**CRIMES VIRTUAIS E DIREITO PENAL: A NECESSIDADE DE UMA POLÍTICA INTERNACIONAL DE COMBATE AO CRIME[[1]](#footnote-1)**

Renato Gonçalves de Sá[[2]](#footnote-2)

Victor Paiva Gomes Marques do Rosário[[3]](#footnote-3)

RESUMO

Crimes cibernéticos são aqueles crimes praticados em ambiente virtual, isto é, com a utilização da internet ou de outras redes de dados. No sistema jurídico brasileiro, eles são enquadrados de forma análoga nos tipos do Código Penal ou de outras leis especiais, sendo assim, importante a criação de uma lei específica para os crimes virtuais, e mais importante ainda a criação de uma política internacional de combate a esse tipo de delito.

Palavras chave: Crimes virtuais, legislação, política internacional

**1 INTRODUÇÃO**

Com o desenvolvimento das tecnologias da informação, e em especial com o advento da internet, a sociedade foi obrigada a enfrentar o surgimento de novos conceitos, novas atividades econômicas, novas formas mais fáceis, rápidas e amplas de comunicação, e, por conseguinte, também brotaram novas práticas criminosas que antes seriam muito difíceis, quando não impossíveis, de serem cometidas.

Como o Direito é uma expressão humana que se transforma de acordo com as exigências sociais da época em que está inserido, faz-se necessária uma evolução imediata das leis que regem o âmbito da informática no que diz respeito às práticas criminosas, que por sua própria natureza possuem peculiaridades distintas daquelas praticadas na realidade comum.

**2 CRIMES DE INFORMÁTICA**

Os crimes virtuais, ou de informática, ou cibernéticos são aqueles praticados através de um ambiente virtual, como a internet. Segundo Ramalho terceiro:

“os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas.” (TERCEIRO, 2002)

Podemos dizer então, que crime de informática é toda conduta:

“típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade.” (ROSSINI, p.110, 2004)

**2.1 Classificações:**

Uma das principais classificações nos crimes de internet é a que os divide em próprios e impróprios. Os próprios são aqueles que só podem ser praticados através dos computadores ou sistemas de informáticas, não havendo como praticá-los de outra forma. Já os impróprios são aqueles crimes de informática que também poderiam ser praticados sem o uso dessas tecnologias. (AQUOTTI, p. 4, 2009)

Outra divisão, diz respeito ao objetivo do crime. São chamados de crimes de informática puros aqueles onde o crime é exercido com a finalidade de atingir um computador, ou um sistema de informática, os dados e informações por ele ordenados. São chamados mistos os crimes de informática onde o computador e os sistemas de informática não são o objetivo final, mas constituem meios indispensáveis para a obtenção do resultado. Por fim, são chamados crimes de informática comuns aqueles onde o computador é utilizado para obter aquele resultado, mas que poderia ser feito também por outro meio. (Ibid.)

**2.2 Exemplos:**

São vários os crimes que podem ser praticados com o uso de um computador com acesso à internet, entretanto é difícil sua tipificação, pois o ordenamento jurídico brasileiro ainda é insuficiente para regulamentar os crimes virtuais de forma específica. Nesse caso, na grande maioria das situações, serão utilizados os tipos do Código Penal ou de outras legislações da forma em que se encaixar melhor cada conduta.

Dentro dos crimes contra a honra, é comum que muitos usuários da rede utilizem do seu relativo anonimato para atentar contra a dignidade da vítima, através de calúnia, difamação ou injúria, na esperança de que serão mais dificilmente identificados por estarem em um ambiente menos vigiado. Além da dificuldade na investigação dos autores no meio virtual, ainda há o agravante de que os usuários mais experientes, ou *hackers,* geralmente utilizam-se de provedores hospedados em territórios estrangeiros onde a legislação permite qualquer tipo de expressão de opinião e se torna impossível retirar a mensagem postada.

Vale ressaltar, que por ser a internet um meio de comunicação de grande alcance, especialmente nos dias atuais, aplicar-se-á nesses crimes o aumento de pena descrito no artigo 141, inciso III: “As penas cominadas neste Capítulo aumentam-se de um terço, se qualquer dos crimes é cometido: [...] III - na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria”.

Também são frequentes os crimes contra a liberdade individual, como a ameaça, inviolabilidade de correspondência e divulgação de segredos. A inviolabilidade de correspondência, por exemplo, pode ser aplicada ao ambiente virtual se considerarmos o *e-mail* como o correspondente eletrônico à carta tradicional. Isso é ainda mais evidente quando lemos o parágrafo primeiro do artigo 151, que tutela a comunicação telegráfica ou radioelétrica, e a conversação telefônica, dos quais a internet nada mais é do que uma evolução em termos tecnológicos. Sendo assim, configura-se crime a violação de *e-mails*, dentro do artigo 151, parágrafo parágrafo primeiro, em proteção à garantia constitucional da inviolabilidade de correspondência. (5º, XII) Igualmente, também podem ser praticados em ambiente virtual os crimes contra a inviolabilidade de segredos (153 a 154).

Os crimes contra o patrimônio: furto, extorsão, dano e estelionato, também podem ser praticados através da internet. O furto, por exemplo, é cometido através da manipulação de dados referentes a contas bancárias, que os permite executar saques, depósitos, obter senhas de outros usuários, tudo de forma a obter vantagem financeira indevidamente. Quanto ao crime de dano, ele pode ser praticado à longa distância através da disseminação de vírus de computador e outras pragas, capazes de danificar e até inutilizar o hardware e o software de várias máquinas de uma só vez. O estelionato, por sua vez, só pode ser praticado com a presença de uma relação psicológica entre autor e vítima de modo que o primeiro venha a iludi-la a praticar ato prejudicial a si que confira ao criminoso ou a terceiro alguma vantagem ilícita. Os meios ardilosos comumente utilizados por quem pratica esse crime são a construção de sites falsos, similares aos originais, capazes de enganar quem os acessa, a disseminação de cavalos de Tróia eletrônicos, utilização de perfis falsos em redes sociais, etc.

Igualmente frequentes na rede são os crimes contra os costumes: favorecimento à prostituição (228), escrito ou objeto obsceno (234), e pedofilia (241 do Estatuto da Criança e do Adolescente). Dentre esses, destaca-se a pedofilia, que se torna cada vez mais motivo de preocupação das autoridades devido ao alarmante número de casos encontrados. Entretanto, como já explicamos anteriormente, muitos casos são difíceis de resolver por que os criminosos utilizam-se de artimanhas para burlar a investigação policial, como a utilização de provedores de internet hospedados em território estrangeiro:

“Necessitamos de um trabalho investigativo rigoroso, que exige uma estrutura grande, com policiais treinados e com conhecimento em informática, computadores de última geração para fazer o rastreamento e localização de forma rápida e tudo isso requer pessoal treinado, tempo e necessita de recursos, mas somos sabedores dos problemas financeiros que nosso país enfrenta, o que torna mais difícil e, principalmente, relevante o trabalho feito pelas autoridades brasileiras. E vale ressaltar aqui, que apesar de todas as dificuldades encontradas, já temos, em todo o Brasil, muitos inquéritos instaurados contra os acusados de pedofilia na Internet. Hoje, há uma conscientização e preocupação muito grande com este problema e órgãos como o Ministério Público Federal e Estadual, a Polícia Civil, Polícia Federal, ABMP, RECRIA, CECRIA, CEDECA, ABRAPIA, UNESCO e muitas outras instituições e entidades estão firmando acordos para combater esses absurdos praticados por esses delinqüentes na WEB” (NOGUEIRA, p.6, 2005)

O ordenamento jurídico brasileiro possui algumas leis penais de natureza informática, que versam sobre ramos específicos do direito, como por exemplo, a lei 8.137/90. Esta lei trata sobre crimes contra a ordem tributária, que considera crime quem divulga ou utiliza programa de processamento de dados que altere o valor contábil que o passivo da tributação receba. É um exemplo de lei penal que tipifica sobre ação informática, visto que o processamento de dados é alterado, ilicitamente, por um programa específico.

Outro exemplo é a lei de nº. 9296/96, que tipifica como crime a conduta de interceptação telefônica, informática, telemática ou quebrar segredo de justiça sem autorização da mesma. Ou seja, é crime a conduta de interceptar informações no espaço cibernético, como, por exemplo, e-mails, sem autorização legal.

**3. Necessidade de política internacional**

Embora no nosso país exista uma preocupação dos legisladores na criação de leis específicas para o ambiente virtual, antes de tudo, é também igualmente necessária a criação de uma política internacional, que incentive o trabalho em conjunto da polícia entre os países nos crimes cibernéticos, permitindo que não passe impune aquele criminoso que utiliza provedores em terras estrangeiras, dando também ao corpo policial todo o preparo e treinamento que precisam para lidar com esse tipo de delito, e a aquisição de equipamentos capazes de rastrear os infratores de maneira mais precisa.

Essa necessidade baseia-se no problema da jurisdição do ciberespaço, que diferentemente do físico, existem situações onde fica difícil saber como aplicar a lei e de qual país aplicar, já que não existem fronteiras físicas delimitadas. Essa peculiaridade é aproveitada de todas as formas pelos agentes do crime, que, com o apoio da tecnologia conseguem passar despercebidos pela investigação policial de um país ao utilizar o ambiente cibernético sob poder jurisdicional de outra nação. A única forma de combater essa facilidade

**4. Conclusão**

Os crimes cibernéticos dentro do sistema jurídico brasileiro são enquadrados normalmente dentro dos tipos existentes no Código Penal ou em algumas leis específicas de forma análoga, isto é, não há uma legislação única que trate especificamente sobre os crimes de informática por si só, o que traz a preocupação do legislativo em criar projetos de lei para suprir essa lacuna.

Entretanto, o maior problema no combate aos crimes cibernéticos, ao invés de ser a falta de legislação específica, é na verdade a natureza imaterial e sem fronteiras do ambiente onde são praticados. Levando isso em consideração, a única forma de combater essa fragilidade típica da investigação sobre os crimes virtuais seria o trabalho em conjunto das polícias dos diversos países, através da assinatura de tratados que permitam o controle cooperacional entre as nações no combate a esses crimes, principalmente no que diz respeito à pedofilia, onde é mais frequente ainda a utilização de servidores estrangeiros para estocar pornografia infantil.

**REFERÊNCIAS**

AQUOTTI, Marcus Vinícius e TAKUSHI, Tiago Tadashi, **Crimes Virtuais**, disponível em:<http://intertemas.unitoledo.br/revista/index.php/ETIC/article/viewFile/2560/2190>, 2009. Acesso em 30 de Outubro de 2011.

NOGUEIRA, Sandro D’Amato. Pedofilia **e Tráfico de Menores Pela Internet: O Lado Negro da Web**, Disponível em: <http://www.ambito-juridico.com.br/aj/eca0010.htm>, 2001. Acesso em: 30 de outubro de 2011.

PINHEIRO, Emeline Piva. **Crimes virtuais: uma análise da criminalidade informática e da resposta estatal.** Disponível em: <http://www.buscalegis.ufsc.br/arquivos/Vi-%203.03.pdf>. Acesso em: 31 de outubro de 2011.

**TERCEIRO, Cecílio da Fonseca Vieira Ramalho. O problema na tipificação penal dos crimes virtuais. Jus Navigandi, Teresina, ano 7, n. 58, 1 ago. 2002. Disponível em:** <http://jus.com.br/revista/texto/3186>**. Acesso em:** 30 out. 2011**.**

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

1. Paper apresentado à disciplina de Direito Penal, da Unidade de Ensino Superior Dom Bosco - UNDB. [↑](#footnote-ref-1)
2. Acadêmico do 6º Período do curso de Direito da UNDB. Email: renatogsah@hotmail.com [↑](#footnote-ref-2)
3. Acadêmico do 6º Período do curso de Direito da UNDB. Email: victor\_paiva@hotmail.com [↑](#footnote-ref-3)