CRIMES CIBERNÉTICOS: ordenamento jurídico frente ao estelionato virtual*

Dion Clésio Pereira da Silva**

Geraldo Miranda Pinto Neto***

RESUMO

Os crimes cibernéticos geram serias questões que vem aumentando gradativamente de forma que o sistema jurídico brasileiro não consiga acompanhar tal crescimento. O grande fator que influencia nessa questão é o barateamento da tecnologia, ou seja, tranou-se acessível para todo cidadão que dela queira usufruir. A internet que em pouco tempo se desenvolve trouxe consigo criminosos virtuais que praticam diversas formas de crimes sem qualquer restrição legislativa eficaz que possa inibir tais ações. E no Brasil, crimes virtuais como estelionato são constantemente cometidos e na maioria dos casos não há leis que possam punir tais meliantes. Restando algumas opções para tentar impedir, que é o uso do Código Penal e a criação de pequenas promotorias especializadas em crimes virtuais, que por sua vez não possui efeito perante as gigantescas modalidades de crimes no ciberespaço.
Palavras-chave: Tecnologia. Cibercrimes. Estelionato.

ABSTRACT

Cybercrime generates serious issues that are gradually increasing so that the Brazilian legal system can not keep pace with such growth. The big factor that influences this issue is the cheapness of technology, or it has become accessible to every citizen who wishes to enjoy it. The internet that in a short time developed brought virtual criminals who practice various forms of de crimes without any effective legislative restriction that could inhibit such actions. And in Brazil, virtual crimes such as stellation are constantly committed and in most cases there are no laws that could punish such misdemeanors. With some options remaining to try to prevent, which is the use of the Penal Code and creation of small prosecution offices specializing in virtual crimes, which in has no effect on the gigantic crime patterns in cyberspace.
Keywords: Technologia. Cybercrimes. Stelionate.

1. INTRODUÇÃO

---

* Trabalho de Conclusão de Curso, apresentado ao Curso de Direito da Faculdade de Jussara/FAJ, como parte obrigatória para obtenção do Grau de Bacharel em Direito.

** Graduando do Curso de Direito da Faculdade de Jussara. E-mail. dionclesio_silva@hotmail.com

*** Professor Orientador da Faculdade de Jussara. Mestre em Direito, Estado e Constituição pela Universidade de Brasília. Correio eletrônico: neto.gmpn@gmail.com. Geraldo Miranda Pinto Neto.

O presente artigo tem o objetivo, demonstrar os crimes mais usuais que são cometidos no universo cibernético, e de que forma os malfeitores se utilizam dela para desenvolver suas ações ilícitas, bem como explicar de que forma o nosso ordenamento jurídico age perante tais crimes.

Com a mutabilidade do comportamento humano no presente contexto histórico, influenciado pela evolução das mídias virtuais, o fato social (crime cibernético) ganhou novos contornos perante a lei, fazendo surgir uma conduta que fosse inserida como crime (fato típico, antijurídico e culpável), como por exemplo, o crime de estelionato virtual, que várias pessoas foram vítimas incluindo a atriz Glória Pires.

Os crimes cibernéticos são uma constante no mundo virtual. É possível verificar a existência de “piratas na net,” ávidos por furtar sua senha de acesso aos provedores de banco, e-mails, empresas, etc. Tendo como objetivo primordial angariar recursos escusos.

Inicialmente, há uma abordagem ao contexto histórico da evolução da *internet,* bem como, os caminhos tomados, desde uso por país que se confrontavam na guerra fria, e avaliando também conceitos como ciberespaço, crime virtual, extraterritorialidade penal brasileira.

Para finalizar, apresentam-se leis específicas para o combate aos crimes cibernéticos, presentes no sistema jurídico brasileiro. Verifica-se a presença de algumas medidas no ordenamento brasileiro, como a criação da Lei n° 12737/12 conhecida como lei Carolina Dieckiman e a Lei n° 12965/14,conhecida como lei do Marco Civil.

Percebe-se que tais institutos normativos realizam alterações no Código Penal com o intuído de atualizar a proteção dos bens jurídicos frente a atualização das mídias sócias.

2. ORIGEM DA INTERNET

A origem da internet aconteceu em 1969, durante a guerra fria, através da Agência de Projetos Avançados (*Arpanet*), pelos Estados Unidos da América (EUA). O país estava preocupado com um possível ataque nuclear por parte da União Soviética, por isso elaborou um sistema de comunicações, que, caso ocorresse o ataque, as comunicações militares governamentais não seriam interrompidas. Ou

seja, era um sistema silencioso e precioso que trazia vantagens aos Estados Unidos da América no contexto da guerra(INELLAS, 2009).

Após terem percebido que o sistema de telecomunicações deixava os Estados Unidos da América em vantagem frente à União Soviética, criaram inúmeras pequenas redes locais que se denominavam*Local Area Network* (LAN) ou rede local. Esse modelo tratava-se de uma configuração para redes de telecomunicação instaladas em pontos menores, como casas e escritórios pequenos.

Dessa maneira, a comunicação era estratégica, pois localizava-seem pontos específicos do país, e era interligada por meio de telecomunicações geográfica. Ao necessitar de uma comunicação com maior amplitude de acesso foi criada a*WideArea Network*(WAN). Que ao contrário da LAN, servia para locais maiores. Que era uma rede de longa distância para cobrir uma área maior com a conexão de Internet[1].

Com o passar dos anos, a *internet,* que antes era usada somente pelas Forcas Armadas, com uso restrito do governo Americano, teve autorização do Estado, para que cidadãos comuns pudessem fazer o uso dessa tecnologia.

O uso massivo da internet só ocorreu a partir do ano de 1973, quando VintonCerf, do Departamento de pesquisa avançada de Universidade de Califórnia e responsável pelo projeto (Protocolo de IP), que é Internet Protocolo. Trata-se de um código que consente aos diversos *networks* incompatíveis por programas e sistemas comunicarem-se entre si, ou seja, endereços que identifica o ponto de partida de cada computador (PAESANI, 2014).

O endereço de IP (Internet Protocolo) é uma forma de identificar a pessoa física ou jurídica que dela se utiliza. Nesse sentido explica Inellas (2009):

> O endereço lógico é identificado por números, denominados IP. Por conseguinte, um usuário, que queira conectar-se à internet, para enviar e receber mensagens, necessita utilizar um endereço lógico, isto é, um endereço de IP. Evidentemente seria praticamente impossível que um usuário utilizasse um catálogo com milhares de números (endereços lógicos) dos locais com quem quisesse entrar em contato. Surgiu, assim, o nome Domínio. O nome de Domínio é o endereço, o nome de pessoa física ou jurídica, tendo, embutido, o endereço de IP. Dessa forma tornou-se mais fácil o acesso a internet (INELLAS, 2009, p. 5).

[1] GIANTOMASO, Isabele. **Entenda o seu roteador: o que é LAN, WAN, WLAN, DNS, WPS e Ethernet.** Disponível em: <http://www.techtudo.com.br/listas/noticia/2017/02/entenda-o-seu-roteador-o-que-e-lan-wan-wlan-dns-wps-e-ethernet.html> Acesso em 06 de Setembro de 2017 às 19hrs53min.

Outro elemento que impulsionou a verdadeira explosão da internet, e que permitiu ainda para que ela se transformasse em um instrumento de comunicação em massa, foi a *World Wide Web WWW*, ou ainda *W3*, ou simples *Web*. Essa conotação surgiu em 1989.

> O WWW nasceu no ano de 1989, no laboratório Europeu de Física de altas energias, com sede em Genebra, sob o comando de T. Berners-Lee e R. Cailliu. É composto por hipertextos, ou seja, documentos cujo texto, imagem e sons são evidenciados de forma particular e podem ser relacionados com outros documentos. Com um clique no *mouse* o usuário pode ter acesso aos mais variados serviços, sem necessidade de conhecer os inúmeros protocolos de acesso (PAESANI, 2014, p. 11).

Após a criação da Internet Protoloco (IP) com o instrumento de identificação contribui para que o sistema de comunicação funcionasse de forma precisa, colaborando assim para a globalização, porque em cada computador utilizado há um numero específico.

Mesmo com o avanço tecnológico que permitiu a disseminação de informações e comunicação em todo o mundo em tempo real é visível a desigualdade sobre o acesso ao meio digital. Segundo o jornal o Estado de SãoPaulo , em reportagem publicada em Julho de 1999, um cidadão que recebesse o salário médio de Bangladesh teria que trabalhar oito anos para comprar um computador (PAESANI, 2014).

Paesania (2014) firma que a *Internet* surgiu no auge do processo de barateamento das comunicações, ocorrido ao longo do sec. XX, Segunda a autora os usuários da *internet*saltaram de 140 milhões de usuários, em 1998 para mais de 800 milhões nos anos seguintes. Analisando tais dados podemos perceber que o número de usuários cresceu rapidamente em um pequeno período temporal(PAESANI, 2014).

Dados revelam que no final do primeiro trimestre de 2008 havia 41,565 milhões de usuários de *Internet* no Brasil. A venda de computadores foi incentivada através da redução de impostos, a ampliação do financiamento e a queda do dólar, permitindo o acesso de consumidores de renda baixa (PAESANI, 2014).

2.1 Internet e crime cibernético

A *Internet* não pertence a ninguém, não é financiada por instituições, governo ou organizações internacionais, e não é um serviço comercial. Até onde existe

informação, os únicos órgãos que desenvolvem a função de direção controle e funcionamento de rede são, respectivamente, a *Internet Society* (Isoc)[2] e a *Internet EngineeringTask Force* (IETF)[3] (PAESANI, 2014).

> Em 2003, a Cúpula Mundial sobre a Sociedade da Informação (CMSI) colocou a questão de governança da *Internet* nas agendas diplomáticas. Foram adotados documentos estruturais: uma Declaração de Princípios e um plano de Ação para ajudar o efetivo desenvolvimento da Sociedade da Informação e propor o estabelecimento de um Grupo de Trabalho sobre Governança da *Internet* (GTGTI) (PAESANI, 2014, p. 2014).

A ampliação do acesso à*Internet* influenciou para uma transformação qualitativa e quantitativa das informações, das relações sociais e possibilitou que qualquer pessoa o acesse uma quantidade exorbitante de conhecimento em qualquer área do saber.

Mesmo diante de inúmeros benefícios que a ampliação do acesso à *internet* provoca fica a pergunta se existem riscos sobre o seu uso. Dessa maneira quais os riscos que a internet pode nos oferecer nos dias atuais? A *internet*pode gera riscos para o cidadão que dela se utiliza, como por exemplo, sofrer danos materiais e morais, como por exemplo a difamação.

Outro risco elencado corresponde aos crimes praticados que se utilizam da *internet*, conhecidos como: crimes cibernéticos ou cibercrime. O que corresponde ao crime cibernético? Crime cibernético, também conhecido como crime eletrônico, crime de informática, crime digital, crime virtual, etc., é um ato típico, antijurídico, culpável e antiético, cometido sempre com utilização de *softwares*[4]e *hardwares*,[5] para transmissão de dados através da Internet, com o intuito de copiar dados sem autorização, prejudicar outrem, atentar contra a liberdade individual, à privacidade, à honra, etc.[6]

---

[2]**Internet Society (Isoc):** Facilita o desenvolvimento aberto de padrões, protocolos, administração e infra-estrutura técnica da Internet

[3] **Internet EngineeringTask Force (IETF):** A Internet EngineeringTask Force (IETF) é uma grande comunidade internacional aberta de designers de redes, operadores, fornecedores e pesquisadores preocupados com a evolução da arquitetura da Internet e o bom funcionamento da Internet.

[4]**Softwares:**Conjunto de componentes lógicos de um computador ou sistema de processamento de dados; programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador; suporte lógico.

[5]**Hardwares:**O hardware é a parte que você pode ver do computador, ou seja, todos os componentes da sua estrutura física.

[6] Neto, Lindolf Pires. **CRIMES CIBERNÉTICOS: necessidade de uma legislação específica no Brasil.**Disponível em <http://www.fespfaculdades.com.br/painel/uploads/arquivos/trabArquivo_11052010080523_LINFOLFO.pdf> Acesso em 07 de Outubro de 2017, às 20hrs00min.

Os crimes virtuais podem ser cometidos por dois tipos de pessoas. Por pessoas que não possuem um amplo conhecimento sobre conteúdo da informática, porém cometem pequenos crimes, como injuria difamação, calunia racismo etc. E também por pessoas com conhecimentos elevados sobre o mundo digital, denominados *Hackers* éticos e*Hackers* não éticos ou conhecidos também como *Crackers*.

> São especialistas, os denominados *hackers* éticos, que invadem sistemas, corrigem falhas de segurança e instalam uma porta única e controlada, com propósito de garantir a exclusividade no acesso. O *hackers* não éticos (*crackers)*, é o invasor destrutivo que tenta invadir na surdina os portões de entrada dos servidos da *internet*, que são a melhor forma de disseminar informações (PAESANI, 2014, p. 22).

"Segundo dados demonstrados pela *Computer Security Institute*[7](CSI), os prejuízos financeiros atribuídos a crime de computador podem ultrapassar US$ 10 bilhões por ano (PAESANI, 2014, p. 23)." Esse crescimento é atribuído à *Internet*, que facilita para os *hackers* cometam vários crimes por ano em diversas regiões do planeta por ano.

A proliferação de conexões de alta velocidade à *Internet*, por linhas telefônicas ou *modems* a cabo permanentemente conectados, aumentou muito o número de alvos disponíveis do crime virtual. Ou seja, qualquer PC[8] que não tenha um sistema de segurança como o um bom antivírus, corretamente configurado será acessível a *hackers* sempre que o computador estiver ligado (PAESANI, 2014).

Assim o rápido desenvolvimento das novas tecnologias para a *Internet* também abre possibilidades para o *cibercrime*, como já cogitado, e é impossível para qualquer grupo corporativo de segurança manter-se atualizado com relação a essa evolução de computadores, ou seja, tornando o a prática de crimes virtuais comuns e incontroláveis (PAESANI, 2014).

3. ESTELIONATO NA INTERNET

Como afirmado no tópico anterior, existem uma série de crimes cibernéticos, ou seja, crimes que se perfazem por meio da *internet*, mais que provocam efeitos na

[7]O Computer Security Institute (CSI) era uma organização de membros profissional que atende profissionais de informações, redes e segurança física habilitada para computador, desde o nível de administrador do sistema até o principal responsável pela segurança da informação. Foi fundado em 1974.
[8]PC: Computador Pessoal (em inglês: Personal Computer).

vida cotidiana de uma série de pessoas. Um desses crimes virtuais corresponde ao estelionato.

O que é estelionato? O termo estelionato vem de *stellio* (camaleão que muda de cor para enganar a presa). Na origem de sua tipificação, o *stelionatus* era considerado um delito extraordinário e abrangia todos os casos em que houvesse fraude, mas que não se amoldasse dentre os crimes patrimoniais. Tratava-se, portanto, de uma espécie de delito subsidiário, de definição genérica.[9]

O estelionato é tipificado em nosso Código Penal Brasileiro, no seu artigo 171, *caput,* que diz:

> " Art. 171. Obter, para si ou para outrem, vantagens ilícita, em prejuízo alhieo, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa."

A fraude é a característica fundamental do estelionato, é a ação física do delito. Trata-se de crime no qual, ao invés da violência ou da ameaça, o sujeito ativo faz uso de estratégias para induzir a vítima em erro, objetivando vantagem ilícita em prejuízo alheio.

O estelionato pode ser cometido por diversas maneiras, como por exemplo, pessoal quanto através da internet. De fato o estelionato é uma dos crimes mais praticados, pois,diariamente pessoas são vítimas de caso com esse tipo de ação, e em grande parte os criminosos atuam sempre induzindo o cidadão comum a erro (NUCCI, 2014).

O Sujeito passivo do crime de estelionato será uma pessoa determinada, ou seja, aquela que se encontra em situação favorável que comete o crime. Se a fraude for direcionada de forma genérica, haverá delito contra a economia popular ou contra as relações de consumo (NUCCI, 2014).

O sujeito ativo da relação jurídica pode ser em das modalidades, que é a exposta, que se encontra no caput do Art. 171, do Código Penal Brasileiro, e nas modalidades previstas no § 2°, do mesmo. Que fundamenta que a pessoa tem que ser pessoa envolvida em dano ou negócio jurídico, ou legitimo possuidor de determinada coisa (NUCCI, 2014).

O bem jurídico tutelado é o patrimônio, pois visa proteger o do patrimônio daquele que sofreu prejuízo com o comportamento fraudulento empregado pelo

---

[9] LUCA, de Caio. **Estelionato.** Disponível em: <https://caiodeluca.jusbrasil.com.br/artigos/148391504/estelionato> Acesso em: 24 de Setembro de 2017 às 10hs07min.

agente que praticou a conduta ilícita. O objeto material pode é considerado a vantagem obtida ou coisa alheia, bem como aquela que incide no erro. Para ser mais claro, o objeto material é momento da ação em que o agente comete o delito e com ele tira vantagens.

O estelionato pode ser praticado por várias formas, desde pequenas vantagens a grandes fraudes, ou seja, é um crime que provoca muitas vítimas no Brasil, e que muitas vezes acontece e o cidadão envolvido não tem conhecimento do que de fato aconteceu.[10] Neste sentido Nucci, aduz que:

> Há várias formas de cometimento de estelionato, prevendo-se a genérica no caput. Obter vantagem (benefício, ganho ou lucro) indevida induzindo ou mantendo alguém em erro. Significa conseguir um benefício ou um lucro ilícito em razão do engano provocado na vítima. Esta colabora com o agente sem perceber que está se despojando de seus pertences. Induzir quer dizer incutir ou persuadir e manter significa fazer permanecer ou conservar. Portanto, a obtenção da vantagem indevida deve-se ao fato de o agente conduzir o ofendido ao engano ou quando deixa que a vítima permaneça na situação de erro na qual se envolveu sozinha. É possível, pois, que o autor do estelionato provoque a situação de engano ou apenas dela se aproveite (NUCCI, 2014, p. 626).

Deste modo, destaco ainda que o estelionato constitui o elemento subjetivo do tipo específico, que pode ser considerado como a vontade do agente em ter vantagens e obter lucros, mediante prejuízo alheio.

3.1 Estelionato virtual

O nosso ordenamento jurídico não comporta leis especificas e processuais no caso do estelionato virtual, utilizando o Código Penal Brasileiro, nessas situações. Percebe-se que o ordenamento comporta certa carência quando se trata de litígios que envolvem a internet.

O estelionato virtual como já mencionado é trabalhando de acordo com o Art. 171, *caput,* do Código Penal Brasileiro. Inellas, explica:

> Dessarte, verifica-se que o crime de estelionato na sua modalidade básica (art. 171, *caput,* do Código Penal) e em seu § 3°, tamb´me pode ser cometido através da internet. Nesse caso, a conduta do agente ativo consiste no emprego do meio informático, para induzir ou manter a vítima em erro, obtendo comisso vantagem ilícita, para si ou para outrem. Tais condutas são as denominadas fraudes eletrônicas. Nesse caso, a conduta utilizada é a de levar a vítima a erro, media ardil. Ardil é o engano praticado por intermédio de insídia (INELLAS, 2009, p.65).

[10] Formas de Estelionato: Brilhete premiado; Falso sequestro; Pacote de dinheiro etc.

A forma mais utilizada para cometer esse crime, é o acesso indevido da internet, principalmente, daqueles que verificam seus saldos bancários pelo computador. Quando a pessoa coloca seus dados como as senhas, e fazem o acesso no sistema bancário, seus dados são transferidos e salvos no sistema de criminosos, facilitando a transferências de valores da conta da vítima (INELLAS, 2009).

Existem diversos outros casos de crimes econômicos, como manipulação de saldos de contas, balancetes em bancos, etc, alterando, omitindo ou incluindo dados, com o intuito de obter vantagem econômica. A fraude informática é o crime de computador mais comum, mais fácil de ser executado, porém, um dos mais difíceis de ser esclarecido (PAESANI, 2014).

O caso de estelionato virtual não requer do sujeito ativo um conhecimento sofisticado em computação e pode ser cometido por qualquer pessoa que obtenha acesso informático. Usando software específico, podem-se codificar amplamente as informações eletrônicas contidas nas tarjas magnéticas dos cartões de bancos e nos de crédito (PAESANI, 2014).

Entretanto, o meio fraudulento deve ser idôneo a induzir a vítima em erro, idoneidade deve ser analisada levando-se em conta as condições pessoais da vítima e as circunstâncias do caso concreto. O sujeito ativo do crime agente utiliza os meios digitais/informáticos para induzir ou manter a vítima, aproveitando a brecha para conseguir extrair em proveito próprio ou de outrem uma vantagem ilícita. Tais condutas, segundo Inellas, são denominadas de fraudes eletrônicas (INELLAS, 2009).

A principal figurapública que sofreu sérios danos com estelionato virtual foià atriz Glória Pires, que recebeu um e-mail, de um amigo que estava fora do paíse pedia-lhes dinheiro para que regressasse ao Brasil.

Segundo informações do site G1, atriz Gloria Pires foi vítima de estelionato pela internet. De acordo com informações do delegado Gilson Perdigão, titular da Delegacia de Repressão aos Crimes de Informática (DRCI) do Rio de Janeiro, a artista esteve nesta sexta-feira (19) na polícia para realizar um registro. A notícia foi veiculada pela Rádio CBN.

Segundo a polícia, a atriz informou que foi procurada, por e-mail, por um amigo que mora fora do Brasil. Ele pedia que a artista depositasse uma quantia, não divulgada, para que ele pudesse voltar ao país, pois ele estaria sem dinheiro e

passaporte. Glória realizou o depósito, mas depois descobriu que o e-mail do amigo havia sido hackeado e que ele não havia recebido o dinheiro.

O delegado informou que instaurou inquérito e pediu a quebra de sigilo de dados para apurar a autoria do estelionato.[11]

Deste modo a compreensão do estelionato virtual fica visível, e não muito distante da realidade de cada um. Notoriamente cada indivíduo da era pós-moderna faz o uso da *Internet*, por algum aparelho eletrônico, seja ele, computador ou celular. Deste modo todos estão sujeitos a sofrer tipos de ações como essa em questão (estelionato).

4. LEGISLAÇÃO E ESTELIONATO VIRTUAL

O primeiro problema a ser enfrentado, nos crimes cometidos por meio da *internet*, é o da autoria, ou seja, a identificação do individuo. Quase nunca uma pessoa que pretende cometer uma infração penal, no meio digital utiliza sua verdadeira identificação pessoal (INELLAS, 2009).

Segunda e questão é o da competência, como o Brasil é um imenso território a dificuldade de identificar o crime e puni-lo é maior. E muitas vezes esses crimes são praticados fora do país, em grande parte não cogita a possibilidade de intervir para restringir esse tipo de ação (INELLAS, 2009).

O Brasil pode proibir, por exemplo, a pornografia na *Internet*, mas não poderá proibir os provedores de outros países, ou seja, os criminosos que atuam fora do país ficam impunes. Como já expresso existe carência de leis nesse sentindo e a quantidade de usuários da *internet* no mundo e no país é gigantesca.

Há um sério problema quando o assunto é legislação para os crimes virtuais (cibercrimes), porque em grande parte desses crimes não a lei adequada. E se não a leis para reger o litígio, não terá como os nossos julgadores fazer um trabalho com excelência.

> A necessidade urgente de leis específicas, penais e processuais penais, com relação aos crimes praticados através da internet, foi alertada pelo desembargador Castro Meira, do Tribunal Regional Federal da Quinta Região, durante o Congresso Internacional de Direito e Tecnologias da Informação. Contudo, esclareceu que, por ora, mesmo sem legislação específica, crimes contra a honra, cometidos pela internet, por exemplo, a

[11] G1 Rio 24/04/2013. **Atriz Gloria Pires é vítima de estelionato pela internet, diz polícia.** Disponível em <http://g1.globo.com/rio-de-janeiro/noticia/2013/04/atriz-gloria-pires-e-vitima-de-estelionato-pela-internet-diz-policia.html> Acesso em 07 de Outubro de 2017, às 21hrs09min.

> seu ver, pode ser capitulados como crimes de imprensa (INELLAS, 2009, p. 14).

Não existe regimento com leis específicas penais e nem processuais no nosso ordenamento jurídico brasileiro, dificultando o trabalho da polícia para a punição dessas pessoas que cometem crimes virtuais. Vários doutrinadores firmam que a omissão legislativa contribui para que o índice de crimes seja extremamente alto.

Vejamos:

> Não possuímos legislação especifica a respeito de crimes virtuais e o nosso Código Penal Brasileiro de 1940. Evidentemente, no combate aos criminosos virtuais, a Justiça utilizada o Código Penal, pois, a grande maioria das infrações penais cometidas através da internet, pode ser capitulada nas condutas específicas, isto é, as condutas criminosas, praticadas através da internet. Os crimes cometidos através da internet são delitos como quaisquer outros; somente seu modo de execução é diferente (ILNELLAS, 2009, p. 35).

E com o estelionato virtual não poderia ser diferente, visto que esse crime não tem lei especifica e nem processual para fazer sua positivação na ceara brasileira, restando tão somente o Código Penal, que servi de base para o enquadramento do criminoso que faz o uso desta ação.

Como no caso mencionado acima em que a atriz Glória Pires foi vitima de estelionato virtual não houve a colocação do crime em lei especifica, mais sim no Código Penal, que prevê as possíveis penas para quem comete o crime de estelionato.

O crime de estelionato virtual é extremamente praticado no dia a dia, e em muitas vezes com quadrilhas especializadas. Como mostra esse julgado do Ceará:

> PENAL. PROCESSO PENAL. HABEAS CORPUS LIBERATÓRIO. PRISÃO PREVENTIVA. QUADRILHA ESPECIALIZADA EM ESTELIONATO VIA INTERNET. ARTIFÍCIOS E MEIOS FRAUDULENTOS DE ALTA TECNOLOGIA. FATOS QUE REQUEREM CONHECIMENTO TÉCNICO MAIS DETIDO DOS RESPONSÁVEIS PELA APURAÇÃO. DEMORA NÃO CONFIGURADA. CONVENIÊNCIA DA INSTRUÇÃO. APLICAÇÃO DO REGIME DE PROGRESSÃO DA PENA À PRISÃO CAUTELAR. IMPOSSIBILIDADE. NECESSIDADE DE MANUTENÇÃO DA PRISÃO PREVENTIVA. 1- Além da comprovação da materialidade dos delitos e dos fortes indícios de autoria que militam contra o paciente, a sua segregação preventiva revela-se conveniente à instrução tendo em vista a natureza dos crimes praticados, que envolvem o emprego de técnicas criminosas na internet, valendo-se de sofisticados artifícios e meios fraudulentos de alta tecnologia, os quais, por si sós, requerem um conhecimento técnico mais detido por parte dos responsáveis pela elucidação dos fatos criminosos, justificando a atual situação processual do paciente. 2- Eventual excesso, apurável ulterior e oportunamente, não pode ser presumido em via de habeas corpus para a liberação de prisão cautelar, onde não há falar em pena, circunstâncias, ou qualificadoras. A prisão preventiva é, em essência, cautelar, não sendo possível a aplicação da progressão de regime consentânea à execução das prisões-penais. 3- Remanescem as razões

> que ditaram a necessidade da prisão preventiva do paciente para assegurar a aplicação da lei penal e a conveniência da instrução criminal, como também como garantia da ordem pública. 4-Ordem denegada.
> (TRF-5 - HC: 2470 CE 0024875-48.2006.4.05.0000, Relator: Desembargador Federal José Baptista de Almeida Filho, Data de Julgamento: 04/07/2006, Segunda Turma, Data de Publicação: Fonte: Diário da Justiça - Data: 25/07/2006 - Página: 471 - Nº: 141 - Ano: 2006).

A *internet* tem certos amparos pela lei brasileira com relação à liberdade de utilização, que de fato não é restrita e nem especificada por pessoa. No artigo 220, da Constituição Federal, de 1988, aduz que “a manifestação do pensamento, a criação, a expressão e a formação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o dispositivo nesta Constituição.”

Na Constituição Federal em seu Artigo 5°, XXXIX, diz que “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal.” Assim como no Artigo 1° do Código Penal Brasileiro. Ou seja, para que o criminoso seja punido deve antes ser analisado o principio da legalidade, que em grande maioria dos casos não há regimento legal para tais crimes cibernéticos, como já mencionado usando o Código Penal.

Como já comentado existem diversas modalidades de crimes que são praticados no ciberespaço, porém muitos desses crimes não podem ser julgados por falta de lei específica e de meios de identificação adequando para punir tais criminosos virtuais.

No ordenamento jurídico do país contém algumas leis que regem certos atos de criminosos virtuais. Que são elas: Lei n° 12737/12, conhecida como Lei Carolina Dieckimann e Lei N° 12965/14, Lei do Marco Civil da Internet.

A lei Carolina Dieckimann trouxe algumas alterações no Código Penal, que são os artigos 154-A e 154-B, que são os delitos informáticos, crimes cometidos contra o computador da vítima, que tenha violação para que o crime seja consumado:

> 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."

De fato esses dispositivos são de certa importância quando olhando por uma visão onde só exista praticada a invasão de privacidade virtual, porém essa é uma pequena alteração quando analisado a gama de crimes existentes no ciberespaço.

Já a lei do Marco Civil, Lei N° 12965/14 em seu Art. 1° diz: "Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria."

"A lei disciplina do uso *internet* tem como fundamento o respeito à liberdade de expressão, comunicação e manifestação do pensamento e tem como objetivo promover a todos o acesso à *internet*(PAESANI, 2014, p. 83)*."*

Com a aprovação do Marco Civil, os *blogs* devem ser guardados por um ano e esse prazo pode ser estendido, ou seja, só será obtido o *blog* por medida judicial assim como outra ordem judicial autoriza a associação entre numero do IP e do numero. Nesse caso, é preciso comprovar que haja um crime naquele horário e que o usuário seja suspeito de ter cometido esse crime (PAESANI, 2014).

Os usuários respondem pelo conteúdo que publicarem e os provedores de acesso não podem ser responsabilizados por danos decorrentes de conteúdos gerados por usuários. Os provedores de conteúdo serão responsabilizados caso não acatem no prazo determinado decisões judiciais que mandem tirar conteúdos gerados pelos usuários (PAESANI, 2014).

Antes da lei do Marco Civil a *internet*, não tinha restrições de provedores, desde modo qualquer pessoa podia fazer o que quisesse e não seria identificado e muito menos tinha responsabilidade por parte dos *sites* ou das páginas de comunicação.

Inellas (2009), diz que crimes cometidos através desse meio (*internet*) éimperativos que nossos legisladores, com maior brevidade criem leis e mecanismos processuais preventivos para proporcionar a Policia Judiciária e ao Ministério Público um efetivo combate a criminalidade virtual (INELLAS, 2009).

Segundo Inellas (2009), além do Ministério Público ser um atuador na questão, existe duas autoridades responsáveis que ajuda na investigação e na identificação de autores que são elas de responsabilidade da Polícia Federal e da Polícia Civil (INELLAS, 2009).

Deste modo é visível que os crimes virtuais praticados no Brasil, em especial o estelionato eletrônico não possui leis direcionadas. Assim o ordenamento jurídico não acompanha tal crescimento dentro do mundo cibernético tornando difícil para que as autoridades cumpram com seu serviço.

5. CONCLUSÃO

A globalização trouxe diversos recursos para a sociedade como, por exemplo, a *Internet.* Com tantas modificações surgem os litígios que devem ser solucionados garantindo a integridade do cidadão que tornou vulnerável diante de tantas mudanças com o passar do tempo.

A *Internet* ensejou algumas mudanças na vida das pessoas no Brasil. O numero de usuários deste meio é grandioso, com isso os conflitos e crimes aumentamà medida que a própria tecnologia desenvolve.

Deste modo com o avanço tecnológico dentro da globalização o ordenamento no Brasil, não comporta e nem acompanha tal velocidade dos crimes virtuais, sendo carente de leis específicas e processuais que tratem diretamente de tais atos. O nível de crescimento é incontrolável, consequentemente os doutrinadores e juristas não conseguem serem eficazes nas positivações das leis.

Para ter uma visão melhor sobre o nosso Código Penal e de 1940, e a cada minuto existe um crime virtual diferente, com ações e modalidades diferentes.

Com isso o crime de estelionato só pode ser aplicado com o Código Penal, ou seja, não tem uma lei específica para essa pratica de crime virtual. Porém existe a Lei n° 12737/12 lei Carolina Dieckimann, que não trata do estelionato e sim da invasão da privacidade*oline.*

O legislador vem tentando aplicar, qualificar tais crimes, porém não surte tanto

efeito para essas praticas do ciberespaço. Então, existe uma necessidade dos legisladores criarem normas legais e processuais para freia/inibir as diversas modalidades de crimes virtuaiscomo já mencionado, o estelionato.

Portanto nota-se que por falta de leis específicas deixam de punir as condutas de pessoas que usam a *Internet,* para cometer crimes virtuais. Deste modo o quanto antes leis voltadas para esse senário de crimes, devem ser criadas para prevenir o cidadão de bem, que é o principal alvo desses criminosos.

REFERÊNCIAS

Brasil, Lei n° 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos**; altera o Decreto-Lei n° 2.848, de 7 de dezembro de 1940 – Código Penal; **e dá outras providências**. Diário Oficial da União, Brasília, 30 de Nov. 2012.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília; Senado Federal. Subsecretaria de Edições Técnicas, 2004.

EBC, Portal. **Entenda o Marco Civil da internet ponto a ponto, 2014**. Disponível em: <http://www.ebc.com.br/tecnologia/2014/04/entenda-o-marco-civil-da-internet-ponto-a-ponto>acesso em 14 maio, 2017, às 09: 30 min.

G1 Rio 24/04/2013. **Atriz Gloria Pires é vítima de estelionato pela internet, diz polícia**. Disponível em <http://g1.globo.com/rio-de-janeiro/noticia/2013/04/atriz-gloria-pires-e-vitima-de-estelionato-pela-internet-diz-policia.html> Acesso em 07 de Outubro de 2017, às 21hrs09min.

GIANTOMASO, Isabele. **Entenda o seu roteador: o que é LAN, WAN, WLAN, DNS, WPS e Ethernet**. Disponível em: <http://www.techtudo.com.br/listas/noticia/2017/02/entenda-o-seu-roteador-o-que-e-lan-wan-wlan-dns-wps-e-ethernet.html> Acesso em 06 de Setembro de 2017 às 19hrs53min.

INELLAS, Gabriel Cesar Zaccaria**. Crimes Na Internet**. 2ºed: São Paulo-SP. Ed. Juarez de Oliveira. 2009.

Lei nº 12.965, de 23 de abril de 2014. **Estabelece Princípios, Garantias, Direitos e Deveres para o uso da Internet no Brasil**. Diário Oficial da União, Brasília. 24 de

abril de 2014. Disponível em: <http://coral.ufsm.br/congressodireito/anais/2015/6-10.pdf> acesso em 14 maio, de 2017, às 10: 43 min.

LUCA, de Caio. **Estelionato.** Disponível em: <https://caiodeluca.jusbrasil.com.br/artigos/148391504/estelionato> Acesso em: 24 de Setembro de 2017 às 10hs07min.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 10º ed: Rio de Janeiro-RJ. Ed. Forense. 2014.

NETO, Lindolf Pires. **CRIMES CIBERNÉTICOS: necessidade de uma legislação específica no Brasil**. Disponível em <http://www.fespfaculdades.com.br/painel/uploads/arquivos/trabArquivo_11052010080523_LINFOLFO.pdf> Acesso em 07 de Outubro de 2017, às 20hrs00min.

SILVA, Remy Gama. **Crimes na Informática.** Disponível em <http://www.cesarkallas.net/arquivos/livros/direito/00715%20%20Crimes%20da%20Inform%E1tica.pdf> Acesso em 09 de Outubro de 2017, às 18hrs52min.

NETO, Lindolf Pires. **CRIMES CIBERNÉTICOS: necessidade de uma legislação específica no Brasil**. Disponível em <http://www.fespfaculdades.com.br/painel/uploads/arquivos/trabArquivo_11052010080523_LINFOLFO.pdf> Acesso em 07 de Outubro de 2017, às 20hrs00min.

PINHEIRO, Emeline Piva. **Crimes virtuais: uma análise da criminalidade informática e da resposta estatal**. Porto Alegre: PUCRS, 2006. Disponível em: <http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2006_1/emelin e.pdf>. Acesso em: 18 de Outubro de 2017.

PEASANI, Liliana Minardi. **Direito e Internet**. 7º ed: São Paulo-SP. Ed. Atlas S.A. 2014.

VAINZOF, Rony. **Leis dos Crimes Virtuais (Lei Carolina Dieckmann).** Análise daLei nº 12.737/12: Avanços e Lacunas. In: PAESANI, Liliana Minardi (Coord.). O Direito na Sociedade da Informação III. São Paulo: Ed. Atlas, 2013.