito Penal. 5ª ed. – Niterói : Impetus, 2010.

Hijacking airplanes with an Android phone. **Help Net Security**. Disponível em: <http://www.net-security.org/secworld.php?id=14733>. Acesso em: 03 jul 2013.

INTERNET WORLD STATS. **Internet Usage Statistics**. Disponível em: <http://www.internetworldstats.com/stats.htm>. Acesso em: 03 jul 2013.

JAYASWAL, Vikas; YURCIK, William; DOSS, David. Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism? In: **IEEE 2002 International Symposium on Technology and Society (ISTAS'02)**: Social Implications of Information and Communication Technology. Proceedings. 2002. ISBN: 0-7803-7284-0. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1013841>. Acesso em: 03 jul 2013.

KARASINSKI, Lucas. PRISM: entenda toda a polêmica sobre como os EUA controlam você. **Tecmundo**. Disponível em: <http://www.tecmundo.com.br/privacidade/40816-prism-entenda-toda-a-polemica-sobre-como-os-eua-controlam-voce.htm>. Acesso em: 03 jul 2013.

KESAN, Jay P.; HAYES, Carol M. Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace. In: **Harvard Journal of Law & Technology**, Cambridge, Massachusetts, vol. 25, nº 2, Spring 2012. Disponível em: <http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech415.pdf>. Acesso em: 03 jul 2013.

KNIGHT, William. License to hack? - Ethical hacking. **Infosecurity**. Disponível em: <http://www.infosecurity-magazine.com/view/4611/license-to-hack-ethical-hacking/>. Acesso em: 03 jul 2013.

MARTI, Yohannis; VEGA-ALMEIDA, Rosa Lidia. Sociedad de la información: Los mecanisnos reguladores en el contexto de una sociedad emergente. **Ciência da Informação**, Brasília, v. 34, n. 1, p. 37-44, jan./abr. 2005. Disponível em: <http://www.scielo.br.ez11.periodicos.capes.gov.br/pdf/ci/v34n1/a05v34n1.pdf>. Acesso em: 03 jul 2013.

MARTINS, Matheus Barcelos; PAZÓ, Cristina Grobério. Acesso ao conhecimento no âmbito digital em face dos direitos autorais. **Revista do Conselho da Justiça Federal**, Centro de Estudos Judiciários, Brasília, Ano XVI, nº 56, jan./abr. 2012

MATTELART, Armand. **Historia da Sociedade da Informação**. Traduzido por Nicolas Nyimi Campanario. – São Paulo: Edições Loyola, 2002.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 4. ed. rev. e atual. – São Paulo : Saraiva, 2009.

MONTEIRO NETO, João Araújo. Crimes Informáticos: uma abordagem dinâmica ao direito penal informático. **Pensar** (UNIFOR), v. 8, p. 39-54, 2003. Disponível em: <http://hp.unifor.br/pdfs_notitia/1690.pdf>. Acesso em: 03 jul 2013.

MONTEIRO NETO, João Araújo. **Aspectos constitucionais e legais do crime eletrônico**. 2008. 191 f. Dissertação (Mestrado em Direito) – Centro de Ciências Jurídicas, Universidade de Fortaleza, 2008.

MONTEIRO, Renato Leite. **Crimes eletrônicos**: uma análise econômica e constitucional. 2010. 192 f. Dissertação (Mestrado em Direito) - Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2010.

MOREIRA, Thiago Freire Feijão. **Série de Diálogos**: Tecnologia na Educação - Ensino Híbrido. Disponível em: <http://www.youtube.com/watch?v=MQpcqnXwnMY>. Acesso em: 03 jul 2013.

ORGANIZAÇÃO MUNDIAL DA PROPRIEDADE INTELECTUAL. Módulo 7: Patentes. **Curso Geral de Propriedade Intelectual**, 2011.

_____. Sítio eletrônico do Centro de *e-learning*. Disponível em: <http://www.wipo.int/academy/pt/courses/distance_learning/catalog/welc.html>. Acesso em: 03 jul 2013.

ORGANIZAÇÃO MUNDIAL DO COMÉRCIO. Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio. Marrakesh, 15 de abril de 1994. Disponível em: <http://www.itamaraty.gov.br/o-ministerio/conheca-o-ministerio/tecnologicos/cgc/solucao-de-controversias/mais-informacoes/texto-dos-acordos-da-omc-portugues/1.3-anexo-1c-acordo-sobre-aspectos-dos-direitos-de-propriedade-intelectual-relacionados-ao-comercio-trips/view>. Acesso em: 03 jul 2013.

PEIXOTO, Mário César Pintaudi. **Criando um CSIRT**: Computer Security Incident Response Team e entendendo seus desafios. – Rio de Janeiro : Brasport, 2008.

PINHEIRO, Patrícia Peck. **Direito Digital**. 3ª ed. rev., atual. e ampl. – São Paulo : Saraiva, 2009.

PORTUGAL. **Livro verde para a sociedade da informação em Portugal**. Lisboa: Ministério da Ciência e da Tecnologia, Missão para a Sociedade da Informação, 1997. Disponível em <http://www2.ufp.pt/~lmbg/formacao/lvfinal.pdf>. Acesso em: 03 jul 2013.

PRADO, Luiz Régis. **Curso de direito penal brasileiro**, parte geral: arts. 1º a 120. 8ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2009, v. 1.

_____. **Curso de direito penal brasileiro**, parte especial: arts. 121 a 249. 11ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2012, v. 2.

RODRIGUES, Arlindo Peixoto Gomes. **A legítima defesa como causa excludente da responsabilidade civil**. – São Paulo : Ícone, 2008.

SANTOS, Márcio Fernando Candéo. O direito ao segredo: a violação da intimidade no âmbito dos direitos da personalidade. In: XVIII CONGRESSO NACIONAL DO CONPEDI, São Paulo, 2009. **Anais do XVIII Congresso Nacional do CONPEDI**, São Paulo, 2009, p. 5547. Disponível em: <http://www.publicadireito.com.br/conpedi/manaus/arquivos/Anais/sao_paulo/2250.pdf>. Acesso em: 03 jul 2013.

SERVIÇO DE RESPOSTA A INCIDENTES DE SEGURANÇA INFORMÁTICA. Enquadramento. Disponível em: http://www.cert.pt/index.php/institucional/enquadramento-e-motivacao. Acesso em: 03 jul 2013.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 32ª ed. rev., atual. e ampl. – São Paulo : Malheiros, 2009.

SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático**. Série Ciência do Direito Penal Contemporânea, vol. 4. – São Paulo : Revista dos Tribunais, 2003.

SOFTWARE ENGINEERING INSITUTE. **Denial of Service Attacks**. Carnegie Mellon University. Disponível em: <http://www.cert.org/tech_tips/denial_of_service.html>. Acesso em: 03 jul 2013.

VIANNA, Túlio Lima. **Fundamentos de direito penal informático**: do acesso não autorizado a sistemas computacionais. – Rio de Janeiro : Forense, 2003.

WERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ciência da Informação**, Brasília, v. 29, n. 2, p. 71-77, maio/ago. 2000. Disponível em: <http://www.scielo.br.ez11.periodicos.capes.gov.br/scielo.php?script=sci_arttext&pid=S0100-19652000000200009&lng=pt&nrm=iso&tlng=pt>. Acesso em: 03 jul 2013.

ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro**: parte geral. 6ª ed. rev. e atual. – São Paulo: Revista dos Tribunais, 2006.