ETIC 2015 - Encontro de Iniciação Científica
ISSN 21-76-8498

CIBERCRIME

Isadora Cavalli de Aguiar FILGUEIRAS[1]
Thaís Soldera de LIMA[2]

RESUMO: Este trabalho tem como objetivo entender como surgiu e se desenvolveu os crimes praticados com um elemento especial, a internet. Este meio tecnológico tão novo preocupa a muitas pessoas e ao Estado, que esta tendo que se modernizar e investir em capacitação para os agentes responsáveis pela persecução penal. A internet surgiu com a finalidade socioeducativa e se desenvolveu de tal forma, que hoje grande parte da população tem acesso a essa tecnologia, e em razão disso é necessário um olhar crítico sobre esse assunto.

Palavras-chave: Cibercriminalidade. Crimes. Internet. Investigação. Competência.

1 INTRODUÇÃO

O presente artigo tem como finalidade analisar a cibercriminalidade, que, por ser um ilícito atual está gerando uma maior preocupação. Com a globalização, os meios tecnológicos cresceram e se espalharam, hoje muito da população tem acesso à rede, computadores, celulares, tablets e aparelhos, que se usados corretamente, servem para facilitar a vida das pessoas, porém, se usados de maneira ilícita, podem causar mau a muita gente.

Por ser um tema novo, as pessoas ainda não sabem como se portar quando deparadas com esses crimes, haja vista que ainda perpetua um receio em relação à apuração do cibercrime e o rastreio dos delinquentes que utilizam da internet um meio de produzir um ilícito penal.

A revolução digital permitiu que muitas pessoas pudessem ter acesso a internet, e este acesso em massa deu aos delinquentes um meio a mais para gerar golpes e crimes, tendo em vista que a investigação ainda é precária.

[1] Discente do 3º ano do curso de Direito do Centro Universitário "Antônio Eufrásio de Toledo" de Presidente Prudente. Isinha_cavalli@hotmail.com
[2] Discente do 3° ano do curso de Direito do Centro Universitário "Antônio Eufrásio de Toledo" de Presidente Prudente. Tatasl_09@hotmail.com

2 GLOBALIZAÇÃO

O fenômeno da globalização começou no século XV com as grandes navegações, na época não se imaginava que atingiria tais proporções, porém desde aquela época a intenção de Portugal e Espanha era crescer com o comércio marítimo e assim levar produções de um lugar ao outro.

A globalização é a interação dos países, que tem o objetivo de fazer com que os extremos do planeta se comuniquem, transformando o mundo em um lugar sem fronteiras, ou seja, corresponde à informação, comunicação, fluxo de pessoas, fluxo de mercadorias, fluxo de capitais, e, hoje em dia, o meio mais fácil é a internet.

A internet surgiu no ano de 1969 no auge da Guerra Fria, era usada apenas por militares e cientistas, mas com o passar do tempo foi liberado seu uso de maneira comercial, e se disseminou de tal forma e velocidade que hoje infinidades de coisas podem ser feitas através da internet, em qualquer lugar e hora do dia.

Uma pesquisa feita pela União Internacional das Telecomunicações, UIT, mostrou que no ano 2000 cerca de 6,5% da população mundial tinha acesso a internet, e no ano de 2015 esse número passou para 43%, que corresponde a cerca de 3,2 bilhões de pessoas conectadas a internet. Quando se compara com pessoas que ainda não tem nenhum contato com a internet esse número não é tão grande, sendo cerca de 4 bilhões de pessoas sem o acesso à internet.

A internet esta presente em vários meios eletrônicos, tudo com a finalidade de facilitar a vida do ser humano. Com a internet fica fácil fazer novas amizades, trocar experiências, divulgar trabalhos, fazer pesquisas rápidas, e milhares de outras funções construtivas e responsáveis, porém cabe aos internautas saberem o que postar e em quais sites entrar.

3 CRIMES CIBERNÉTICOS

Ter acesso à internet, hoje, é uma facilidade para muitas pessoas. Diversos aparelhos eletroeletrônicos funcionam a base da rede, e quem não os tem,

pode frequentar lugares próprios, como os *cyber* cafés, as *LAN houses,* que são estabelecimentos comerciais próprios para as pessoas que queiram pagar para, em um tempo determinado, ter acesso a um computador e a uma rede.

Estando ao alcance de várias pessoas, a rede – que inicialmente era para ser usada pelos militares e que após a Coexistência Pacífica com as duas maiores potências mundiais, EUA e URSS em acordo, foi passada às universidades – era para ser usada com fim educativo, contudo não é mais a única finalidade.

Hoje, a internet atingiu grandes proporções podendo ser usada para o bem, e mero deleito das pessoas, ou por mentes ruins, usado para atingir os cidadãos de forma ilícita, e então o que ninguém antes pensava, hoje é algo que preocupa, e muito, o Estado.

O cibercrime é uma pratica que consiste em burlar a segurança de computadores ou de redes empresariais. É o crime feito via internet, e pode assumir várias formas, podendo ocorrer a qualquer hora e lugar. Os criminosos que usam da informática desenvolveram uma grande habilidade, e, portanto, conseguem a todo instante mudar a tática de como obterem o esperado.

A cibercriminalidade engloba um grande arsenal de atividades ilícitas, como a falsificação, a fraude, o acesso não autorizado, a violação da propriedade intelectual, distribuição de material pornográfico, entre outros.

Independentemente de ainda não possuir legislação específica no Brasil, é possível que seja tipificado alguns delitos no código penal vigente.

Sérgio Marcos Roque diz que o cibercrime é “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material.”

3.1 DIVISÕES DO CIBERCRIME

Há uma divisão do cibercrime em próprio, impróprio, comum, puro e misto:

O próprio ocorre quando o sistema informático é usado para lesar a vítima, por exemplo, alteração de dados, roubo de identidade virtual, interceptação informática e invasão de dispositivos. Atinge diretamente o hardware ou o software do computador, sendo praticado unicamente por este.

Os impróprios são aqueles que fazem do sistema um meio de execução para atingir um determinado bem jurídico, por exemplo, fraudes com cartão de crédito, crimes contra a honra, pedofilia. Ofende à "realidade", ou seja, fora do meio informático. O STJ diz:

> "(...) 3. No presente caso, há hipótese de atração da competência da Justiça Federal, uma vez que o fato de haver um usuário do Orkut, supostamente praticando delitos de divulgação de imagens pornográficas de crianças e adolescentes, configura uma das situações previstas pelo art. 109 da Constituição Federal.
> 4. Além do mais, é importante ressaltar que a divulgação de imagens pornográficas, envolvendo crianças e adolescentes por meio do Orkut, provavelmente não se restringiu a uma comunicação eletrônica entre pessoas residentes no Brasil, uma vez que qualquer pessoa, em qualquer lugar do mundo, desde que conectada à internet e pertencente ao dito sítio de relacionamento, poderá acessar a página publicada com tais conteúdos pedófilos-pornográficos, verificando-se, portanto, cumprido o requisito da transnacionalidade exigido para atrair a competência da Justiça Federal. (...)"
> (CC 111.338/TO, Rel. Ministro Og Fernandes, Sexta Turma, julgado em 23/06/2010)

Comuns são aqueles em que usam da internet para realizar um crime já descrito no código penal, por exemplo, a calúnia, um crime tipificado pelo código penal que passou a ser cometido também através da rede.

O puro tem por único objetivo atingir o sistema informático, ou seja, através do computador trazer algum dano a vitima, é o caso do vírus Melissa que causou uma despesa de U$ 80.000.000,00 em 1999.

Por fim, o misto é aquele em que utiliza-se do meio informático para causar danos porém, seu objetivo é diverso do informático. Por exemplo, usa-se do home-banking para fazer transferências não autorizadas, lesando desta forma a vítima, mas a invasão do home-banking não é o objetivo principal, sendo o objetivo o furto.

4 FRENTE À LEGISLAÇÃO

No Brasil os meios investigativos ainda são muito precários, falta equipamentos, pessoas devidamente capacitadas para tal cargo, e, desta forma, o crime digital acaba se alastrando com certa velocidade.

O Estado já esta começando a investir em cursos de capacitação para os agentes responsáveis pela persecução penal, e hoje existem diversos departamentos especializados neste assunto. No estado de São Paulo tem a DIG-DEIC, que tem capacitação para investigar crimes praticados por meios eletrônicos, no Rio de Janeiro, tem a DRCI (Delegacia de Repressão aos Crimes de Informática), nos estados do Espírito Santo, Minas Gerais, Paraná, Rio Grande do Sul, Distrito Federal, Goiás, Pará, Mato Grosso- Cuiabá, Sergipe- Aracaju, também possuem estabelecimentos especializados, aonde eventuais vítimas encontram orientações detalhadas de como proceder diante de um crime virtual.

Existem algumas legislações que tipificam condutas ilícitas realizadas por meio da rede, como por exemplo, a Lei n°9.296, de 24 de julho de 1996 em seu artigo décimo que fala:

> "Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
>
> Pena: reclusão, de dois a quatro anos, e multa."

A Lei n° 12. 737 de 30 de novembro de 2012, conhecida como Lei Carolina Dieckmann, tem seu cunho calcado na tipificação criminal de delitos informáticos, e em seu artigo 154-A descreve sobre o delito e as penas cominadas:

> "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."

Por regra, a competência para julgar os cibercrimes é da Justiça Comum Estadual, contudo o Manual Prático de Investigação do Ministério Público Federal em São Paulo, prevê que:

> "Nos termos do artigo 109, inciso IV, da Constituição brasileira, compete aos juízes federais processar e julgar os crimes cometidos em detrimento de bens, serviços ou interesses da União, suas entidades autárquicas ou empresas públicas. Assim, é competência da Justiça Federal julgar os crimes eletrônicos praticados contra os entes da Administração Federal indicados nesse inciso. Podemos citar, a título exemplificativo, o estelionato eletrônico, o dano ou a falsificação de dados constantes em sistemas informatizados mantidos por órgão ou entes da administração pública federal."

5 COMO PREVENIR A CIBERCRIMINALIDADE

As sugestões de prevenção dos crimes pela internet são simples, uma vez que muitos dos crimes só acontecem porque são os próprios usuários que, ao clicar em algum *link,* deixam que o vírus entre e se difunda no computador.

É importante que haja programas com software de segurança, com firewall e programas antivírus, esses programas vão fazer uma defesa online e fazer com que não entre conteúdos indesejados pela internet.

É preciso que haja mais cautela por parte dos internautas, pois não é seguro dar informações pessoais via internet, podendo vir a gerar danos decorrentes das informações prestadas. A verificação constante de extratos bancários tem a

função de analisar se por alguma razão o cartão não foi clonado e usado de maneira errônea.

6 CONCLUSÃO

As práticas ilícitas pela internet são gradativas, uma vez que muitos pensam não ter meios para desvendar tais crimes e, portanto serão delitos feitos no anonimato e que não terão os culpados, punição alguma.

O fenômeno da globalização foi importantíssimo para expandir os meios tecnológicos, e, sobretudo a internet.

Os cibercrimes são os chamados delitos com um elemento especial, a internet, portanto é possível que ocorram lesões a diversos bens jurídicos através da rede. Hoje em dia já existem algumas leis que preveem delitos via internet com cominações de penas respectivas.

Em diversos estados da federação, já estão sendo instalados departamentos especializados em crimes virtuais. Estas delegacias estão a disposição da população que sofrer algum abuso pela internet, e vão ser de vital importância para a investigação desses delitos.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília: Senado, 1988.

CENTRO UNIVERSITÁRIO “ANTONIO EUFRÁSIO DE TOLEDO”. **Normalização de apresentação de monografias e trabalhos de conclusão de curso.** 2007 – Presidente Prudente, 2007, 110p.

Disponível em: http://g1.globo.com/tecnologia/noticia/2015/05/mundo-tem-32-bilhoes-de-pessoas-conectadas-internet-diz-uit.html (Acesso em 15/08/15)

Disponível em: http://br.norton.com/prevention-tips/article (Acesso em 15/08/15)

Disponível em: http://br.norton.com/cybercrime-definition (Acesso em 15/08/15)

Disponível em: http://jus.com.br/artigos/33636/crimes-ciberneticos#ixzz3jNKiVMcG (Acesso em 23/08/15)

MINISTÉRIO PÚBLICO FEDERAL. Crimes Cibernéticos. Manual Prático de Investigação. 2006, p. 41.

Disponível em: http://www.crimespelainternet.com.br/delegacias-de-crimes-digitais/ (Acesso em 23/08/15)

Disponível em: http://www.planalto.gov.br/CCivil_03/LEIS/L9296.htm (Acesso em 23/08/15)

Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm (Acesso em 23/08/15)

MANUAL DE POLÍCIA JUDICIÁRIA: DOUTRINA, MODELOS, LEGISLAÇÃO/ COODERNADOR CARLOS ALBERTO MARCHI DE QUEIROZ.- SÃO PAULO: DELEGACIA GERAL DE POLÍCIA, 6 EDIÇÃO, 2012.

ROQUE, Sérgio Marcos. Criminalidade informática: crimes e criminosos do computador. São Paulo: ADPESP Cultural, 2007. P. 25.