Novo cenário dos crimes cibernéticos no Brasil e as leis que gerem esse mercado

Bruno Nascimento Verçosa[1]

[1]Departamento de Ciência da Computação – Universidade Federal de Goiás(UFG)
CEP: 75704-020 – Catalão –GO – Brasil

bruno.nv@hotmail.com

Abstract. *This article describes how crimes that were previously exercised only physically, in person or more concretely, are now taking over computers and other new technologies. Anyone who is in direct or indirect contact with computers, may suffer damage caused by these crimes. In addition, it intends to highlight how the current Brazilian legislation tries to prevent this type of event and how these laws need to evolve to contain a greater number of cybercriminals.*

Resumo. *O presente artigo descreve crimes que antes eram exercidos apenas fisicamente, presencialmente ou de forma mais concreta, que hoje estão tomando conta de computadores e outras novas tecnologias. Qualquer pessoa que esteja em contato direto ou indireto com computadores, pode vir a sofrer com os danos causados por esses crimes. O artigo apresenta ainda o estado atual das leis no Brasil para barrarem esse tipo de manifestação e o quanto essas leis precisariam evoluir afim de reduzir ao máximo , o número de cibercriminosos. Utilizando-se de leituras de outros artigos e sites sobre o assunto.*

1. Introdução

Nenhum nicho de Mercado se desenvolveu tanto e tão rápido quanto o da tecnologia, em especial o da computação. Com tal evolução, surge o crescimento dos crimes praticados por meio de computadores e da internet, ou cibercrimes.

A grande questão sobre essa verdadeira invasão dos computadores na vida das pessoas e empresas é saber os reflexos dessa tecnologia no mundo jurídico.

As brechas no código penal, no que se diz respeito a crimes cibernéticos, põe os "crackers" e demais criminosos do ramo mais à vontade para a prática das mais perniciosas, custosas e danosas ações eletrônicas.

Quando se consegue identificar a origem ou autoria desses crimes, surgem não mais que uma inglória tentativa de penalização por vias análogas de clássicos e antigos crimes.

2. Os crimes cibernéticos

Na internet podemos pagar contas, trocar mensagens, participar de salas de bate-papo, "baixar" arquivos de música, imagem ou texto, comprar produtos, solicitar serviços, acessar sites com informações das mais diversas. Em todas essas atividades há o risco de encontrar alguém que se aproveita da velocidade e da escala em que as trocas de informações ocorrem na rede para cometer crimes.

De acordo com a "Convenção sobre a Cibercriminalidade" transcrita no manual de investigação de crimes cibernéticos do ministério público constante nas referencias abaixo citadas, adotada pelo Conselho da Europa em 2001, podemos 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;
    - 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
    - Falsificação de dados;
    - Estelionatos eletrônicos;
- Infrações relativas ao conteúdo
    - Pornografia infantil (produção, oferta, procura, transmissão e posse de fotografias ou imagens realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito);
    - Racismo e xenofobia (difusão de imagens, idéias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica; injúria e ameaça qualificada pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade);
- Atentado à propriedade intelectual e aos direitos que lhe são conexos. [4]

3. Classificação dos crimes de informática

Os crimes da informática podem ser próprios ou impróprios. Os primeiros são aqueles que só podem ser praticados através da informática, sem ela é impossível a execução e consumação da infração. São tipos novos, que agridem a informática como bem juridicamente protegida. Daí porque em virtude da pouca legislação existente, alguns fatos são atípicos e portanto não podem ser punidos.[5]
Por exemplo, a violação do e-mail, pirataria de software, pichação de homepages, dano em arquivos provocado pelo envio de vírus e etc.
Os crimes de informática impróprios são os que podem ser praticados de qualquer forma, inclusive através da mesma. Assim, para que o individuo cometa o crime, utiliza-se do computador, o qual é um meio, um instrumento para a execução do crime. São delitos que violam bens já protegidos por nossa legislação, como patrimônio e honra. Como por exemplo: ameaça , estelionato, calúnia e pedofilia. Portanto recorre-se a legislação vigente. [6]

4. O projeto de lei do Brasil

O Código Penal brasileiro não possui leis especificas que combatam com exatidão os novos crimes no ramo cibernético.Com essa lacuna vários deles não conseguem ser julgados assim como os antigos cometidos por outros meios.

Um exercício, portanto, de adaptação analógica terá de ser feito para a interpretação criminal do fato, sendo que, em razão do princípio (constitucional) da inocência, "in dubio pro reo", será sempre em favor do infrator a interpretação de dúvidas e lacunas da legislação. Assim, não havendo estrita conformação da conduta eletrônica ao crime, mesmo quando certa e indiscutível do ponto de vista tecnológico, impor-se-á a absolvição. [1]

Portanto, a tarefa mais urgente é adequar antigos "crimes"aos atuais "crimes da rede", tarefa essa que não é fácil já que tal medida precisa estar sob o olhar do princípio constitucional, da legalidade, estrita tipicidade da conduta, para que haja a regulamentação de tais crimes (princípio do "nullum crimen, nulla poena, sine lege").

Há uma tendência em todo o mundo moderno, de regramento dos tipos tecnológicos, que caminha para um antagônico sentido, que é o da limitação mais "aberta" dos elementos que os caracterizem na lei, pois com a velocidade da inovação tecnológica não se pode perder a essência deste, com a evolução das alterações na estrutura. O que nos leva a pergunta: Como podemos conciliar na lei penal brasileira a correta definição de novos crimes informáticos?

Já tramita, há quase sete anos, no Congresso Nacional, três projetos de lei, dois são provenientes do Senado e um da Câmara (PLS 76/2000, PLS 137/2000, e PLC 89/2003), estes voltados para a definição brasileira de crimes cibernéticos.

Em 2005, foram todos reunidos no Senado Federal, para uma tramitação conjunta, vindo a tornar-se relator dos mesmos o Senador Eduardo Azeredo. Em seu relatório, o referido Senador apresentou na Comissão de Educação, Substitutivo que aglutina os três projetos.

- **Apresentação:** O Substitutivo apresentado pelo Senador Eduardo Azeredo aglutinou três projetos de lei que já tramitavam no Senado, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.[2]

- **Ementa:** Altera o Decreto-Lei nº 2848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 9.296, de 24 de julho de 1996, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), a Lei nº 10.446, de 8 de maio de 2002, e a Lei nº 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 dá outras providências.[2]

Como pontos principais do Substitutivo (aos referidos projetos de lei) apresentado pelo Senador Eduardo Azevedo+, podemos destacar:

- A inserção no código penal brasileiro, das seguintes modalidades de novos crimes:
    - A modalidade de crime de dado: o "Dano por difusão de código malicioso eletrônico ou similar";
    - Violação da Rede de computadores, dispositivo de Comunicação ou sistema informatizado.
    - A divulgação maliciosa do código.
    - Violão de banco de dados ou a divulgação não devida de informações depositadas no mesmo.
- Definição, no Código Penal, dos elementos – das circunstâncias elementares – que constituam "*Dispositivo de comunicação, sistema informatizado, rede de computadores, defesa digital*" – o que afasta as até agora costumeiras incertezas interpretativas do fato, pela expressa previsão da hipótese fática.[1]
- A obrigação de conservação de dados eletrônicos do usuário de sistemas de telecomunicações, com penalização pecuniária, o que se adéqua à exigência da Convenção Européia de Cybercrimes.

Além disso, no art 109, V e parágrafo 5º, estabelece a competência da Justiça Federal para a apreciação de crimes previstos em tratados ou em convenções internacionais, mesmo que o início desse crime tenha sido fora do país e aqui apenas consumados, ou o inverso.

5. Conclusão

Muitos países já possuem leis sobre esta matéria, enquanto que no Brasil ainda se apresenta um quadro muito aquém do que seria necessário para a incriminação de usuários maliciosos que utilizam a internet para prejudicar ou tirar proveito de terceiros.

O crime na internet e a impunidade tornaram-se um círculo vicioso que sob o ponto de vista tecnológico parece não ter limites.

Carl Segan em seu livro "O mundo Assombrado pelas Demônios" faz a seguinte citação:

"Nós criamos uma civilização global em que elementos cruciais - como as comunicações, o comércio, a educação e até a instituição democrática do voto - dependem profundamente da ciência e da tecnologia. Também criamos uma ordem em que quase ninguém compreende a ciência e a tecnologia. É uma receita para o desastre. Podemos escapar ilesos por algum tempo, porém, mais cedo ou mais tarde, essa mistura inflamável de ignorância e poder vai explodir na nossa cara."

Apesar de já haver projetos de lei tramitando tanto no Congresso Nacional quanto na Câmera, o Brasil ainda é bem carente no que se diz respeito ao combate e penalização de crimes informáticos. Toda a lei brasileira precisa mudar tão ou mais rápido quanto a tecnologia tem mudado, para que possa inibir e punir pessoas que se utilizam de computadores e afins com objetivo de cometerem delitos.

Referências

[1] Alice Ramos - Crimes e Cybercrimes – Parte IV - http://www.aliceramos.com/view.asp?materia=1222, acesso em 28/10/2010

[2] PL sobre Crimes Cibernéticos | Safernet Brasil - http://www.safernet.org.br/site/institucional/projetos/obsleg/pl-azeredo, acesso em 27/10/2010

[3] Secretaria Geral da Mesa –Senado Federal - Atividade Legislativa – Projetos e Matérias - http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=63967, acesso em 27/10/2010

[4] Adriana Shimabukuro Kurokawa - Crimes Cibernéticos – Manual de investigação – Ministério Público Federal, Procuradoria da República no Estado de SP, acesso em 02/10/2010

[5] ARAÚJO DE CASTRO, Carla Rodrigues – Crimes de Informática e seus Aspectos Processuais, 2ª edição;

[6] MORAES, Alexandre. Direitos fundamentais. 1ª ed., São Paulo, 1998.