A Internet e o Direito: Uma abordagem sobre cibercrimes

Humberto Lidio Antonelli[1], **Emerson Gervásio de Almeida**[2]

[1]Departamento de Ciência da Computação – Universidade Federal de Goiás (UFG)– Campus Catalão Avenida Dr. Lamartine Pinto de Avelar, 1120 – Setor Universitário – 75.704-020 – Catalão – GO – Brasil

[2]Departamento de Engenharia Civil – Universidade Federal de Goiás (UFG)– Campus Catalão Avenida Dr. Lamartine Pinto de Avelar, 1120 – Setor Universitário – 75.704-020 – Catalão – GO – Brasil

humberto.antonelli@gmail.com, emersongervasio@yahoo.com.br

Abstract. *Technological advances and the advent of the Internet brought about the emergence of new types of crimes, and new ways of doing crimes known and typified by law, cybercrime born that way. This paper aims to briefly review raved about the cyber crime, but also expose a view of what exists in Brazil, the legal regulations to combat these new criminal charges.*

Resumo. *Os avanços tecnológicos e o surgimento da Internet*[1] *propiciaram o aparecimento de novos tipos de crimes, além de novas maneiras de praticar crimes já conhecidos e tipificados por lei, nasceu assim o cibercrime. Este trabalho tem por objetivo discorrer brevemente uma análise a cerca dos cibercrimes, como também, expor uma visão sobre o que existe, no Brasil, de regulamentação jurídica no combate à estas novas práticas ilícitas.*

1. Introdução

As últimas décadas foram marcadas por avanços na área da informática e da tecnologia, sendo que o marco principal está relacionado ao surgimento da Internet, que permitiu uma numerosa troca de informações em um curto espaço de tempo entre as diversas partes do planeta, além de proporcionar uma alta taxa de inclusão digital.

Com o advento da Internet e o crescimento expressivo do número de usuários, chegando aos 2 bilhões em 2010, segundo dados da *International Telecommunication Union* (ITU)[2], intensificaram-se também os crimes digitas ou cibercrimes. De acordo com os dados do SaferNet Brasil[3], no primeiro semestre de 2011 foram registradas 19.311 denúncias acerca de crimes cibernéticos, isso representa um aumento de 42,4% em comparação com o mesmo período de 2006.

O presente artigo tem como objetivo expor uma abordagem geral acerca dos cibercrimes e o que existe de regulamentação nos entraves de ordem jurídica, que o uso inapropriado do espaço cibernético pode levar, verificando se a legislação brasileira encontra-se preparada para este tipo de crime. Para tanto, a metodologia utilizada foi baseada em levantamento bibliográfico.

[1]Segundo o dicionário Michaelis, a palavra Internet se escreve com letra maiúscula

[2]http://www.itu.int/ITU-D/ict/statistics

[3]http://www.safernet.org.br

Este artigo está organizado da seguinte forma: a seção 2 discorre de maneira breve sobre a Internet e os cibercrimes, tratando de maneira mais específica os cibercrimes na seção 3. A seção 4 aborda sobre a Convenção de Budapeste e as leis brasileiras acerca dos cibercrimes. Finalmente conclui-se o artigo na seção 5.

2. Breves considerações acerca da Internet e os cibercrimes

Atualmente, a Internet é uma rede que interliga milhões de computadores em torno de todo o mundo. Ela nasceu em 1969, de um projeto do Departamento de Defesa dos Estados Unidos (DoD) como o nome de *Advanced Research Projects Agency Network* (ARPANET). O objetivo apresentado para este projeto era garantir que as comunicações fossem capazes de sobreviver a um ataque nuclear. Inicialmente, a rede era composta por apenas quatro Universidades, a Universidade da Califórnia (Los Angeles), SRI (Stanford Research Institute), Universidade de Utah e Universidade da Califórnia (Santa Bárbara). O desenvolvimento do protocolo TCP/IP, entre 1973 e 1978, possibilitou a expansão e incorporação de diversas redes [Almeida 2005, Pinheiro 2006, Henning 1993].

Até o ano de 1990, a Internet era controlada pelo Departamento de Defesa dos Estados Unidos com seu uso restrito. A partir deste ano, por ter uma tecnologia já considerada obsoleta, a ARPANET foi retirada de operação e a administração foi confiada à *National Science Foundation* (NSF) com o nome de NSFNET, que foi extinta em 1995 abrindo caminho para a operação privada da Internet, a qual possibilitou rapidamente o crescimento da rede. É importante ressaltar que a criação do *World Wide WEB* (WWW) por Robert Caillaiu e Tim Berners-Lee, do *HyperText Markup Language* (HTML), e dos *Browsers* foram decisivos para a expansão da utilização da Internet [Castells 2003, Pinheiro 2006, Andrade 2006].

No Brasil, o primeiro contato com a Internet ocorreu em 1988, quando as comunidades acadêmicas do Rio de Janeiro e São Paulo foram incorporadas à rede. Em 1989, o governo federal criou a Rede Nacional de Pesquisa (RNP), que montou toda a infra-estrutura denominada espinha dorsal (ou *backbone*), para receber o *link* internacional e disponibilizar os serviços de acesso à Internet para a comunidade acadêmica e agências do governo. Apenas no ano de 1994 iniciou-se a exploração comercial com o projeto da Embratel em parceria do Ministério da Ciência e Tecnologia (MCT) e das Comunicações (MC), permitindo acesso a Internet através das linhas telefônicas [Henning 1993, Vieira 2003, Queiroz et al. 2008].

Atualmente, existem diferentes métodos de acesso a Internet, seja através de uma linha telefônica (banda larga ou discada) ou sem fio (rádio, celular ou satélite). A popularização e facilidade de acesso à Internet possibilitou que grande parte da população entrasse na rede.

A disseminação do acesso à Internet trouxe inúmeros benefícios, como facilidade de comunicação, novas formas de relacionamentos pessoais, profissionais e comerciais, entre outros. Entretanto, a Internet facilitou também a prática de crimes existentes (estelionato, por exemplo) e, sobretudo, o surgimento de uma nova modalidade de práticas ilícitas, o cibercrime, além de criminosos especializados que se proliferam em todo o mundo, causando danos de todas as ordens [Queiroz et al. 2008, Couri 2009].

Com o surgimento de novas práticas ilícitas é preciso ter em vista que, num mundo cada vez mais informatizado, há a necessidade de que o Direito Penal também acompanhe

as constantes evoluções tecnológicas, afim de garantir a aplicação de punições adequadas e, por conseguinte, atingir o ideal da justiça e a promoção da paz social.

3. Os cibercrimes

Existem várias nomenclaturas utilizadas para designar um crime praticado através de um computador conectado à Internet, dentre elas pode-se citar: crimes virtuais, digitais, informáticos, fraude informática, delitos cibernéticos, cibercrimes, entre outras. Neste trabalho, foi adotado como designação padrão o termo "cibercrimes".

Cibercrime significa: "qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados" [Neto and Guimarães 2003]. Em outras palavras, é aquele realizado contra pessoas ou entidades com o objetivo de obter benefício próprio ou prejudicar a estrutura de funcionamento ou a imagem pública do atacado, através de ferramentas tecnológicas conectadas à rede mundial de computadores [Bueno and Coelho 2008, Conte and Santos 2008, da Sivla 2009].

São várias as classificações utilizadas nos cibercrimes. Em geral, os autores costumam classificá-los como cibercrimes próprios e cibercrimes impróprios. O primeiro refere-se aos crimes praticados contra um sistema de informática em todas as suas formas. São novos tipos de delitos praticados contra a informática, onde ela é tratada como bem juridicamente protegido e, em vista da escassa legislação existente, alguns fatos, portanto, não podem ser punidos. Pode-se citar com exemplo destes tipo de crimes a violação de e-mail, pirataria de software, danos provocados por vírus, entre outros [Neto and Guimarães 2003, Bueno and Coelho 2008, Redivo and Monteiro 2009].

O cibercrime impróprio diz respeito aos crimes praticados contra outros valores sociais ou bens jurídicos no qual o agente utiliza-se do sistema de informática para praticá-los. Este tipo de crime consiste basicamente em uma nova forma de praticar velhos crimes, já tipificados pela lei brasileira, na qual o computador e a Internet são utilizados como instrumentos para a prática do delito. Um exemplificação deste tipo de crime é o estelionato, previsto no artigo 171, do Código Penal Braseiro[4] [Queiroz et al. 2008, Couri 2009, Susana and Leite 2010, Aquotti and Takushi 2010].

De acordo com a "Convenção sobre a Cibercriminalidade" [of Europe 2001, BRASIL 2007], adotada pelo Conselho da Europa em 2001, pode-se destacar como cibercrimes:

- Infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos:
  - acesso doloso e ilegal a um sistema de informática;
  - interceptação ilegal de dados ou comunicações telemáticas;
  - atentado à integridade dos dados (conduta própria de um subgrupo *hacker*, conhecido como *cracker*);
  - atentado à integridade de um sistema;
  - produção, comercialização, obtenção ou posse de aplicativos ou códigos de acesso que permitam a prática dos crimes acima indicados.
- Infrações informáticas:

[4]Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm

  - falsificação de dados;
  - estelionatos eletrônicos.
- Infrações relativas ao conteúdo:
  - pornografia infantil;
  - racismo e xenofobia.
- Atentado à propriedade intelectual e aos direitos que lhe são conexos:
  - Exibição pública de filme sem autorização do detentor dos direitos.

4. A Convenção de Budapeste e a legislação brasileira

A "Convenção de Budapeste" (ou "Convenção sobre a Cibercriminalidade") foi o primeiro tratado internacional com a finalidade de tipificar os principais crimes cometidos através da Internet e outras redes de computadores. A negociação do tratado teve início em 1997, seguindo uma determinação do Conselho da Europa, que o caráter transnacional de cibercrime somente poderia ser tratado a nível global. A Convenção de Budapeste foi aberta para assinatura em novembro de 2001, entrando em vigor em julho de 2004 [Archick 2002, Solagna and Souza 2011]. Até 16 de agosto de 2011, 16 (dezesseis) Estados haviam assinado, ratificado ou aderido à Convenção, enquanto mais 31 (trinta e um) Estados a assinaram, mas não a ratificaram[5] [Redivo and Monteiro 2009, Gouveia 2007].

Essa convenção possui uma significativa importância pelo fato de ser bastante atualizada e, com isso, ter posições definidas, que objetivam impedir os crimes praticados contra a confidencialidade, integridade e disponibilidade de sistemas e dados informáticos, bem como a utilização fraudulenta dos mesmos. Segundo seu Preâmbulo, o principal objetivo da Convenção é o de estabelecer uma "política criminal comum" para melhor combater crimes relacionados a computadores em todo o mundo através de harmonização das legislações nacionais, aumentando a capacidade de aplicação da lei judicial, e melhorar a cooperação internacional [of Europe 2001, Souza and Pereira 2009].

A Convenção é dividida em quatro capítulos. O primeiro capítulo trata de questões de direito material, como o acesso ilegal, uso indevido de aparelhos e crimes relacionados à pornografia infantil. O segundo trata de medidas que devem ser tomadas a nível nacional, entre elas a preservação de dados armazenados, busca e apreensão de dados informáticos e interceptação de dados de conteúdo. O terceiro contém disposições relativas à assistência mútua em casos de crime tradicional e de cibercrime, bem como as regras de extradição. O quarto contém as disposições finais, com destaque para os artigos que tratam da adesão à Convenção, da aplicação territorial e de seus efeitos [of Europe 2001, Souza and Pereira 2009].

Apesar da Convenção possuir um texto flexível e, sobretudo, apontar caminhos e não propor soluções rígidas, o Brasil não pode simplesmente aderir à Convenção, mas precisa ser convidado pelo Conselho Europeu. Tal fator é observado no artigo 37º, que trata da adesão à Convenção, que diz: "(...) O Comitê de Ministros do Conselho da Europa pode(...) convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção" [of Europe 2001].

Segundo estudo realizado pela empresa Akamai[6], no início de 2011, o Brasil era o quarto país de onde mais se originam ataques virtuais a sites, sendo responsável por

[5] Segundo dados do sítio do Concelho da Europa (http://conventions.coe.int)

[6] http://www.akamai.com

8% dos ataques. Dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[7] diz que o número de fraudes na Internet cresceu 6.513% no País entre o período de 2004 a 2009.

A justiça brasileira encontra-se desprovida de leis que possibilitem a punição de condutas reprováveis praticadas no mundo virtual. Atualmente, no país, existem apenas as Leis 9.609/98 e 9.610/98 que protegem o direito autoral de programas de computador. Não obstante, existem projetos de leis em tramitação no Legislativo Nacional, como é o caso do Projeto de Lei da Câmara (PLC) 89/2003 [Neto 2009].

Há cerca de onze anos, tramitam três Projetos de Lei no Congresso Nacional — dois do Senado e um da Câmara (PLS 76/2000, PLS 137/2000, e PLC 89/2003) — todos voltados para a definição brasileira de crimes cibernéticos. Sendo que, em 2005, foram todos reunidos pelo Senador Eduardo Azeredo para tramitação conjunta. O projeto já foi discutido e aprovado na Câmara dos Deputados e no Senado Federal, voltando ao Congresso para sua última fase de avaliação. Caso os deputados votem a favor, apenas a presidenta Dilma Rousseff terá poder de vetá-lo [Brasil 2008, Cunha 2011].

Resumidamente, esse projeto de lei vem tipificar, expressamente, os crimes praticados através da Internet, como a difusão de vírus, o acesso indevido a sistemas informatizados e o furto de senhas, a divulgação de dados pessoais e de informações privadas presentes em banco de dados, o atentado contra segurança de serviço de utilidade pública e a falsificação de cartão de crédito ou de débito.

A principal crítica dos opositores ao projeto é que a medida irá provocar a burocratização do acesso e a perda de privacidade dos usuários, devido ao fato da identificação dos usuários na Internet ser obrigado por lei, ficando os provedores responsáveis pelo cadastro, além de manter os dados armazenados por três anos. Entretanto, o conteúdo do projeto busca seguir as definições estabelecidas pela Convenção de Budapeste, estando, nesse sentido, em harmonia com a mesma [Neto 2009, Goyanes 2007].

5. Considerações Finais

As novas tecnologias de informação e, de maneira especial, a Internet, instigaram o processo de globalização, tornando os equipamentos informáticos indispensáveis no dia-a-dia. A facilidade de acesso a todo tipo de conteúdo, que pode ser manipulado de maneira simples, faz com que o número de usuários que acessam a Internet continue crescendo, pois até mesmo pessoas com poucos conhecimentos na área de informática usufruem dos benefícios oferecidos.

Entretanto, com o crescimento de usuários, cresce também as oportunidades para práticas de condutas igualmente lesivas, mas ainda não consideradas crimes passíveis de punição, por dependerem de regulamentação específica (como é o caso do dano praticado contra informações e programas contidos em computador), que proliferam em ritmo acelerado, e por vezes incontrolável.

É preciso, portanto, a adoção de parâmetros legais que combatam eficazmente as infrações supracitadas para que as investigações sejam mais criteriosas e resultem em um procedimento penal correspondente. Contudo, cabe ressaltar que o Poder Legislativo, na

[7] http://www.cert.br/

medida do possível, vem tomando medidas, almejando ser implacável na imposição de sanção diante da realização de crimes praticados na Internet, como é o caso do projeto 89/2003. No entanto, a concretização dessas ações caminha a passos lentos.

Enfim, somente a elaboração de leis, decretos e manuais de conduta não trarão grandes resultados no combate aos crimes de informática. O aperfeiçoamento dos meios de investigação, o progresso técnico dos profissionais ligados à área da persecução penal, a melhor formação e treinamento dos auxiliares da Justiça e a conscientização dos internautas e usuários constituem elementos essenciais a coibir práticas desonestas no mundo virtual.

Referências

Almeida, J. M. F. (2005). Breve história da internet. Disponível em: <http://repositorium.sdum.uminho.pt/handle/1822/3396>. Acesso em: 14 ago. 2011.

Andrade, W. A. (2006). *Crimes na Internet: uma realidade na sociedade de informação*. Graduação, Faculdade de Direito de Presidente Prudente, Presidente Prudente, SP.

Aquotti, M. and Takushi, T. (2010). Crimes virtuais. *ETIC - Encontro de Inciação Científica*, 5(5). ISSN 21-76-8498.

Archick, K. (2002). Cybercrime: The council of europe convention. In *CRS Report for Congress RS21208*, Washington, DC: Congressional Research Service.

BRASIL (2007). *Crimes cibernéticos: manual prático de investigação*. São Paulo: Comitê Gestor da Internet no Brasil, 2th edition. ISSN 8560062041.

Brasil, S. (2008). Pl sobre crimes cibernéticos. Disponível em: <http://www.safernet.org.br/site/institucional/projetos/obsleg/pl-azeredo>. Acesso em: 15 ago. 2011.

Bueno, J. N. and Coelho, V. M. B. G. (2008). Crimes na internet. *JUS-FADIVA*. ISSN 2176-2686.

Castells, M. (2003). *A Galáxia Internet: Reflexões sobre Internet, Negócios e Sociedade*. Jorge Zahar, Rio de Janeiro, RJ. ISBN 8-571-10740-8.

Conte, C. P. and Santos, C. A. d. A. C. (2008). Desafios do direito penal no mundo globalizado: a aplicação da lei penal no espaço e os crimes informáticos. *Revista de Direito de Informática e Telecomunicações*, 3(4).

Couri, G. F. (2009). Crimes pela internet. Disponível em: <http://tinyurl.com/6khbmqx>. Acesso em: 12 ago. 2011.

Cunha, A. R. (2011). "lei azeredo" só pode ser vetada pela presidenta. Disponível em: <http://www.direitoacomunicacao.org.br/content.php?option=com_content&task=view&id=8064>. Acesso em: 16 ago. 2011.

da Sivla, S. R. R. (2009). *Crimes Cibernéticos e a Investigação Policial*. Especialização, Academia de Polícia Civil do Distrito Federal Faculdades Fortium, Brasília, DF.

Gouveia, F. (2007). Tecnologia a serviço do crime. *Ciência e Cultura*, 59:6 – 7. ISSN 0009-6725.

Goyanes, M. (2007). Cibercrimes e as leis no ambiente virtual. *Custo Brasil - Soluções para o Desenvolvimento*, (7):64–69.

Henning, P. C. (1993). Internet @rnp.br: um novo recurso de acesso à informação. *Ciência da Informação*, 22(1):116–124.

Neto, J. P. M. (2009). *Crimes de Internet*. Especialização, Academia de Polícia Civil do Distrito Federal Faculdades Fortium, Brasília, DF.

Neto, M. F. and Guimarães, J. A. C. (2003). Crimes na internet: elementos para uma reflexão sobre a ética informacional. *Revista CEJ*, 7(20). ISSN 2179-9857.

of Europe, C. (2001). Convenção sobre o cibercrime. Disponível em: <http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf>. Acesso em: 14 ago. 2011.

Pinheiro, E. P. (2006). *Crimes Virtuais: Uma análise da criminalidade informática e da resposta estatal*. Graduação, Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), Porto alegre, RS.

Queiroz, A. E., Inácio, A. D., Costa, D., Santos, D. B. d., and Inacio, O. J. a. (2008). A internet como novo âmbito de perpetração de crimes. pages 116–124, Paraná. Congresso Internacional de Direito "Direito Virtual", UDC. ISSN 1983-7453.

Redivo, R. and Monteiro, G. (2009). O direito frente à era da informática. *ETIC - Encontro de Inciação Científica*, 3(3). ISSN 21-76-8498.

Solagna, F. and Souza, R. H. V. (2011). Entre utopias e heterotopias da rede: a regulação dos fluxos de informaçãocomo agenda global. Curitiba, PR. Reunião de Antropologia do Mercosul, UFPR.

Souza, G. L. M. and Pereira, D. V. (2009). A convenção de budapeste e as leis brasileiras. Paraíba. Seminário Cibercrime e Cooperação Penal Internacional, UFPB.

Susana, S. and Leite, K. (2010). Sanção e coação: uma perspectiva para os crimes de internet. *Anuário da Produção de Iniciação Científica Discente*, 10(11). ISSN 2178-6879.

Vieira, E. (2003). *Os Bastidores da Internet no Brasil*. Manole, Barueri, SP, 1th edition. ISBN 8-520-41708-6.