

**UMA ANÁLISE DA INEFICÁCIA DO DIREITO PENAL BRASILEIRO EM  
RELAÇÃO À INTERNET<sup>1</sup>**

Arthur Gomes Tabet<sup>2</sup>  
Luiza Barbosa Pereira<sup>3</sup>  
Ricardo Clemente Jorge<sup>4</sup>

**RESUMO**

O presente trabalho versa mais precisamente sobre crimes cibernéticos, ou seja, os crimes que passaram a ser perpetuados em ambiente virtual, buscando verificar até que ponto é possível viabilizar a aplicação da lei penal no ambiente cibernético no qual, a cada dia, amplia fortemente a execução de condutas delituosas. Para isso foi feito uma pesquisa descritiva, bibliográfica e documental com o objetivo de estabelecer um breve histórico do contexto social e legalista dos crimes virtuais, analisando também como outros países reagiram a esse fenômeno, além da evolução do Direito Penal brasileiro no que concerne os crimes virtuais e o impacto que eles trazem para a sociedade.

**PALAVRAS-CHAVE: CRIMES VIRTUAIS. INTERNET. CRIMES CIBERNÉTICOS.**

---

<sup>1</sup> Este artigo foi desenvolvido na disciplina Projeto Integrador, no quarto período do curso de Direito das Faculdades Integradas Vianna Júnior durante o segundo semestre de 2016

<sup>2</sup>email: arthurgomestabet@gmail.com

<sup>3</sup>email: luizab38@gmail.com

<sup>4</sup>email: ricardo\_clemente\_jorge@hotmail.com

## INTRODUÇÃO

No mundo globalizado que vivemos a rápida e crescente evolução da tecnologia fez com que as distancias em todo o mundo fossem encurtadas e as relações entre as pessoas passassem a serem feitas na maior parte das vezes utilizando equipamentos eletrônicos conectados a uma chamada rede mundial de computadores, “internet”.

Buscaremos como objetivo geral, verificar até que ponto a legislação brasileira se aplica nesses crimes e como é executada essa aplicação na prática. Para isso faremos diversas pesquisas bibliográficas, jurisprudenciais, comparando com legislações estrangeiras e, dessa maneira, tentando obter uma abordagem investigativa do impacto que os crimes cibernéticos têm causado na sociedade. Repara-se hoje, que o Brasil tem quase 80 milhões de internautas, porém o nosso Código Penal nem menciona a palavra “internet”, na nossa legislação não há previsão legal para punir crimes virtuais; tudo é muito novo e faltam equipamentos, leis que tipifiquem o crime virtual, mecanismos tecnológicos de rastreamento a nível mundial e acima de tudo, informação.

Visto as informações e dados colhidos observamos a que é necessário compreender melhor os fenômenos sociais causados pela evolução tecnológica e pela globalização decorrente desta, bem como indagar a eficiência e abrangência da lei penal brasileira diante dos crimes virtuais e a impunidade acarretada pelo cenário legal nos dias de hoje.

## 1 HISTÓRICO E EVOLUÇÃO

### 1.1 O começo dos crimes cibernéticos

Em 1987, a internet foi liberada para o uso comercial, sendo esta etapa considerada como um grande marco para o desenvolvimento desta tecnologia. Em 1993, com o desenvolvimento do World Wide Web (WWW), a internet popularizou-

se. Especificamente no Brasil, a internet deu seus primeiros passos apenas em 1988, quando a Rede Nacional de Pesquisa(RNP) e o Ministério da Ciência e Tecnologia começaram a investir na tecnologia. Em 1992, os primeiros pontos de pesquisas foram instalados em algumas universidades e, em 1995, a rede mundial de computadores foi liberada para uso comercial, dando início aos grandes avanços das telecomunicações no Brasil.

No entanto, ao lado de todos os benefícios trazidos pela internet, surgiram novas formas de violação de bens jurídicos protegidos pelo ordenamento, os quais passaram a ser realizados não mais no plano físico, mas, sim, no plano virtual. Conforme Colli (2009, p. 07):

Apesar de a internet facilitar e ampliar a intercomunicabilidade entre as pessoas, ela pode ter sua finalidade transformada em um meio para a prática e a organização de infrações penais. Dentre estas despontam os chamados crimes informáticos.

A internet pode ser tanto ambiente propício para a consumação de crimes, quanto para a realização de seus atos preparatórios, como nos casos de rixas entre torcidas organizadas. Os primeiros registros de ocorrência dos crimes virtuais ocorreram por volta de 1970, sendo realizados em sua grande maioria por pessoas que detinham grande conhecimento na área informática, tendo como objetivo principal burlar o sistema de segurança de grandes conglomerados empresariais.

## **1.2 Como o Direito Penal pode acompanhar a evolução tecnológica**

O Direito Penal encontra muitas dificuldades de adaptação dentro deste contexto. O Direito em si não consegue acompanhar o frenético avanço proporcionado pelas novas tecnologias, em especial a Internet, e é justamente neste ambiente livre e totalmente sem fronteiras que se desenvolveu uma nova modalidade de crimes, uma criminalidade virtual, desenvolvida por agentes que se aproveitam da possibilidade de anonimato e da ausência de regras na rede mundial

de computadores. Percebe-se de forma indutiva que muitos indivíduos que não seriam capazes de cometer delitos nas relações concretas (indivíduo x indivíduo), encontram no meio virtual segurança para o cometimento de delitos, seja tendo o virtual como meio (tráfico de drogas), seja como forma direta de prática de crime (estelionato).

Ao Direito Penal enquanto ciência, lhe é conferida a forma subsidiária de resolução dos conflitos instalados entre os membros da coletividade, demonstrando, portanto, que é imprescindível a concretização ou a grande possibilidade de dano para a penalização das condutas desenvolvidas pelo meio digital, porém não será proveitoso somente a previsibilidade do dano se não existir uma proporcionalidade entre a conduta delitativa, agora descrita conforme as perspectivas de risco da coletividade e a pena ao qual se imputará, trazendo à tona mais uma vez a importância da descrição de tais condutas nas normas penalizadoras, ou seja necessidade de classificação específica para os delitos virtuais.

### **1.3 Posicionamento jurisprudencial atual**

De início, deve-se analisar o posicionamento do Superior Tribunal de Justiça no Conflito de Competência n.º 116.926/SP, no qual foi discutida a competência territorial a respeito de um crime de racismo cometido em comunidade virtual. No caso, vários agentes proferiam em rede social posicionamentos visualizados como racistas, mas cada qual os enviou de uma localidade distinta. Ao verificar a localidade precisa de cada indiciado, o inquérito foi desmembrado para que cada um fosse processado e julgado na sua respectiva jurisdição. (BRASIL, 2013)

Ao apreciar o caso, o Superior Tribunal de Justiça entendeu que o crime praticado dentro de um círculo de confiança, fazendo com que cada atitude isolada fosse unida às demais configurando um único conjunto probatório, fato que tornaria o juízo do primeiro inquérito, no caso, o de São Paulo, preventivo para processar e julgar todas as ações delituosas. Assim, foi determinado o retorno de todos os

processos ao juízo prevento, ressalvados os casos em que já houvesse publicação de sentença.(BRASIL, 2013)

Por fim, deve-se analisar um caso que tem a rede mundial de computadores como base para a consumação do delito. Trata-se do Habeas Corpus n.º 198401/CE acerca de um furto qualificado cometido contra instituições bancárias pela internet. No caso, os pacientes utilizaram a rede mundial de computadores para furtar uma quantia aproximada de um milhão de reais. (BRASIL, 2011)

Ao apreciar o caso, o Superior Tribunal de Justiça reforçou o entendimento de que prisão cautelar é medida excepcional e que só deve ser decretada nos casos em que houver suficiente fundamentação que a justifique. No entanto, o caso versava sobre agentes que já haviam reiterado suas ações, acumulando como resultado de suas condutas delituosas uma quantia de expressivo valor comercial. (BRASIL, 2011)

Em sua fundamentação, os ministros afirmaram que a soltura dos mesmos provocaria a fragilidade do conjunto probatório, tendo em vista se tratar de um crime cometido na esfera virtual, fato que dificulta a reunião do conjunto probatório. Ademais, os antecedentes dos pacientes indicavam ser altamente provável que os mesmos, caso fossem libertos, retornariam a cometer seus crimes pela rede mundial de computadores ou, pior, fugiriam. Logo, a ordem foi denegada e a prisão foi mantida.(BRASIL,2011)

#### **1.4A legislação brasileira no que concerne crimes virtuais**

O ordenamento é formado por vários ramos jurídicos, cada qual com sua legislação específica, ocorrendo o mesmo com os crimes informáticos. No entanto, durante muitos anos, esta parte do ordenamento esteve sem cobertura legal específica, pois foi apenas em 2012 que o legislador federal editou as duas leis que atualmente norteiam o direito informático, quais sejam, a Lei n.º 12.735 (BRASIL, 2012) e a Lei n.º 12.737 (BRASIL, 2012), ambas do dia 30 de novembro de 2012. Tipificando as condutas realizadas mediante uso de sistema eletrônico, digital ou

semelhante, que sejam praticadas contra sistemas informatizados e similares. Sendo um verdadeiro suporte para as demais legislações que venham a ser aprovadas no ordenamento brasileiro, pois trazem a determinação de que os órgãos da polícia judiciária devem estruturar setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado, tudo de acordo como determinar o regulamento específico, além de editar a tipificação criminal dos principais delitos informáticos, relacionados com a invasão de dispositivos informáticos e a divulgação indevida de dados computacionais.

## **2 SEGURANÇA E ESTABILIDADE NOS CRIMES VIRTUAIS**

### **2.1 A possibilidade de segurança no ambiente virtual**

O processo vertiginoso de globalização que vemos nos dias atuais é fruto das novas tecnologias e meios de informação que surgiram no novo século, destacando aqui a internet. Todas essas tecnologias fizeram surgir avanços grotescos ligados a comunicação, onde hoje todos se veem conectados à rede.

A realidade virtual, somada ao acesso rápido às informações dadas pela internet dão um sentimento de liberdade para o indivíduo. A evolução ágil e eficaz desses novos meios fez surgir, também, novas medidas e normas na sociedade atual, como é o caso do Direito. Em face de toda essa liberdade e facilidade que o ambiente virtual proporciona, ocasionou o surgimento de novas práticas delitivas específicas nesse contexto, denominados de crimes virtuais (PINHEIRO, 2006).

Com o surgimento desses novos crimes o Estado teve que se ajustar para garantir a segurança e estabilidade dos indivíduos e usuários desses meios. O Direito existe para regular o convívio social e garantir uma igualdade de direitos, sendo que se necessário deve haver uma utilização do Direito Penal, o qual “constitui-se por um conjunto de normas jurídicas, conhecimentos e princípios, que têm por objetivo dar efetiva resposta à atos praticados contra bens jurídicos de

profunda relevância social e que outras esferas do Direito não sejam capazes de coibir”, como afirma Pinheiro (2006).

Nesse âmbito cibernético, com o crescente número de crimes virtuais, o Direito Penal teve de atuar para a garantia da liberdade, honra e bens jurídicos da sociedade contemporânea. O fim pretendido por quem comete esses crimes se assemelha aos crimes tipificados pelo Código Penal diferenciando um pouco nas técnicas utilizadas. Devido a isso e a ausência de uma lei que aborda sobre o assunto e que seja eficaz, o judiciário brasileiro optou por utilizar as leis já em vigor, fazendo uma analogia com os crimes cibernéticos. Para o entendimento dessa analogia podemos apresentar como exemplo o artigo 171 do referido código: “Artigo 171: Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento”. Conforme se verifica o artigo supra é bem amplo e abrange algumas modalidades de crimes virtuais. Outros crimes, como no caso da pedofilia são enquadrados no Estatuto da Criança e do Adolescente.

A preocupação maior para a garantia de uma estabilidade segura no mundo virtual é quando tratamos dela no âmbito internacional, como afirma Pinheiro (2006):

A Organização das Nações Unidas (ONU) reconheceu que este tipo de delito é um sério problema, já que vários países ainda não adequaram suas legislações mediante a criação de novos tipos penais e procedimentos investigativos, que pudessem ser implementados para o fim de inibir o crescimento dos delitos eletrônicos.

A referida autora continua dizendo que no nosso país há essa preocupação em se adequar a esse novo crime. O legislador brasileiro vem tentando adaptar o Direito com essa nova realidade, um bom exemplo disso são os 13 projetos de lei tramitando no Congresso que versam sobre o assunto.

A segurança garantida pelo Estado, por meio do Direito, para com o mundo cibernético é seguradora dos direitos de liberdade, expressão e bens materiais

apresentados pelos novos meios de comunicação, dessa maneira, Oliveira e Dani concluem (2011):

O Brasil precisa urgentemente criar uma legislação específica para crimes virtuais, uma vez que, a internet hoje tornou-se indispensável para a sociedade, não lhe conferindo mais apenas o caráter de lazer como antigamente, mas sim um caráter de informação, trabalho e lazer

## **2.2 Entendimento e proteção da legislação sobre a possibilidade de instabilidade nos crimes cibernéticos**

Segundo Sergio José Barbosa Junior (2015), o ordenamento jurídico brasileiro é formado por inúmeros ramos, cada qual com sua especialidade, não ficando de fora os crimes virtuais. Contudo, essa parte da legislação esteve sem cobertura legal nos últimos anos, conseguindo só agora, o legislador editar as duas leis mais utilizadas no ambiente cibernético, sendo elas a Lei n.º 12.735 e a Lei n.º 12.737, ambas do dia 30 de novembro de 2012.

O autor explica a importância dessas novas leis, podendo destacar um comentário feito a respeito da garantia de segurança para os usuários dos novos meios de informação, com destaque para a Lei n.º 12.735 de 2012, Barbosa Junior (2015) diz que a lei:

Tipifica as condutas realizadas mediante uso de sistema eletrônico, digital ou semelhante, que sejam praticadas contra sistemas informatizados e similares. É um verdadeiro suporte para as demais legislações que venham a ser aprovadas no ordenamento brasileiro, pois traz em seu artigo 4º a determinação de que os órgãos da polícia judiciária devem estruturar setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado, tudo de acordo como determinar o regulamento específico.

Esse artigo, na Lei n.º 12.735 de 2012 foi de fundamental importância por garantir que a polícia judiciária brasileira organize em seus regimentos setores

especializados em crimes cibernéticos, promovendo um suporte para o legislador brasileiro em criar e editar legislações que versam sobre o assunto.

Ainda há garantia quanto à discriminação nas redes, segundo Sérgio José Barbosa Júnior (2015):

Prevedo a possibilidade de o juiz, verificando a ocorrência de crimes cometidos na esfera virtual relacionados a raça, cor, etnia, religião ou procedência nacional, determinar a cessação da transmissão que contenha o referido delito.

A Lei n.º 12.737, foi editada no mesmo dia da anteriormente citada, trazendo em seu texto “a tipificação criminal dos principais delitos informáticos, relacionados com a invasão de dispositivos informáticos e a divulgação indevida de dados computacionais”.

O artigo 2º dessa segunda lei, modificou o Código Penal Brasileiro, adicionando os artigos 154-A e 154-B ao nosso referido código. Como afirma Barbosa Junior (2015) “Estes artigos dispõem sobre as condutas combatidas na esfera virtual, a respectiva sanção legal a ser aplicada aos futuros infratores e a forma de procedimento da respectiva ação penal”.

O artigo 154-A vem trazendo para o ordenamento o crime de invasão de dispositivo informático, deixando explícito a multa e prevendo detenção de 3 (três) a 1 (um) ano para o indivíduo que invadir dispositivo informático com violação dos mecanismos de segurança, visando a obtenção, alteração ou destruição de dados virtuais sem o consentimento ou autorização do proprietário e ainda garante quanto a instalação de programas em aparelhos com o fim de vantagem ilícita (BARBOSA JUNIOR, 2015).

Esse mesmo artigo trata, também, da distribuição de dispositivos que tenham em seu interior a possibilidade de acometer ao crime mencionado acima. Os casos de invasão e obtenção de dados sigilosos ou pessoais da vítima, seja sobre sua vida pessoal ou dados comerciais e industriais, são garantidos por esse artigo, sendo tratado mais duramente (BARBOSA JUNIOR, 2015).

O artigo 154-B que foi juntamente incluído no Código Penal Brasileiro pela Lei n.º 12737/12 determina a representação para as ações penais que tratam de delitos cibernéticos, havendo a exceção caso o crime seja cometido contra a administração federal, estadual, distrital ou municipal e ainda se cometido contra empresas de serviços públicos. Essa mesma lei acrescentou, ainda, parágrafos aos artigos 266 e 298 do nosso ordenamento penal, tipificando o crime de interrupção de serviços vinculados a comunicação e também tipifica quanto ao crime de falsificação de documento particular.

Por mais que existam leis específicas o judiciário brasileiro ainda aplica, em muitos casos, leis já existentes no Código Penal brasileiro. O avanço tecnológico é rápido e especializado, não tendo como o legislador se ajustar a tantas mudanças repentinas e aumentos desses tipos criminais, sendo assim o judiciário utiliza-se de normas padrões para se ajustar com o tipo de crime. (PINHEIRO, 2006)

### **3 IMPACTO NA SOCIEDADE**

“A parte está no todo, assim como o todo está na parte”. Assim começa Juremir Machado da Silva o seu artigo ‘Pensar a vida’, de 2009 viver o pensamento. Frase que descreve perfeitamente a conjuntura global em que vivemos, onde não existe mais isolamento.

Para Edgar Morin (2007), o que chamamos de globalização hoje em dia é o resultado no momento atual de um processo que se iniciou com a conquista das Américas e a expansão dominadora do ocidente europeu sobre o planeta. Para ele não há uma única globalização (ou modernização), mas duas que são ligadas e antagônicas. E há fenômenos quase ambivalentes, como o desenvolvimento das comunicações. Ambivalentes porque o desenvolvimento das comunicações, sobretudo nos últimos anos, com o fax, o telefone celular, a Internet, a comunicação instantânea em todos os pontos do planeta, é um fenômeno notável no sentido que pode ter efeitos muito positivos, que permitam comunicar, entender e intercambiar informações.

Nesse passo, é possível observar que a Internet corresponde a um salto no desenvolvimento da humanidade, a uma mudança de paradigmas no pensar e agir da sociedade, a uma verdadeira revolução na história. Assim, relação entre as realidades virtual e real consiste atualmente em um dos problemas centrais da filosofia e da ciência em geral. Para muitos, a realidade virtual cada vez mais toma o lugar da realidade real, o que faz com que os crimes virtuais tenham um maior poder, trazendo a sociedade uma grande insegurança, um impacto social maior do que previsto pelo código penal.

### **3.1 Crianças e Adolescentes**

Levando em consideração o exposto a cima, podemos observar, de acordo com o Dr. Thomás de Figueiredo Ferreira, que os adolescentes de hoje fazem parte do final da geração Y ou início da geração Z, sendo suscetíveis aos avanços da internet, de forma a usufruir do maior número possível de recursos tecnológicos.

A cada minuto um novo aplicativo é lançado e nascem novas redes sociais, conectando todo tipo de gente, dos mais diversos lugares possíveis. Além disso, chats, jogos on-line e, todos os demais recursos tecnológicos, como smartphones e tablets, são extremamente atraentes aos adolescentes, até mesmo porque é justamente nessa fase da vida que existe grande demanda para estarem conectados em tempo integral aos demais amigos (FERREIRA, 2015).

Ocorre que a concepção de muitos adolescentes na utilização da web é que no universo virtual tudo é permitido, não existem regras nem sanções, e lá podem falar tudo o que pensam, sendo isentos de punições. Além disso, existem adolescentes que replicam na internet o seu comportamento na vida real e adolescentes com receio de ficar com má fama entre os amigos e que passam a praticar atos reprováveis na Internet. A cada dia que passa, observamos mais e mais incidentes na esfera virtual que acabam repercutindo e causando estragos no mundo real (FERREIRA,2015).

De acordo com o site de advocacia Figueiredo e Ferreira os crimes mais recorrentes em que as crianças e adolescentes se tornam vítimas são: i) Publicação de boato e ofensa à imagem de uma pessoa; ii) Ameaças e “agendamento” de brigas; iii) Divulgação de fotos e/ou vídeos íntimos; iv) Invasão de computadores e divulgação de documentos confidenciais.

Assim sendo, ainda de acordo com o site, a ocorrência desses casos, apesar de praticados por adolescentes no mundo virtual, pode desencadear uma série de responsabilizações tanto criminais quanto cíveis, abrangendo na última hipótese, os pais e responsáveis pelo menor.

No âmbito penal, os atos praticados pelos menores de 18 anos são considerados “atos infracionais”, ou seja, a conduta de desrespeito às leis, à ordem pública, aos direitos dos cidadãos ou ao patrimônio, cometido por crianças ou adolescentes. Uma vez praticado um ato infracional, os menores estão sujeitos às medidas sócio educativas previstas no art. 112 do Estatuto da Criança e do Adolescente, medidas essas que vão desde uma advertência e prestação de serviços à comunidade, até a internação em estabelecimento educacional, dependendo da gravidade do ato cometido.

Já na esfera Cível, conforme previsto no art. 932, inciso I, do nosso Código Civil, os pais são responsáveis pela reparação civil dos atos praticados pelos filhos menores que estiverem sob sua autoridade e em sua companhia. Ou seja, os prejuízos causados no ambiente virtual, são passíveis de indenizações judiciais no mundo real, arcando os genitores com o pagamento desses ressarcimentos.

É notável que tais crimes virtuais envolvendo adolescentes na Internet devem ser combatidos de forma preventiva, pelas famílias, pela escola e pelo governo. Devido às atribuições da vida moderna, os pais ficam cada vez mais distantes dos filhos, vindo estes, como consequência, a fazer uso de dispositivos com acesso à internet desde cedo e sem orientação sobre o seu uso de forma adequada e com segurança.

A escola, por meio de um corpo docente devidamente treinado e qualificado, composto por professores e psicólogos, deverá exercer seu papel de contribuir para

a formação do aluno, por meio de programa de prevenção de riscos em ambiente virtual.

Por fim, o Governo deverá estimular a criação de programas destinados a alunos que fazem parte de famílias com baixa condição socioeconômica, para que possam tomar conhecimento dos cuidados a serem tomados na internet e as consequências da prática de determinados atos.

Quando ingressarem no mercado de trabalho, os adolescentes de hoje deverão estar preparados para se comportarem de forma adequada e segura em ambiente virtual. Em seu trabalho, poderão ter acesso a documentos e informações confidenciais e diversos recursos tecnológicos. Suas interações serão cada vez mais intensas por meio de ferramentas de comunicação. A Internet irá além do mero entretenimento, busca de informações sobre trabalhos escolares e rede de amizades.

### **3.2 Fobia, medo, insegurança**

A Segurança Pública pode ser compreendida como a estabilidade de expectativas com relação à ordem pública englobando o aspecto social-cooperativo. Fundamentada nesta visão a criminologia procura desenvolver o estudo da criminalidade, analisando as políticas públicas e as práticas criminosas tendo por referência o medo, a sensação de insegurança, a instabilidade de expectativas da sociedade. O fator basilar pelo crescimento vertiginoso dos crimes virtuais no Brasil é justamente a visão ultrapassada sobre crime e criminoso que permeia na sociedade brasileira, sendo necessário uma mudança radical na análise dos fatores intrínsecos ligados diretamente à perturbação da ordem pública (LOPES, 2006).

Sendo assim, vivemos cercados pelo medo, temos nossa liberdade cerceada, estamos acuados em nossas casas, ou nas ruas, estamos sempre acompanhados da crescente criminalidade e da violência em todos os segmentos sociais. A constante sensação de insegurança nos acompanha de forma ininterrupta. A sensação de insegurança que predomina na população brasileira é alimentada por

vários fatores: visibilidade dos crimes c, participação intensiva da mídia, o comportamento elitista da sociedade e o distanciamento entre as pessoas. (LOPES, 2006). Os meios de comunicação contribuem para aumentar essa sensação de insegurança ao divulgarem os crimes cometidos por cidadãos marginalizados, policiais no exercício de suas funções e delitos cometidos pelos detentores do poder político. A imprensa falada e escrita sempre procura mostrar que os níveis de violência e criminalidade no Brasil extrapolam a normalidade criminal criando um sentimento de insegurança que permeia toda sociedade, deixando o brasileiro totalmente inseguro diante do crescimento vertiginoso da criminalidade divulgado pela mídia. (LOPES, 2006).

O medo e a sensação de insegurança são reforçados também pelo distanciamento entre os cidadãos, denominado rompimento das relações verticais de comunicação, com o abandono dos espaços sociais e pela constante desconfiança dos cidadãos, uns em relação aos outros e destes com as instituições oficiais, instituições que se tem mostrado incapazes de responder aos anseios da população de desfrutar uma maior qualidade de vida, idealizada através do conceito de segurança (LOPES, 2006).

Uma sociedade que discrimina, que divide, seleciona seus indivíduos contribui sensivelmente para a elevação da sensação de insegurança entre os membros da sociedade. Diante do exposto, conceituar segurança pública pode se tornar arriscado, pois, um conceito sintético torna reducionista o referido tema, já o conceito amplo pode tornar a concepção abstrata e não esclarecer. Estamos vendo que inserido no conceito de segurança pública deve ser levado em consideração à sensação de segurança, a participação da mídia no trato com a criminalidade, o nível do racismo e do elitismo social, o dever do Estado, a garantia da ordem, obrigação da polícia, as relações verticais de comunicação e a formação da própria sociedade. (LOPES, 2006).

Segurança Pública, assim sendo, não é uma atividade exclusiva do Estado e sim da sociedade em seu conjunto, compreendendo por uma condição de percepção e sensação por parte do elemento social de ter plena liberdade de ir vir, possuir bens

materiais e subjetivos sem ser molestado por forças antagônicas. Segurança Pública abrange a possibilidade de todos os cidadãos viverem em sociedade com sentimento de segurança virtual e real, protegidos em seus direitos. Espero que tenha ficado claro que a criminalidade não atinge somente o indivíduo, mas, também, a memória coletiva comprometendo o presente e o futuro social. (SILVA, 2003). Para que o ideal segurança seja atingido, o professor Jorge da Silva (2003) em sua obra “Segurança Pública e Polícia”, sugere que se diminuam os riscos reais ou imaginários e gerencie os riscos e o medo através de novos posicionamentos os quais passamos a ressaltar: O paradigma de sociedade paradisíaca, sem conflitos, sem crimes, deve ser superado. O objetivo do Estado em prover segurança a todos os cidadãos indistintamente é inatingível, pois, a violência e a criminalidade são fatores inerentes ao convívio social. Concluindo, para minimizar a insegurança e o medo advindo do aumento da criminalidade deve existir uma política de segurança pública integrada, em nível nacional, visando objetivamente diminuir os elevados índices de criminalidade e dar ao povo brasileiro o sentimento de segurança. A criminalidade não pode ser enfrentada apenas pelo sistema repressivo do Estado e sim por toda a sociedade. Consideramos que é atribuição específica do Estado é a melhoria da organização policial e do sistema prisional dentro de parâmetros democráticos e respeito aos direitos humanos. Não se pode falar em diminuição da criminalidade e sentimento de segurança sem a existência de uma sociedade solidária e que predomine a justiça social. (SILVA, 2003)

#### **4 DIREITO COMPARADO**

A evolução no tratamento dos crimes digitais, apesar da sua complexidade para legislar, ocorre concomitantemente ao avanço da tecnologia, cada vez mais os países passam a investir em estudos tecnológicos e agora, sabendo dos grandes riscos que correm na incidência da não previsibilidade de legislação que disponibilizem meios de preservar expectativas contrafaticamente, é possível vislumbrar até mesmo uma mudança de paradigmas sobre tal assunto. As

codificações penais estrangeiras passaram a tutelar bens incorpóreos que ainda não eram possíveis a sua previsão, no que se refere à tecnologia, e a partir desse reconhecimento sofrem mudanças também as medidas aplicáveis à proteção desses bens.

#### **4.1 Diferença de legislações**

Para Sieber (2011), acerca da criminalidade informática existem hoje seis ondas legislativas criadas em diversos países como Áustria, Alemanha, Suécia, Espanha, França, Estados Unidos, Finlândia, Irlanda, Holanda, Japão, Israel, Canadá, entre tantos outros visando a proteção dos novos bens jurídicos a fim de garantir a segurança jurídica, bem como da soberania de seus territórios, são elas: Proteção da privacidade; Direito Penal econômico; Proteção da propriedade intelectual; Conteúdo ilegal e lesivo; Leis de segurança.

Diante dessas informações torna-se necessária uma análise sobre as formas legislativas adotadas em alguns países, assim como os seus mecanismos de coibição, a fim de contrastar os diferentes sistemas para que, dessa maneira, seja possível concluir o que seria melhor e mais aplicável no caso brasileiro com base nos exemplos de mais eficácia à respeito dos crimes cibernéticos ao redor do mundo.

#### **4.2 Estados Unidos**

Como bem se sabe o direito norte-americano baseia-se no Common Law (modelo de justiça baseado em precedentes judiciais). É implantado aos Estados Unidos a política do federalismo, ao qual é permitido aos demais estados criarem suas próprias regras sem que seja preciso utilização do processo legislativo, cada estado desenvolve seu modelo de justiça. O Common Law é capaz de criar um direito ou dever a partir de uma decisão judicial que sirva como precedente, vinculando todas as outras decisões posteriores, ele é regido pelo princípio

do “stare decisis”. Contudo, estando verificada a controvérsia em caráter divergente da decisão anterior poderá o tribunal decidir o seguinte caso como um novo precedente. Para o direito penal norte-americano o crime é a violação ou negligência de obrigação legal, de tal importância pública que o direito, costumeiro ou estatutário, toma conhecimento e implementa punição. A maioria dos crimes é de competência estadual (GODOY, 2007)

É possível afirmar que uma das primeiras manifestações informáticas ilegítimas aconteceram nos Estados Unidos com Robert Tappan Morris, um estudante de pós-graduação, que começou a trabalhar em um programa de computador, explorando os defeitos de segurança que havia descoberto na internet, a fim de demonstrar a inadequação das medidas de segurança nas redes de computadores, criando os “worms” vírus capazes de se expandirem em outros computadores com o objetivo inicial de ocupar pouco do funcionamento das máquinas, com a intenção de apenas demonstrar a insegurança das redes computacionais, porém, o experimento acabou tomando proporções maiores e os vírus começaram a se reproduzir e a infectar mais máquinas causando grande prejuízo para as redes de computadores à época. (UNITED STATES OF AMERICA, 1991)

A partir de então, os Estados Unidos travaram um verdadeiro combate à criminalidade informática, tal combate se deu em dois patamares: o estadual e o federal. No âmbito federal encontrou-se a Lei de Proteção aos Sistemas Computacionais (“Federal Computer System Protection Act of 1981”), que determinava como conduta delituosa o uso de computadores com o objetivo de praticar fraudes, furtos ou espécies de apropriação indébita. Em seguida, em 1982 surgiu a “Electronic Funds Transfer Act” (lei que trata da regulamentação de transferências eletrônicas de fundos, incriminando as fraudes informáticas que não continham relações interpessoais). A principal lei que traz à baila a responsabilização criminal de condutas ilícitas no âmbito informático é a “Computer Fraud and Abuse Act” (Lei de Fraude e Abuso Computacional) datada de 1986

que visa proteger a acessibilidade dos sistemas para a obtenção de segredos nacionais ou com o intuito de obter vantagens financeiras.(CRESPO, 2011)

### **4.3 Suécia**

A Suécia foi o primeiro país a elaborar norma incriminadora com o intuito de proteger os bens informáticos. Ademais o sistema processual Sueco, regido pelo Código “Rättegångsbalken”, em vigência desde 1948, e à época considerado um código moderno, é aplicável tanto à seara Cível como Penal, desde que pertencentes à Corte Ordinária. Em regra, todos os casos devem ocorrer na primeira instância não existindo em sede de crimes peculiaridades no seu tratamento, no que diz respeito ao instrumentalismo de acordo com a gravidade do crime. É importante salientar que o processo penal Sueco é adversarial, ou seja, o juiz não conduz de forma ativa o processo, este será conduzido pelas partes, guardando semelhança com o direito processual norte-americano, logo não será um processo investigativo. Apresentada à Corte pelas partes o conteúdo fático e de direito da demanda, esta ficará adstrita a decidir unicamente com base no que foi apresentado. O promotor será o autor no processo penal e a vítima funcionará como litisconsorte ativo facultativo (ORTON, 2011).

Sendo interessante comentar que na Suécia, ainda no campo da legislação, a evolução da sociedade da informação caminha para um novo conceito de democracia: o fenômeno da “e-democracy”, que é a participação dos cidadãos na vida política de seu país pelo voto eletrônico, desta forma a internet é utilizada como meio de estabilização e maior participação em leis e questões políticas, em busca de estabelecer um feedback estatal (salientando ainda mais a importância da segurança no ambiente virtual). Na vanguarda desse movimento temos o partido político “Demoex” que, de acordo com Azevedo (2012, p.5):

Funciona de forma que o representante eleito vote de acordo com os resultados das votações online feitas pelos membros. O

objetivo é que o representante atue da maneira mais fiel possível à opinião dos membros do partido, não imprimindo a sua vontade acima da opinião da maioria. Ou seja, o representante seria apenas uma mera formalidade, pois o poder estaria nas mãos dos membros do partido. O Demoex utiliza a distribuição estatística, o que significa que o representante na câmara decide seu voto com base na estatística extraída da participação dos membros na internet

#### **4.4 Alemanha**

Aparentemente em meados dos anos 80 deram-se início às primeiras formas de responsabilização penal pelos delitos tecnológicos na Alemanha. Existem afirmativas de que na sociedade alemã a conduta delituosa em crimes informáticos não possui grande relevância, devido a sua pequena incidência. Seus principais problemas na esfera tecnológica se referem ao uso abusivo de informações, porém, em 1986 foi editada a Segunda Lei de Combate à Criminalidade Econômica, que traz em seu texto normas contra a criminalidade informática. Na presente legislação, não são punidas meras invasões de sistema, porém, alguns delitos são tipificados de forma especial como: espionagem de dados; extorsão informática; falsificação de elementos probatórios, incluindo aí a falsidade documental e a ideológica; sabotagem informática; alterações de dados e utilização abusiva de cheques ou cartão magnéticos. (CRESPO, 2011)

#### **4.5 França**

Via de regra, a França não apresenta legislação destinada a punição de condutas criminosas no âmbito digital fazendo valer a ideia de que a expressão “manoeuvres frauduleuses” seria bastante ampla a ponto de compreender qualquer nova situação moderna. Em 1995 o Código Penal Francês, passou a constar no próprio código em seus arts. 323-1 ao 323-7 denominados delitos informáticos. Percebe-se então ao visualizar a presente legislação, que mediante a necessidade de tais delitos não seria outro o caminho a não ser

responsabilizar penalmente de forma coerente e específica a criminalidade informática. (CRESPO, 2011)

## CONCLUSÃO

Após a realização deste estudo, é possível concluir que se faz necessário a imediata tipificação em nosso ordenamento jurídico, de condutas criminosas praticadas por meio da internet. Visto que, o Brasil está atrasado no aspecto jurídico, mas em progresso na criminalidade realizada por meios virtuais, devendo-se igualar aos países que já possuem legislação específica para crimes virtuais, para que não sejamos um paraíso aos criminosos desse setor.

Devido a isso, é necessário tentar minimizar ao máximo a insegurança e o medo gerado pelo aumento da criminalidade nesse âmbito cibernético, devendo existir uma política de segurança pública integrada, em nível nacional, visando diminuir os elevados índices de crimes virtuais e dar ao povo brasileiro o sentimento de segurança e não de impunidade.

Ao passo que, a jurisprudência nacional tem se mostrado a favor da responsabilização/condenação dos indivíduos que cometem delitos por meio da internet, mas por haver lacunas na lei a respeito do tema, ainda existem criminosos que não podem ser condenados. Estamos entre os dez países que mais utilizam a internet, em um mercado promissor e crescente, sem uma legislação que defina e classifique quantos e quais são os crimes cometidos virtualmente, para amparar os usuários desse serviço e não gerar insegurança na sociedade.

## REFERÊNCIAS

AZEVEDO, Mauricio Maia Vinhas. **Algumas considerações acerca da democracia direta eletrônica**. Revista de Informação. v.13, n.14. Agosto 2012. Disponível em: <<http://eprints.rclis.org/17599/1/Azevedo-13-4-8-2012.pdf>>. Acesso em: 30. nov. 2016.

BARBOSA JUNIOR, Sérgio. **Crimes informáticos**: delitos virtuais no direito brasileiro. Santa Catarina: 2015. Disponível em: <<http://www.egov.ufsc.br>>. Acesso em: 04 de dez. 2016.

BRASIL. Decreto-Lei 2.848, de 7 de dezembro de 1940. **Código Penal**. *Diário Oficial a União*, Rio de Janeiro, 31 dez. 1940. VadeMecum. São Paulo: Saraiva, 2016

BRASIL, **Lei n.º 12.737 de 30 de novembro de 2012**, que traz a tipificação criminal de delitos informáticos. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/l12737.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm)>. Acesso em: 10 out. 2016.

BRASIL, **Lei n.º 12.735 de 30 de novembro de 2012**, que tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2011-2014/2012/Lei/L12735.htm](http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm)>. Acesso em: 10 out. 2016.

BRASIL, **Superior Tribunal de Justiça**. Competência em crimes informáticos. Conflito de competência n.º 116.926 SP. Juízo Federal da 9ª Vara Criminal da Seção Judiciária do Estado de São Paulo e Juízo Federal da 12ª Vara da Seção Judiciária do Estado do Ceará. Relator: Ministro Sebastião Reis Júnior. Terceira Seção. 04 fev. 2013. DJe 15 fev. 2013.

BRASIL, **Superior Tribunal de Justiça**. Pedido de relaxamento de prisão relacionada a crimes cometidos pela internet. Habeas Corpus n.º 198401/CE. Paulo Cauby Batista Lima e Outros e Tribunal Regional Federal da 5ª Região. Relator: Ministro Og Fernandes. Sexta Turma. 16 jun. 2011. DJe 24 ago. 2011.

COLLI, Maciel. **Cibercrimes**: limites e perspectivas para a investigação preliminar policial brasileira de crimes cibernéticos. Porto Alegre: PUCRS, 2009. Disponível em: <[http://tede.pucrs.br/tde\\_busca/arquivo.php?codArquivo=2477](http://tede.pucrs.br/tde_busca/arquivo.php?codArquivo=2477)>. Acesso em: 10 out. 2016.

CRESPO, Xavier de Freitas. **Diretivas Internacionais e Direito Estrangeiro**. In: Crimes Digitais. São Paulo: Saraiva, 2011.

DA SILVA, Jorge. **Segurança pública e polícia**: criminologia crítica aplicada. Rio de Janeiro: Forense, 2003.

FERREIRA, Thomás; YAMADA, Fernando. **Crimes virtuais envolvendo adolescentes: responsabilidades e prevenção**. Figueiredo e Ferreira Advocacia. 2015. Disponível em: <<http://figueiredoeferreira.com.br/noticias/crimes-virtuais-envolvendo-adolescentes>>. Acesso em: 04 dez. 2016.

GODOY, Arnaldo Sampaio de Moraes. **Direito penal nos Estados Unidos**. Revista Jus Navigandi, Teresina, ano 12, n. 1481, 22 jul. 2007. Disponível em: <<https://jus.com.br/artigos/10179>>. Acesso em: 4 dez. 2016.

LOPES, Roquete Liliane. **Segurança pública**: uma questão social, legal e de polícia. Disponível em: <<http://www.atenas.edu.br/Faculdade/arquivos/NucleoIniciacaoCiencia/REVISTAJU RI2006/9.pdf>>. Acesso em: 02 dez. 2016.

MORIN, Edgar. **As duas globalizações**: comunicação e complexidade. 3 ed. São Paulo: Sulina, 2007.

OLIVEIRA, Luiz Gustavo Caratti de; DANI, Marília Gabriela Silva. **Os crimes virtuais e a impunidade real**. In: Âmbito Jurídico, Rio Grande, XIV, n. 91, ago. 2011. Disponível em: <[http://www.ambito-juridico.com.br/site/index.php?n\\_link=revista\\_artigos\\_leitura&artigo\\_id=9963](http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9963)>. Acesso em: 02 dez. 2016.

ORTON, Frank. **Algumas características especiais do Processo Civil Sueco**. Tradução: Alexandre Freitas Câmara. R.EMERJ, Rio de Janeiro, v.14, n.54. 2011. Disponível em: <[http://www.emerj.tjrj.jus.br/revistaemerj\\_online/edicoes/revista54/Revista54\\_7.pdf](http://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista54/Revista54_7.pdf)>. Acesso em: 05 dez. 2016

PINHEIRO, Emeline P. **Crimes virtuais**: uma análise da criminalidade informática e da resposta estatal. Disponível em: <<http://www.egov.ufsc.br/portal/conteudo/crimes-virtuais-uma-analise-da-criminalidade-informatica-e-da-resposta-estatal>>. Porto Alegre, 2006. Acesso em: 01 dez. 2016.

SIEBER. Apud. CRESPO, Xavier de Freitas. **Diretivas Internacionais e Direito Estrangeiro**. In: Crimes Digitais. São Paulo: Saraiva, 2011.

SILVA, Jorge da. **Segurança pública e polícia: criminologia crítica aplicada**. Rio de Janeiro: Forense, 2003.

SILVA, Machado Juremir. **Pensar a vida**. Disponível em:  
<<http://www.correiodopovo.com.br/blogs/juremirmachado/2009/11/11/7/>>. São Paulo, 2009. Acesso em: 02 dez. 2016.

UNITED STATES OF AMERICA, **apelle, Robert Tappan Morris, defendant-apellant**. 1991. Disponível em: <[http://www.loundy.com/CASES/US\\_v\\_Morris2.html](http://www.loundy.com/CASES/US_v_Morris2.html)>. Acessado em: 3 dez. 2016.