

**CENTRO UNIVERSITÁRIO TABOSA DE ALMEIDA- ASCES/ UNITA
DIREITO**

**O DIREITO DIGITAL E OS CRIMES CIBERNÉTICOS: OS LIMITES
DA ATUAÇÃO CRIMINAL NO ÂMBITO VIRTUAL NO BRASIL**

RENATA CARVALHO DE AZEVEDO RÉGIS

CARUARU

2018

RENATA CARVALHO DE AZEVEDO RÉGIS

**O DIREITO DIGITAL E OS CRIMES CIBERNÉTICOS: OS LIMITES
DA ATUAÇÃO CRIMINAL NO ÂMBITO VIRTUAL NO BRASIL**

Trabalho de Conclusão de Curso, apresentado ao Centro
Universitário Tabosa de Almeida - ASCES/ UNITA,
como requisito parcial para obtenção do grau em Direito.
Orientador: Prof. Esp. Marupiraja Ribas

CARUARU

2018

BANCA EXAMINADORA

Aprovado em: ____/____/____

Presidente: Prof. Esp. Marupiraja Ribas

Primeiro Avaliador: Prof.

Segundo Avaliador: Prof.

RESUMO

O presente artigo faz um estudo dos Crimes Cibernéticos frente à Teoria das Janelas Quebradas, demonstrando a importância do efetivo enquadramento penal e da repreensão a estas condutas no meio virtual. Para tanto, através do método lógico dedutivo, demonstra-se a necessidade de regulação das novas relações no campo da Internet, diante do considerável crescimento de usuários da Grande Rede experimentado nos últimos anos, bem como da evolução do Direito para englobar e regular estas relações, frente aos diversos conflitos que surgem neste meio. Evidencia-se que as vítimas destes crimes ainda possuem descrença de que podem ser apurados, resolvidos e devidamente punidos, fato que leva à escassez de denúncias e à impossibilidade de quantificar, de acordo com a realidade, sua verdadeira ocorrência. Neste sentido que é defendida a Teoria das Janelas Quebradas, tendo em vista que, como sustenta a teoria, o Princípio da Insignificância deve ser dispensado em alguns casos, por estimular a reiteração criminosa. A referida teoria defende que a ausência de punibilidade ou a punibilidade branda dos crimes que ocorrem no meio virtual pode vir a resultar em sua banalização. Para corroborar as afirmações feitas, há a exposição de dados estatísticos que demonstram a descrença da população na apuração destes crimes, bem como a reiteração criminosa por parte dos agentes, pela impunibilidade e falta de repreensão adequada experimentada em diversos casos no Brasil. Dessa forma, expõe-se a necessidade da adequação do Direito Penal para os Crimes Virtuais, tendo em vista que o Direito Penal brasileiro não admite a analogia, se esta não se der em favor do réu, ante as consequências que essa omissão vem causando no mundo fático.

Palavras-Chave: Crimes Cibernéticos; Crimes Virtuais; Internet; Teoria das Janelas Quebradas.

ABSTRACT

The present article makes a study of the Cybernetic Crimes compared to the Broken Window Theory, demonstrating the importance of the effective penal framework and the reprimand to these conducts in the virtual environment. In order to do so, through the deductive-logic method, it is necessary to regulate the new relations in the Internet field, owing to the considerable growth of users of the Great Network experienced in recent years, as well as the evolution of the Law to encompass and regulate these relations, given the various conflicts that arise in this environment. It is evident that the victims of these crimes still have disbelief that they can be ascertained, resolved and properly punished, a fact that leads to the scarcity of denunciations and the impossibility of quantifying, according to reality, its true occurrence. In this sense that is defended the Broken Window Theory, considering that, as the theory maintains, the Principle of Insignificance should be dispensed in some cases, because it encourages criminal reiteration. The said theory argues that the lack of punishability or the soft punishability of crimes that occur in the virtual environment may result in their trivialization. In order to corroborate the statements made, there is the exposure of statistical data that demonstrate the disbelief of the population in the investigation of these crimes, as well as the criminal reiteration on part of the agents, for the impunity and lack of adequate reprimand experienced in several cases in Brazil. So, it is exposed the necessity of the adequacy of the Criminal Law of Virtual Crimes, considering that the Brazilian Criminal Law does not admit the analogy, if not in favor of the defendant, in order of the consequences that this omission have been causing to the world.

Keywords: Cybernetic Crimes; Virtual Crimes; Internet; Broken Window Theory;

SUMÁRIO

INTRODUÇÃO	06
1 O DIREITO DIGITAL, A INTERNET E OS CRIMES CIBERNÉTICOS	07
2 A PUNIBILIDADE DOS CRIMES INFORMÁTICOS E A TEORIA DAS JANELAS QUEBRADAS	15
3 O PROCESSO JUDICIAL PARA PUNIÇÃO DOS DOS CRIMES CIBERNÉTICOS E A SOLUÇÃO PARA AS LACUNAS NORMATIVAS DO BRASIL	21
CONSIDERAÇÕES FINAIS	25
REFERÊNCIAS.....	27

INTRODUÇÃO

O presente artigo propõe-se a analisar casos reais, juntamente com a lei brasileira, relacionando-os, com o objetivo de fazer uma exposição acerca dos crimes virtuais e do Direito Digital, bem como evidenciar de forma clara os limites da atuação e as consequências dessa limitação, mais precisamente no Brasil, onde estes crimes crescem consideravelmente. Dessa forma, visa atrair atenção para um tema que ocorre com frequência, mas ainda possui dificuldades para sua atuação, investigação e, conseqüentemente, imposição de sanções jurídicas.

Neste raciocínio, tem como principal objetivo evidenciar a dificuldade de atuação da polícia frente aos crimes cibernéticos a partir de diversos âmbitos: as limitações da investigação – visto que o Brasil ainda é um país carente de tecnologias realmente eficientes voltadas para este aspecto, deixando muitas vezes o pensamento de que a *Internet* é uma terra sem lei se disseminar, sendo o país conhecido como maior exportador de crimes eletrônicos do mundo –, bem como no sentido de que muitas vezes não há denúncias, devido a esta descrença na resolução de tais transgressões.

Além disso, é importante ressaltar que a ocorrência destes crimes virtuais, ainda que por vezes haja o pensamento de que se resumem ao âmbito virtual, tem consequências no mundo real, atingindo bens jurídicos palpáveis, deixando o sentimento de que poderiam ter sido evitados com antecedência se tivessem sido devidamente investigados e resolvidos.

A codificação do país também se mostra extremamente escassa, criando leis nesse sentido que não têm efetiva aplicação na prática, dando aos aplicadores do Direito a tarefa, por vezes árdua, de enquadrar tais crimes em normas antigas.

Evidencia-se ainda a importância do estudo de tais crimes no âmbito criminal, para a sociedade em geral, que em sua maioria já foi ou pode vir a ser vítima desse tipo de conduta, para a prevenção, evitando que estes saiam do meio virtual para o real e passem a diminuir, para os legisladores, num incentivo à supressão das lacunas normativas e um combate à impunidade, evitando que os transgressores saiam ilesos.

O maior objetivo deste estudo se dá no âmbito da prevenção, para que estas condutas possam ser menos reincidentes e as vítimas tenham mais confiança em denunciá-las, tendo em vista que os relatos deste crime são ínfimos frente ao número de casos reais que atingem diversas vítimas.

Desta feita, o presente artigo será baseado na doutrina brasileira e internacional, bem como no estudo de artigos científicos referentes ao tema, no estudo de casos reais e

dados estatísticos sobre o tema, para que se torne possível uma análise sólida da própria realidade do Brasil. Terá como principal orientador o Código Penal e demais leis correlacionadas, como também a Lei Maior Brasileira.

1 O DIREITO DIGITAL, A INTERNET E OS CRIMES CIBERNÉTICOS

O Direito surge frente à sociedade humana, e expande-se a partir do desenvolvimento das civilizações. À medida que o homem passa a progredir e prosperar, mostram-se cada vez mais necessárias regras que ditem e protejam a convivência pacífica, a harmonia e a paz social. Dito isto, o Direito emana do homem e seu objetivo primordial é regular as relações sociais.

Neste sentido, preleciona o autor Paulo Nader:

As necessidades de paz, ordem e bem comum levam a sociedade à criação de um organismo responsável pela instrumentalização e regência desses valores. Ao Direito é conferida esta importante missão. A sua faixa ontológica localiza-se no mundo da cultura, pois representa elaboração humana. O Direito não corresponde às necessidades individuais, mas a uma carência da coletividade. A sua existência exige uma equação social. Só se tem direito relativamente a alguém. O homem que vive fora da sociedade vive fora do império das leis. O homem só, não possui direitos nem deveres. (2014, p. 52)

Dessa forma, para manter tal organização da sociedade e cumprir sua finalidade principal, mostra-se necessário o emprego de instrumentos de controle social, através de normas.

A prevenção, por exemplo, implementa coação psicológica nos indivíduos, para que não realizem determinada conduta. Se esta falha, há a aplicação de outro método: as sanções, que podem realizar outros tipos de coação neste mesmo indivíduo. O doutrinador, sobre esta temática, contribui:

A participação do Estado na vida do Direito não se restringe ao controle da elaboração das regras jurídicas. Além de zelar pela manutenção da ordem social por seus dispositivos de prevenção, com o seu aparelho coercitivo aplica o Direito a casos concretos. (NADER, 2014, p. 149)

Seguindo também esta linha, encontra-se o doutrinador Hans Kelsen, autor da Teoria Pura do Direito, apud Eduardo García Máñez: “em determinadas circunstâncias, um determinado sujeito deve observar tal ou qual conduta; se não a observa, outro sujeito, órgão do Estado, deve aplicar ao infrator uma sanção.” (1964, p. 169).

Por esse motivo, alguns autores afirmam que o Direito tem função ordenadora na sociedade (CINTRA, GRINOVER E DINAMARCO, 1991, p. 25), ou seja, o Direito organiza as relações, visando o bem comum e a manutenção da ordem. Assim, segundo este autor, o Direito não apenas coordena a sociedade, mas o faz compondo seus conflitos, para que prevaleça a harmonia social.

É seguindo essa linha em que surge o próprio Direito, que nasce o Direito Digital. Se o Direito e suas normas reguladoras exercem a função de ordenar a sociedade, devem evoluir à medida que a sociedade evolui, como tem ocorrido nos últimos anos. Assim, não poderia ser diferente em relação aos novos meios tecnológicos que ocupam cada vez mais espaço na vida e cotidiano das pessoas. A especialista na temática do Direito Digital, Patrícia Peck, discorre neste diapasão:

Ter uma janela aberta para o mundo exige muito mais que apenas a seleção do público-alvo. Exige a criação de uma logística jurídica que reflita a diversidade cultural dos consumidores/clientes virtuais. No aspecto de atendimento ao consumidor, por exemplo, parte das empresas inseridas na rede recorrem à terceirização, contratando contactcenters especializados para atender a demanda de usuários de diferentes culturas e países. No aspecto jurídico, é preciso que os profissionais de Direito também estejam preparados para criar essa logística, sabendo que a todo o momento terão de lidar com diferentes normas, culturas e legislações. (PINHEIRO, 2009, p. 22)

Desta feita, o Direito Digital nada mais é que uma extensão do próprio Direito, frente à necessidade e à evolução do próprio indivíduo. Quando a Internet e os meios eletrônicos passaram não só a integrar a convivência, mas também a fazer parte da vida das pessoas, tornaram-se necessárias medidas capazes de regular, também, as relações neste meio, visto que nem sempre se mostram positivas.

Segundo Corrêa:

A presença cada vez mais forte dos computadores em nossas vidas, a capacidade de coletar e analisar dados pelas empresas e pelo Estado, e de disseminá-los através das rápidas vias das telecomunicações, nos têm proporcionado benefícios, mas, na mesma proporção, também malefícios. (CORRÊA, 2000, p. 20).

Neste mesmo sentido, discorre Salo de Carvalho:

“[...] fundamental que os operadores das ciências criminais tenham (cons)ciência de que os riscos da sociedade pós-industrial (riscos catastróficos e imensuráveis) estão para além da capacidade de controle penal, e que a era da segurança (jurídica) foi soterrada pelo próprio projeto que a construiu: a Modernidade.” (CARVALHO, 2004, p. 208)

Assim, torna-se uma árdua tarefa para o Direito acompanhar, compreender e amparar as novas demandas de uma sociedade moderna que evolui constantemente, necessitando de

meios que auxiliem na manutenção da ordem social. Em meio a esta exigência, surge o Direito Digital, para ajudar a suprir lacunas decorrentes da modernidade e da evolução tecnológica. Neste diapasão, contribui ainda:

A tecnologia digital é uma realidade, e justamente por isso estamos diante da criação de lacunas objetivas, as quais o direito tem dever de estudar, entender e, se necessário, preencher. Com a crescente popularização da grande rede, evidenciamos a criação de novos conceitos sobre tradicionais valores, tais como a liberdade, a privacidade e o surgimento de “crimes” digitais. (CORRÊA, 2010, p. 21)

No que diz respeito à popularização da rede supracitada, tornou-se imprescindível a atenção a esse âmbito do Direito frente aos vastos números referentes à utilização de meios eletrônicos, que evidenciam que mais de metade do Brasil encontra-se conectada.

Afirma-se isso de acordo com apuração feita pelo TIC Domicílios 2014, pesquisa realizada pelo Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (G1, 2015). Este centro elaborou a pesquisa a partir de entrevistas a moradores de 19 mil domicílios em mais de 350 municípios de todo o Brasil entre outubro de 2014 e março de 2015.

Nesse sentido, tal popularização nem sempre se mostra benéfica. Se, por um lado, o acesso à informação mostra-se uma maneira prática e útil de conhecimento, por outro, o crescimento de usuários desencadeia também o crescimento de crimes, fraudes e violações no campo digital.

Nos últimos anos, o assunto tem sido priorizado por diversos estudiosos, em busca de tentar minimizar os danos causados *online*. Porém, trata-se de uma tarefa árdua, já que muitos vêem a *Internet* como “terra de ninguém”, em que o anonimato é garantido e a facilidade da desapareição, que ocorre em questão de segundos, dificulta a identificação dos autores.

Nesse campo de incertezas e frente à necessidade de regras e normas que possam regular os relacionamentos virtuais, o Direito Digital tem seus pilares.

Posto isso, o Direito Digital é essencialmente o resultado da relação entre a ciência do Direito e a ciência da computação. Da mesma forma que, no desenvolvimento das civilizações passaram a ser necessárias normas para proteger a harmonia e a paz social, no âmbito das novas tecnologias também surge a necessidade de instrumentos que regulem a relação do homem com as inovações tecnológicas. Ou seja, não se trata de uma nova área do Direito, mas do próprio Direito sendo aplicado no âmbito virtual. José Almeida conceitua:

Trata-se do conjunto de normas e conceitos doutrinários destinados ao estudo e normatização de toda e qualquer relação em que a informática

seja o fator primário, gerando direitos e deveres secundários. É o estudo abrangente, com o auxílio de todas as normas codificadas de Direito, a regular as relações dos mais diversos meios de comunicação, dentre eles os próprios da informática. (ALMEIDA, 2005, p. 15)

Esclarecido o conceito de Direito Digital, importante também para compreensão do referido estudo é a conceituação da Internet, visto que este termo será amplamente utilizado no presente artigo.

A *Internet* é um conjunto de redes, que possibilita a comunicação e a circulação de dados online em todo o mundo. Segundo Corrêa:

A Internet é um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina a qualquer outra máquina conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento (CORRÊA, 2000, p. 8).

Assim, segundo o entendimento do doutrinador, a Internet pode ser definida com um conjunto de computadores interligados, facilitando a comunicação e a disseminação de informações. Nesta mesma esteira, discorre Fabrizio Rosa:

A Internet consiste num conjunto de tecnologias para acesso, distribuição e disseminação de informações em redes de computadores. (ROSA, 2006, p.35)

Desta feita, nota-se a semelhança nos conceitos dos doutrinadores, ao tratarem a Internet como um meio de comunicação que tem como principal objeto de uso o computador.

Já a doutrinadora Liliane Paesani conceitua:

Sob o ponto de vista técnico, a Internet é uma imensa rede que liga elevado número de computadores em todo o planeta. As ligações surgem de várias maneiras: redes telefônicas, cabos e satélites. Sua difusão é levemente semelhante à da rede telefônica. Existe, entretanto, uma radical diferença entre uma rede de computadores e uma rede telefônica: cada computador pode conter e fornecer, a pedido do usuário, uma infinidade de informações que dificilmente seriam obtidas por meio de telefonemas. (PAESANI, 2013, p. 12)

Nesse sentido, Paesani ressalta a ligação entre as máquinas, equiparando-a a uma rede telefônica, mas diferenciando-a pela grande quantidade de informações possíveis de se obter através da Grande Rede.

Para Gabriel Inellas:

A definição do conceito de internet pode ser apresentada como uma rede de computadores interligada a uma rede de menor porte que se comunica entre si, utilizando um endereço “lógico” chamado de endereço IP, onde diversas

informações são trocadas, surgindo daí um problema, pois existe uma infinidade de informações pessoais disponíveis na rede, ficando à disposição de milhares de pessoas que possuem acesso à internet, e quando não são disponibilizadas pelo próprio usuário, são procuradas por outros usuários que buscam na rede o objetivo única e exclusivamente de cometer crimes, os denominados Crimes Virtuais [...]. (INELLAS, 2004, p. 3).

Com efeito, a Internet é um verdadeiro mundo virtual, no qual ocorrem diversas relações, circulam inúmeras informações e são estabelecidas várias formas de comunicação, que necessitam de atenção e controle jurídico próprio, acerca das infrações penais cometidas na rede.

O assunto vem ganhando espaço na modernidade, visto que a Internet está cada vez mais disponível para todos os seguimentos da sociedade, gerando, conseqüentemente, o crescimento no número de infrações penais. Porém, a carência dessa temática ainda é enorme e necessita de supressão de lacunas normativas.

Já em relação à Internet, com os avanços na área da tecnologia, a maior difusão de produtos e aparelhos conectáveis à Internet, e a maior facilidade no acesso à rede, houve grande revolução nas relações. Isso porque, com o uso da Internet estendido a grande parcela da população, inúmeras facilidades foram disponibilizadas para seus usuários, transformando a vida das pessoas e impactando a nova geração.

Porém, como se trata de uma extensão do mundo real, este “novo mundo” também é habitado pelos mesmos cidadãos, dotados de vontades, valores e opiniões distintas. Dessa forma, como é observado na convivência de pessoas, são necessários mecanismos de controle, que estabeleçam deveres, para que os interesses de uma determinada parcela não se sobressaiam sobre os interesses dos demais.

Além disso, tais mecanismos são importantes também para auxiliar na preservação de direitos dos próprios indivíduos. Isso porque, desde os primórdios da civilização, quando há convivência em sociedade em que não é exercido nenhum tipo de regulamentação ou controle, é natural que surjam conflitos, decorrentes de lesões a direitos alheios e invasões à sua individualidade, quando estes deveriam ser protegidos.

Nesse contexto, no âmbito da Internet, também existem violações ao direito alheio. Os Crimes Cibernéticos – também chamados de Crimes Virtuais, Crimes Digitais, Crimes Informáticos ou Cyber Crimes – tratam-se, de forma genérica, de um ou vários atos ilegais e puníveis, cometidos na esfera virtual, utilizando-se de tecnologia para sua realização ou

concretização. Ou seja, diz respeito ao uso indevido da tecnologia para causar prejuízo a outrem. Para Corrêa:

Poderíamos dizer que os “crimes” digitais seriam todos aqueles relacionados ‘as informações arquivadas ou em trânsito por computadores, sendo esses dados acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico. Toda sociedade dependente da informação acaba sendo vítima de simples ameaças e até do terrorismo e do vandalismo eletrônicos (CORRÊA, 2010, p. 63).

Para o autor Neil Barrit, é possível conceituá-los como: “a utilização de computadores para ajuda em atividades ilegais, subvertendo a segurança de sistemas, ou usando a Internet ou redes bancárias de maneira ilícita.” (BARRET, 1997, p.31).

Segundo Ferreira (2000, p. 211), este tipo de crime “consiste na utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele a ordem econômica, à liberdade individual, à honra, ao patrimônio público ou privado, etc”. Sendo assim, esse crime ainda é um grande desafio para ciência jurídica, em razão da dificuldade de identificação do seu autor, da velocidade do meio virtual e da carência legislativa. Nesse sentido:

A reprimenda à criminalidade praticada com o emprego dos meios eletrônicos, notadamente os que avançam na rede mundial de computadores, terá de ser acionada por todos os povos civilizados e essa perspectiva deriva, com certeza, do próprio fenômeno da globalização que, em ritmo especial, pauta pelo célere avanço tecnológico alcançado na última década (DAOUN; BLUM, 2000, p. 118).

Os crimes virtuais no Brasil têm crescido gradativamente, à medida que os meios tecnológicos se tornam cada vez mais acessíveis, caindo, por vezes, em mãos erradas. Frente a este fato, torna-se necessária a prevenção de tais crimes quando ainda se encontram no âmbito da Internet, para que estes não tenham espaço no mundo real. Porém, ainda há grande dificuldade no mapeamento e prevenção destes crimes, visto que avançam de acordo com as tecnologias, e ficam, dessa forma, cada vez mais difíceis de combater. Nessa esteira:

A informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar instrumentos nas mãos dos criminosos, cujo alcance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução (FERREIRA, 2000, p. 208).

Para compreensão desses crimes, necessário torna-se primeiro distingui-los, visto que há duas modalidades, adotadas pelo presente artigo seguindo alguns doutrinadores, de crimes informáticos:

Os impróprios, como sendo aqueles que já existem na vida cotidiana, que são até regulamentados por leis, mas que sua prática se estendeu ao mundo virtual, ou seja, os meios informáticos servem como mais um instrumento para realização e concretização de tais crimes; os próprios, que são os que surgiram acompanhando a própria tecnologia, nasceram nos terrenos da Internet, sendo estes restritos ao mundo virtual, ou seja, condutas nunca vistas antes.

Sobre o tema, discorre Aldemário Araújo Castro (2003):

Os tais "crimes de informática" são classificados de diversas formas. Destacamos as duas mais utilizadas. Existiriam os crimes de informática próprios e os impróprios. Os primeiros são aqueles que somente podem ser efetivados por intermédio de computadores ou sistemas de informática, sendo impraticável a realização da conduta por outros meios. Já os qualificados como impróprios admitem a prática por diversos meios, inclusive os meios informáticos.

Dessa forma, infere-se que, além de instituir uma nova modalidade de crimes, o advento da Internet também potencializou alguns já existentes.

É o caso, por exemplo, da pornografia infantil. Este crime, tipificado no art. 241 do Estatuto da Criança e do Adolescente já existe e é punido há alguns anos. Com a Internet, a divulgação da pornografia passou a se dar também através do computador, das salas de bate-papo online e de meios afins, ou seja, esta foi utilizada como mais uma ferramenta para auxiliar o cometimento do crime.

Neste caso, os crimes serão enquadrados conforme o tipo penal já existente, não existindo óbice quanto à sua tipificação, visto que ocorrerá da mesma maneira dos demais crimes praticados que incidem no artigo 241 do Estatuto da Criança e do Adolescente, havendo inovação tão somente no meio utilizado para sua prática.

Porém, em contrapartida, outros crimes foram instituídos com a própria Internet. É o caso, por exemplo, do roubo ou dano a dados online, que não possui previsão legal e surgiu com o advento da própria Internet. Sobre esta modalidade de crimes é que há maior preocupação, visto que, diante das lacunas normativas, não há a punibilidade adequada, e, por consequência, a prevenção a estes crimes. Nessa esteira de entendimento, está Demócrito Filho:

Para alguns, os chamados "crimes informáticos" são apenas uma faceta de realidades já conhecidas, crimes e condutas já tipificadas em sua definição material que apenas são cometidos com o auxílio de outros recursos (os

elementos informáticos). A grande verdade, porém, é que determinadas condutas surgidas nesses ambientes são inteiramente novas, e não guardam relação ou similitude com tipos já descritos na lei atual, havendo uma necessidade de sua reformulação para "acompanhar os novos tempos – a Era Digital”.

No caso concreto, um indivíduo que foi pego em flagrante destruindo e danificando dados de uma empresa que constavam em CDs com o intuito de prejudicá-la será enquadrado apenas no art. 163 do Código Penal, em que diz: “Destruir, inutilizar ou deteriorar coisa alheia: pena – detenção, de um a seis meses, ou multa”.

Sabe-se que o Direito Penal não pode punir pessoas virtuais e abstratas, havendo a necessidade de identificação de um infrator fixo para que haja a punibilidade deste, visto que, nos delitos em estudo, há uma ausência física do autor do crime, sendo este identificado, inicialmente, no âmbito virtual.

Diante disso, no que diz respeito aos sujeitos que participam dessa modalidade de crime, Rogério Sanches Cunha discorre sobre o sujeito ativo: “Sujeito ativo do crime é a pessoa que pratica a infração penal. Qualquer pessoa física capaz e com 18 (dezoito) anos completos pode ser sujeito ativo de crime.” (2016, p. 154).

No crime em estudo, o sujeito ativo é aquele que utiliza-se da Internet, como ferramenta ou meio para atentar contra um bem juridicamente protegido, podendo ser a privacidade, a imagem, a honra, etc.

Porém, ante o caráter virtual deste tipo de crime, a identidade do sujeito ativo está protegida pela criptografia, visto que as transações da Internet são realizadas através de chaves. Assim, nem sempre é possível identificar o sujeito ativo deste crime, ou para identificá-lo, são necessários maiores recursos.

Nesse sentido, os crimes virtuais encontram mais um impasse: identificar seus infratores. Isso porque, diante da mobilidade de informações em curto espaço de tempo, os dados se proferem e acabam por se afastar daquele que os pôs em circulação.

Ainda há, também, outro óbice: carência de recursos para identificá-los. Muitas vezes, os autores dos crimes são pessoas que possuem alto conhecimento técnico acerca dos recursos da Internet, enquanto que o Brasil ainda é um país carente em tecnologias que tenham efetividade para identificá-los.

Assim, grande parte das vítimas tem certa descrença na apuração destes crimes, visto que não são de fácil verificação, necessitando de tecnologia, profissionais com conhecimento técnico na área e, em alguns casos, demandando tempo. Dessa forma, permanecem em silêncio, o que aponta mais uma das barreiras enfrentadas para a prevenção destes crimes.

No que diz respeito ao sujeito passivo, lecionam André Estefam e Victor Eduardo Rios Gonçalves: “O sujeito passivo (material ou eventual) é o titular do bem jurídico protegido pela norma penal” (2012, p.184).

No caso do crime em estudo, o sujeito passivo é o titular do bem jurídico contra o qual alguém atenta por meio da Internet.

Discorre Gouvêa sobre o tema:

Hoje em dia, entretanto, não se pode restringir a tutela para determinados agentes. Assim como qualquer pessoa pode praticar crimes por meio da informática, qualquer um pode ser vítima. Qualquer usuário pode ter seus programas destruídos por vírus, ou ter o número do cartão de crédito interceptado em redes de computadores, pois está ocorrendo uma verdadeira “democratização” destes crimes. (GOUVÊA, 1997, p. 61)

Assim, qualquer pessoa que tenha acesso à rede, através de computadores, tablets, celulares, smartphones, está sujeito a ser vítima da ação de um agente lesionador.

Porém, no que tange ao objeto tutelado pelo ordenamento jurídico, ou seja, o bem jurídico que está sendo ameaçado ou prejudicado, há de se observar qual tipo de crime está se configurando. A título de exemplo, deve-se verificar: se há invasão a sites, roubo de dados, o objeto jurídico tutelado é a privacidade. Se, por outro lado, são divulgadas fotos pornográficas sem autorização, o bem jurídico ferido é a honra e a imagem da vítima. Se há roubo de senhas de bancos, o bem ameaçado é o patrimônio da vítima.

Desta feita, a determinação do objeto se dará apenas com a identificação do caso concreto, só podendo ser determinado de forma geral e a título de exemplificação.

2 A PUNIBILIDADE DOS CRIMES INFORMÁTICOS E A TEORIA DAS JANELAS QUEBRADAS

Segundo o art. 5º, inciso II da Constituição Federal, ninguém é obrigado a fazer ou deixar de fazer nada, senão em virtude da lei. Ainda neste sentido, o art. 1º do Código Penal dispõe sobre esta mesma temática, quando anuncia “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”.

Tais disposições supramencionadas dizem respeito ao princípio da legalidade, no âmbito do Direito Penal. Este princípio tem como escopo limitar a atuação estatal na vida privada dos indivíduos, estabelecendo limites de interferência, sendo estes delimitados pela lei. Ou seja, o indivíduo só se obrigará com aquilo que estiver disposto em lei. Fora desses parâmetros, o Estado não poderá interferir, conferindo segurança jurídica aos cidadãos e coibindo ilegalidades e abusos.

A respeito do tema, leciona Rogério Sanches:

Conhecido em latim como *nullum crimen, nulla poena sine lege*, é mandamento revestido de maior importância num Estado Democrático de Direito, servindo como determinante à subordinação de todos à imperatividade da lei, limitando inclusive o exercício do poder pelo governante. (2016, p. 83)

Também sobre esta temática, contribui Alexandre de Moraes:

O art. 5º, II, da CF preceitua que ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei. Tal princípio visa combater o poder arbitrário do Estado. Só por meio das espécies normativas (CF, art. 59) devidamente elaboradas, conforme regras de processo legislativo constitucional, podem se criar obrigações para o indivíduo, pois são expressão da vontade geral. Com o primado da lei, cessa o privilégio da vontade caprichosa do detentor do poder em benefício da lei. (2007, p. 97)

Desta forma, como bem esclarecem os doutrinadores, esse princípio é crucial para determinar a área de atuação do governante, proibindo o exercício do poder arbitrário e garantindo a liberdade dos indivíduos.

Como é cediço, o princípio da legalidade se aplica a diversas áreas do direito. Porém, especialmente no Direito Penal, tem uma conotação específica, como regulamenta o próprio artigo 1º do Código Penal, já mencionado. Segundo esse dispositivo legal, não haverá crime se não houver lei anterior que o defina.

Assim, segundo o princípio, não basta apenas que a infração penal seja instituída na lei, mas esta deve ser anterior ao fato, ou seja, deve estar escrita (CUNHA, 2016, p.84).

É o que diz Ferreira sobre o tema: “O conceito de ação abrange qualquer comportamento humano, positivo ou omissivo, desde que seja típico, ou seja, corresponda ao modelo previsto na lei como crime, com a respectiva penalidade, atendendo-se ao princípio *nullum crimen nulla poena sine lege*.” (FERREIRA, 2000, p. 211)

Indispensável também, nesse contexto, compreender o conceito interpretativo das leis penais referentes à analogia, que se trata de uma interpretação extensiva, em que “o intérprete amplia o significado de uma palavra para alcançar o real significado da norma” (CUNHA, 2016, p. 61). Dessa forma, na analogia, são enquadradas algumas condutas em determinados tipos penais, de acordo com uma interpretação ampla.

No que tange ao princípio da legalidade e à analogia, há distintas opiniões acerca do tema. Porém, como decidido pelo Superior Tribunal de Justiça, no que diz respeito à lei penal, a analogia não pode ser utilizada se tem o condão de prejudicar o réu:

O princípio da estrita legalidade impede a interpretação extensiva para ampliar o objeto descrito na lei penal. Na medida em que as multas não se inserem no conceito de tributo é defeso considerar que sua cobrança, ainda

que eventualmente indevida - quer pelo meio empregado quer pela sua não incidência - tenha o condão de configurar o delito de excesso de exação, sob pena de violação do princípio da legalidade, consagrado no artigo 5º, XXXIX da Constituição Federal e artigo 1º do Código Penal. (STJ- Sexta Turma- REsp 4 76.315- Rei. Ministro Celso Limongi (des. convocado)- DJe 22/02/2010).

Dessa forma, com relação aos crimes virtuais, à legalidade e à analogia, tem-se dois tipos de crimes, como já mencionado no presente artigo. Os crimes impróprios, que são aqueles que já têm sua tipificação no Código Penal, não necessitam de uma tipificação específica com relação ao uso de instrumentos como a Internet, pois estes já se encontram descritos na lei penal.

Este é o entendimento do Supremo Tribunal Federal, no julgamento de Habeas Corpus 76689, ao tratar do caso de adolescentes de quinze anos que incluíram fotos de crianças e adolescentes na rede, nus, em práticas sexuais. Contra o argumento de que não existe previsão legal no ordenamento jurídico brasileiro que proíba a inclusão de pornografia na rede, tem-se a decisão do R. Juízo:

(...) Crime de Computador: publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte.

1. O tipo cogitado - na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" - ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador.

2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.

3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial. (STF - HC: 76689 PB, Relator: SEPÚLVEDA PERTENCE, Data de Julgamento: 22/09/1998, Primeira Turma, Data de Publicação: DJ 06-11-1998 PP-00003 EMENT VOL-01930-01 PP-00070)

Assim, não é necessário que seja utilizada a interpretação ampla, posto que estes crimes já são enquadrados num tipo penal, e sua prática se estendeu ao campo virtual, não deixando, entretanto, de ser a mesma prática já tipificada.

Porém, em relação à outra modalidade, os crimes próprios, tem-se um problema: a sociedade avança, os meios tecnológicos avançam ainda mais, tendo em vista a velocidade e eficiência dos criadores e desenvolvedores de sistemas, redes e tecnologias em criar a cada minuto inovações, enquanto que o legislador encontra-se parado no tempo, fazendo com que as normas se tornem obsoletas em relação à realidade atual.

Dessa forma, como explanado, se estes novos crimes não possuem codificação, não pode ser utilizada a analogia para enquadrá-los, visto que, sem lei anterior, não há crime. Isto porque, em razão da sua especialidade, os bens jurídicos ofendidos não possuem proteção da norma, ou, se possuem, esta não é adequada, não podendo receber a devida punição, ainda que estas infrações venham a prejudicar grandemente um indivíduo.

Sendo assim, acaba que, por fim, o agente não recebe a punição necessária a promover o controle social e evitar as reiteradas condutas, resultando no crescimento de ocorrências destes crimes e restando a sensação de impunidade.

Em face disso, importante é destacar uma teoria que será abordada no presente trabalho, a Teoria das Janelas Quebradas (OLIVEIRA, 2014). Segundo esta teoria, que consiste, em síntese, na afirmação de que desordem gera desordem, a ação humana está relacionada ao meio social em que este se insere.

A Teoria das Janelas Quebradas foi desenvolvida em Chicago, pelos estudiosos americanos James Q. Wilson e George Kelling. Com o auxílio da Universidade de Stanford (EUA), os referidos pesquisadores realizaram testes visando embasar sua teoria, deixando, em locais diferentes, dois veículos idênticos parados durante algumas semanas.

O ponto significativo dessa ação se deu em razão dos carros terem sido deixados em bairros distintos, ficando um em um bairro economicamente inferior, e o outro em um bairro economicamente superior.

Assim, na primeira semana o veículo que se encontrava em bairro nobre permaneceu intacto, enquanto que o veículo localizado em bairro mais humilde foi encontrado danificado, tendo sido objeto de furtos, sujeira e suas peças avariadas.

Dessa forma, foi procedido outro experimento: no carro deixado em um bairro tranquilo e rico, foram quebradas as janelas para verificar qual seria a repercussão de tal ato. O resultado foi semelhante ao carro deixado em zona pobre e de conflitos, o veículo foi encontrado nas mesmas condições, objetos furtados e automóvel danificado.

Com isto, os pesquisadores concluíram que existe uma íntima relação de causalidade entre desordem e criminalidade: o mesmo veículo que permaneceu por dias intocável, quando aparentou estar em descuido, desordem e desleixo, ganhou as mesmas repercussões de fato

que o outro que se encontrava em zona conflituosa. Constatou-se, assim, que o ser humano é movido pelas relações no meio em que se encontra.

Nessa esteira, evidenciou-se que, para combater a criminalidade, é necessário que haja combate, na mesma forma e proporção, da microcriminalidade e da macrocriminalidade. Isto porque, pequenos delitos desencadeiam maiores, que, por conseguinte, podem ser evitados.

Com relação ao tema, colaciona-se jurisprudência do R. Tribunal de Justiça do Estado de São Paulo, proferida em Recurso de Sentido Estrito nº 0018910-29.2009.8.26.0077 em que a teoria em discussão foi aplicada ao caso concreto:

EMENTA: RECURSO EM SENTIDO ESTRITO - REJEIÇÃO DE DENÚNCIA - ACOLHIMENTO DO PRINCÍPIO DA INSIGNIFICÂNCIA - DISSENSO JURISPRUDENCIAL QUE NÃO AUTORIZA O ACOLHIMENTO DA TESE ADOTADA - CONTRAPOSIÇÃO DO POSICIONAMENTO PELA ADOÇÃO DA TEORIA DA JANELA QUEBRADA - PRETENSÃO MINISTERIAL ACOLHIDA E DETERMINAÇÃO PARA SEGUIMENTO DA AÇÃO PENAL EM SEUS ULTERIORES TERMOS RECURSO PROVIDO.

A causa supralegal porque não prevista em lei há que ser reconhecida pelo aplicador do direito com prudência. Destarte, como se olvidar da “Teoria das janelas quebradas no Direito Penal”. Ora, tal orientação vem se disseminando, sendo ligada à criminologia, ciência auxiliar do Direito Penal, e que o socorre para identificação de fatores conducentes à prática de crime. E em que consistiu tal experiência guindada à alçada de teoria auxiliar do Direito Penal? Com efeito, o estudo foi desenvolvido para verificar se pobreza é fator estimulante ao crime. Destarte, dois automotores foram colocados em bairros distintos, um de classe abastada e outro em periferia pobre. Aqui houve danificação imediata, com pronta subtração de peças e acessórios. Ao outro nada ocorreu, de sorte que a inicial conclusão advinda do estudo desenvolvido foi no sentido de que pobreza, de fato, é fator estimulante ao crime.

O estudo aqui não estagnou e por tal razão é que se tornou teoria que ganha relevância. O veículo do bairro abastado, em complemento à pesquisa, teve então seus vidros quebrados para se apurar a consequência. E, apurou-se, que no bairro de classe econômica alta, quando o veículo foi deixado com a janela quebrada, ocorreu também a subtração de peças e objetos em seu interior.

Daí segue a inelutável conclusão: não é só pobreza fator conducente à criminalidade, ou seja, à prática de infrações penais, mas também impunidade e sua crença quando se está diante de crimes de pequena gravidade. A este teor, com a devida vênia, há que se repudiar a aplicação do princípio da insignificância para inúmeros fatos típicos porque, desta forma, estimula-se a reiteração criminosa.

Portanto, ainda que o delito não tenha gravidade exacerbada, há que se punir, sob pena de estimular crimes mais graves. Em suma, delitos mais graves e condutas criminosas mais gravosas surgem em sociedades em que crimes pequenos ou menores não são punidos. De feito, nada obstante se deva reconhecer existência de flagrante divergência que alimenta o

entendimento aqui expandido, é caso de prosseguimento da ação penal, mormente porque a coisa subtraída é uma utilidade para seu proprietário, mesmo quando de menor expressão econômica.

Conforme brilhante entendimento da Teoria das Janelas Quebradas e aplicação dela ao caso concreto, analisa-se a ligação do tema com o estudo dos crimes virtuais.

Sabe-se que estes ainda possuem pouca visibilidade, por não se caracterizarem, aos olhos da sociedade, como crimes tão ofensivos como aqueles praticados pessoalmente. Porém, o equívoco se encontra justamente no fato de que tais crimes são tão lesivos quanto aqueles, mas, para isso se utilizam de uma perigosa ferramenta, o que os torna ainda mais difíceis de combater: a tecnologia.

Sendo assim, o principal fato trazido em questão se trata de, em razão da não aplicação da lei frente a estes casos de menor potencial, estes virem não apenas a se realizar, mas também a se tornar crimes maiores .

Ou seja, o perigo resultante da não punibilidade ou da punibilidade branda desses crimes, não adequada ao caso concreto, é o de que estes venham a e reiterar cada vez mais, banalizando sua ocorrência.

Dessa forma, o que se propõe é que a lei já existente no Brasil se adequue, de forma a possibilitar a responsabilização dos agentes que fazem uso destes meios telemáticos de práticas criminosas, e não necessariamente que seja criada uma nova legislação especial que trate apenas destes crimes, visto que, em alguns casos as leis existentes podem se adequar.

Porém, diante das lacunas normativas, o Direito brasileiro tem o dever de supri-las, tendo em vista que, no âmbito Internacional, diversos países já uniformizaram a aplicação da lei a estes casos criando dispositivos que tratam da temática.

É o caso, por exemplo, da Convenção de Budapeste, Conselho da Europa, em que os países membros estudam meios de evitar a ocorrência destes crimes, bem como a criação de medidas necessárias para evitá-lo, inclusive legislativas.

O Peru, como outro exemplo, incluiu em seu próprio código penal medidas contemplando os crimes virtuais. O mesmo também ocorre no Chile, visto que este país já possui legislação específica acerca do tema, enquanto os EUA também possuem inúmeras leis sobre os estes aspectos. Além desses países, muitos outros já têm suas adaptações para que não haja impunidade frente a estes determinados crimes, enquanto que o Brasil, como desenvolvido no tópico anterior, possui pouca codificação e alguns projetos de lei.

Assim, ante a dificuldade de enquadrar as condutas em tipos penais, para que seja possível a prevenção de crimes cibernéticos, o avanço legislativo dessa matéria, o

investimento em tecnologia e a capacitação de órgãos e agentes para combater e elucidar os crimes são ferramentas imperiosas e indispensáveis, e que podem tornar, um dia, possíveis a supressão desses tipos de conduta.

3 O PROCESSO JUDICIAL PARA PUNIÇÃO DOS CRIMES CIBERNÉTICOS E A SOLUÇÃO PARA AS LACUNAS NORMATIVAS DO BRASIL.

Como já demonstrado, torna-se preocupante o processo de punição dos autores de crimes cibernéticos. Isto porque, os crimes próprios, como explanado anteriormente, tratam-se de uma modalidade de infrações inovadoras, que vieram à tona com o advento da Internet.

Essa preocupação se dá em razão, basicamente, de dois fatores: o primeiro deles é a escassez de denúncias. Sobre isso, argumenta Corrêa:

(...) Talvez o pequeno número de casos submetidos à polícia e a nossos tribunais faça com que a habilidade técnica para “fechar o cerco” a tais “crimes” deixe a desejar. Isso é preocupante, pois, como demonstrado anteriormente, a tendência é o aumento qualitativo e quantitativo de tais ilícitos. (CORRÊA, 2010, p.91)

Dessa forma, torna-se cada vez mais difícil o aperfeiçoamento de normas que se enquadrem a estes crimes, bem como sua investigação, visto que essas transgressões são deixadas, por diversas vezes, no silêncio.

Outro aspecto desafiante para os aplicadores do Direito Penal é a questão da investigação de tais crimes. Isso porque, a grande ausência de evidências contra o agressor, a dificuldade na detecção para encontrá-lo, a escassez de evidências, a carência de tecnologias e equipamentos adequados no Brasil, e a adversidade para definir o local do crime são diversos obstáculos à apuração destas condutas.

Percebe-se, também, que esse aspecto está intimamente ligado ao primeiro, sendo a escassez de denúncias uma consequência direta das adversidades encontradas na investigação de tais crimes. Corrêa, em brilhante colocação, explana nesse mesmo sentido: “(...) pelo fato do crime ser ‘perfeito’, a vítima não reportaria o fato à polícia; assim, as autoridades não iriam desconfiar de algo sem evidências e aparentemente sem vítimas.” (CORRÊA, 2010, p. 92).

Há, ainda, um terceiro aspecto, que também possui ligação direta com os anteriores: a prevenção. Isso porque, em razão da ausência de denúncias, da dificuldade na investigação, consequentemente estes crimes não experimentarão a prevenção, tendo muito mais chances de se reiterar por diversas vezes, tendo em vista que os infratores não temem por punições.

Neste sentido, entra um quarto e último aspecto: a carência legislativa. Isto se dá em razão de, pela dificuldade de enquadramento das referidas condutas, e como o Direito Penal não pode enquadrar uma conduta em um tipo penal por analogia para prejudicar o réu, as punições a este crime se dão de forma branda.

Ou seja, há enorme dificuldade em constatar a existência do crime e identificar o agente causador. Porém, quando todas essas etapas são concluídas e se obtém sucesso em levar o causador do dano à justiça, este é julgado com enquadramento em crimes que, por sua vez, não são suficientes ante as condutas praticadas e aos danos gerados.

Diante dessas considerações, traz-se ao estudo uma pesquisa realizada pela empresa Sysmantec, fabricante de softwares de segurança, denominada “Relatório de Crimes Cibernéticos NORTON: O impacto humano.”

Nessa pesquisa, foram entrevistados mais de 7.000 adultos de 14 países (Austrália, Brasil, Canadá, China, França, Alemanha, Índia, Itália, Japão, Nova Zelândia, Espanha, Suécia, Reino Unido, EUA), considerando como crimes cibernéticos: vírus/malware de computador; fraude de cartão de crédito online; pirataria (hacking) online; assédio online; roubo de identidade online; golpes online (por exemplo., sorteios fraudulentos/oportunidades de emprego); assédio sexual e phishing online.

Segundo esse relatório, no Brasil, 6 em cada 10 computadores são vítimas de algum crime cibernético. Na pesquisa, o cenário atual é definido como uma “epidemia digital global silenciosa”, por defender que a maioria das pessoas no mundo já foi vítima desses crimes, se sente impotente perante eles e não os denuncia, fazendo com que fiquem em silêncio. Para corroborar tal afirmativa, traz dados relativos a 79% das pessoas do mundo não acreditam que um criminoso virtual vai ser levado à justiça.

No relatório, ainda, são mencionados termos como “impotência apreendida” para fazer referência à paralisação em que as vítimas desse crime se submetem, tendo em vista que não tomam atitudes que visem solucionar os problemas que decorrem de lesões online.

A pesquisa traz também o dado de que, no Brasil, são levados, em média, 48 dias para solucionar um crime dessa espécie, além do custeio para esses procedimentos serem bastante dispendiosos.

Sendo assim, ante os dados trazidos pela pesquisa realizada pela empresa Sysmantec acima exposta, embora haja uma margem de erro de 5%, sendo o nível de confiança das informações por ele prestadas estimado em 95% segundo o próprio relatório, resta demonstrado que os crimes virtuais no Brasil causam grande inquietação às vítimas, seja pela

impotência em que estas sentem, ou pela descrença gerada pelo próprio sistema brasileiro e pela característica anônima no uso da Rede.

Assim, no que diz respeito ao processo judicial para julgamento desses crimes, como já explanado, este encontra inúmeras adversidades para ocorrer.

Ressalte-se ainda que, quando esses crimes são levados à justiça, depara-se com o óbice do seu enquadramento penal.

É o que ocorre, a título de exemplo, no Revenge Porn (Pornografia de Vingança). Este “crime” – pois não possui tipificação específica – se caracteriza como sendo a exposição de fotos íntimas sem o consentimento da vítima por meio da Rede. Surgido no âmbito de ascensão da Internet, tornou-se cada vez mais comum no meio virtual, e teve crescimento significativo nos últimos anos.

Ressalte-se o caráter perverso dessa prática, haja vista que é capaz de causar danos irreparáveis à vida da vítima. Desperta sentimentos como impotência, vergonha, constrangimento e ofende profundamente a intimidade da pessoa que foi lesada.

Porém, no que diz respeito à mencionada conduta, o agente é punido, em diversos casos, através de um enquadramento por adequação no Código Penal, como sendo o crime de difamação, exposto no art. 139 deste dispositivo, com pena de detenção de três meses a um ano, e multa.

Assim, fica claro que, em relação ao sofrimento experimentado pela vítima, essa punição se encontra desproporcional e destoante da realidade. Esse fato ocorre porque os tribunais estão, diante de cada caso em espécie, buscando uma solução que pareça justa.

Porém, essa tarefa não cabe aos juízes. Em razão da omissão legislativa, sobra aos magistrados o árduo papel de legislar quando são colocados frente a casos concretos.

É certo que diante a própria necessidade, o Brasil promulgou a Lei 12.737/12, conhecida Lei Carolina Dieckmann, devido à invasão ao computador da atriz brasileira, com roubo de dados e mídias, que acabaram por viralizar na Internet.

Embora essa lei represente o reconhecimento da necessidade de regulamentação de tais ilícitos e um avanço legislativo na matéria, em face das necessidades concretas do Brasil, o referido dispositivo ainda é insuficiente para abraçar as condutas realizadas no país.

Assim, chega-se a um impasse: como punir essas condutas, diante da carência legislativa brasileira? E mais: uma legislação sobre essa temática seria eficaz para diminuição dos crimes?

Para alguns, uma tipificação penal desses crimes não é a solução, por representar um mais um acúmulo de normas penais. Aury Lopes Júnior (2001), em artigo, critica inclusive a

política de tolerância zero e a Teoria das Janelas Quebradas, fazendo comentários em que esclarece que a tipificação de crimes não diminui sua ocorrência e condena a repressão aos pequenos delitos.

O referido autor critica a pena de prisão, por não acreditar que no país esta seja eficaz, pois não ressocializa e não educa os apenados. Critica também o Brasil, afirmando que caminha para o chamado “Direito Penal Simbólico”, composto por diversas leis e presídios cheios, mas não combate a criminalidade.

Há também o fato de que no Brasil opera o Princípio da Insignificância e da intervenção mínima, em que o Direito Penal deve ser *ultima ratio*.

Demonstrando um caso em que houve rejeição do Princípio da Insignificância, colaciona-se parte do Acórdão TJSP - RSE 0018910-29.2009.8.26.0077, Rel. Des. Euvaldo Chaib, DJ. 22.02.2011, seguindo o mesmo entendimento aqui explanado, no sentido de estimular os crimes:

Portanto, ainda que o delito não tenha gravidade exacerbada, há que se punir, sob pena de estimular crimes mais graves. Em suma, delitos mais graves e condutas criminosas mais gravosas surgem em sociedades em que crimes pequenos ou menores não são punidos. De feito, nada obstante se deva reconhecer existência de flagrante divergência que alimenta o entendimento aqui expendido, é caso de prosseguimento da ação penal, mormente porque a coisa subtraída é uma utilidade para seu proprietário, mesmo quando de menor expressão econômica.

Assim, ainda que a prisão no Brasil não cumpra seu papel efetivo, deve-se ter em mente que, no caso dos crimes virtuais, estes não podem ser considerados como “menos ofensivos” que os demais, tendo em vista que têm as mesmas consequências no mundo real e na vida das pessoas, afetando-as da mesma forma e lesando bens juridicamente protegidos.

Porém, o que se defende no presente trabalho não é uma política de tolerância zero, com embasamento de que a punição para os crimes virtuais é unicamente necessária para coibi-los. Também não é defeso que seja necessária a criação de uma lei unicamente voltada para todos os crimes virtuais, tendo em vista a impossibilidade e a morosidade desse processo.

O que realmente é destacado é a necessidade de resposta estatal para esses crimes. As vítimas não podem ficar sem amparo e estas não devem permanecer em silêncio e descrentes.

Uma dessas soluções seria, inicialmente, o investimento em recursos para apurá-los. Isto porque, como já mencionado alhures, além de ser altamente custosa e dispendiosa a identificação do infrator, o Brasil não possui recursos rápidos e eficazes. Dessa forma, o investimento em tecnologias adequadas teria grande caráter repressivo, visto que diversos agressores em todo país temeriam por suas identidades reveladas.

Outra possível solução estudada – e mais eficaz e viável – é a questão de tratados internacionais. Isso porque, em razão da territorialidade, por a Internet não possuir um local fixo e este ser mundial e virtual, tornam-se necessárias políticas de apoio mútuo e cooperação recíproca entre os países, para que os agressores não fiquem fora da competência brasileira e saiam ilesos.

A Convenção de Budapeste é um ponto importante a ser avaliado. Essa convenção se trata, em síntese, de um tratado de prevenção e combate aos crimes praticados na Internet ou com o uso do computador em que 56 países do mundo são signatários.

O tratado visa obter cooperação entre os membros, para adotar medidas legislativas que busquem a prevenção destes crimes, bem como o seu combate. Em seu teor, engloba diversas modalidades de crimes virtuais, dando auxílio inclusive tecnológico e informático para seus membros.

Sendo assim, tendo em vista tudo que foi explanado no trabalho, o ingresso do Brasil à referida Convenção de Budapeste parece, por hora, ser a solução mais viável no combate aos crimes virtuais no Brasil e em resposta à carência legislativa do país.

Isto porque, em razão do processo legislativo no Brasil ser amplamente moroso, necessitar de diversas peculiaridades, da decadência do sistema jurídico brasileiro e dos legisladores do país, uma lei específica tratando do tema não passaria apenas de utopia.

CONSIDERAÇÕES FINAIS

A Internet experimentou um amplo crescimento nos últimos anos. Com isso, o número de usuários também cresceu consideravelmente, fazendo com que os crimes cibernéticos surgissem no âmbito virtual.

Para regular tais relações, tem-se o Direito Digital: uma modalidade do Direito própria para analisar e regular o comportamento humano frente ao mundo virtual, visto que nem sempre essas relações se dão de forma benéfica.

Frente a isso, tem-se o conceito de Crimes Cibernéticos, como sendo infrações penais a bens juridicamente tutelados pelo Estado, como a privacidade, honra, imagem, etc. A peculiaridade destas transgressões é que ocorrem no meio virtual, ou seja, são crimes que necessitam de um meio eletrônico para que se concretize.

Sobre eles, podem ser classificados em duas modalidades: próprios e impróprios. Os primeiros são aqueles que nasceram juntamente com o advento da Internet. Já os segundos são crimes já existentes, mas que a Internet veio a potencializá-los.

Nesse ponto, fica caracterizado o desafio para o país: enquanto que os crimes impróprios já vêm sendo punidos, pois já possuem tipificação penal, os impróprios não têm seu enquadramento legal, recebendo punições brandas ou até deixando os seus infratores ilesos.

Isso porque, o Brasil não acompanhou a evolução tecnológica da Internet em dois aspectos: no jurídico, visto que não possui legislação capaz de enquadrar todos os crimes virtuais; e no da própria informática, visto que não possui recursos eficazes para captá-los.

Assim, no que diz respeito a esses aspectos, tanto em relação à omissão legislativa como também em relação à carência de tecnologias, há consequências diretas na sociedade, fazendo com que haja descrença da população acerca da resolução desses crimes, tornando, conseqüentemente, as denúncias cada vez mais raras.

Em relação aos infratores, esses também não possuem temor algum. Em razão da ausência de punibilidade ou da punibilidade branda, os infratores acreditam que a Internet é “terra de ninguém”. Assim, as sanções aplicadas não têm caráter preventivo.

Porém, diante da realidade brasileira, a criação de uma lei específica para regular tais crimes se trata de uma ideia utópica, tendo em vista os diversos fatores que contribuem para sua impossibilidade.

Desta feita, para que os crimes cibernéticos não permanecem em silêncio e que não seja permitida a reiteração criminosa no Brasil, devem ser feitos investimentos na tecnologia para captar a ocorrência de tais crimes, bem como identificar seus infratores.

Há também a necessidade da repressão para essa modalidade de conduta, sendo viável ao Brasil ser signatário da Convenção de Budapeste, tratado internacional que visa o combate aos crimes cibernéticos através da ajuda mútua entre os membros e do reconhecimento de diversas espécies de crimes cibernéticos, para efetivamente identificá-los e puni-los.

REFERÊNCIAS

ALMEIDA FILHO, José Carlos de Araújo. **Direito Eletrônico ou Direito da Informática: Informática Pública**. Vol. 7, 2005. Disponível em: <http://www.ip.pbh.gov.br/ANO7_N2_PDF/IP7N2_almeida.pdf>. Acesso em agosto de 2017.

BARRET, Neil. **Digital Crime**. London: Kogan Page, 1997.

CARVALHO, Salo de. **A ferida narcísica do direito penal: primeiras observações sobre as (dis)funções do controle penal na sociedade contemporânea**. In: GAUER, Ruth M. Chittó (Org.). Rio de Janeiro: Lumen Júris, 2004. p. 179-211.

CASTRO, Aldemario Araújo. **Internet e os Tipos Penais que Reclamam Ação Criminosa em Público**. In: Webly. Disponível em <<http://www.webly.com.br/forum/lofiversion/index.php/t11293.html>>. Acesso em agosto de 2017.

CINTRA, Antônio Carlos de Araújo; DINAMARCO, Cândido Rangel; GRINOVER, Ada Pellegrini. **Teoria Geral do Processo**. 3ª Ed. São Paulo: Revista dos Tribunais, 1991.

CONVENÇÃO SOBRE O CIBERCRIME. Disponível em: <http://ccji.pgr.mpf.gov.br/documentos/docs_documentos/convencao_cibercrime.pdf>. Acesso em: 13 de fevereiro de 2018.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da Internet**. 5ª Ed. São Paulo: Saraiva, 2010.

CUNHA, Rogério Sanches. **Manual de Direito Penal: Parte Geral**. 4ª Edição. Salvador: JusPODIVM, 2016.

DAOUN, Alexandre Jean.; BLUM, Renato Opice. Cybercrimes. In: LUCCA, N.; SIMÃO FILHO, A. (coord.). **Direito e internet: aspectos jurídicos relevantes**. Bauru: Edipro, 2000.

ESTEFAM, André; GONÇALVES, Victor Eduardo Rios. **Direito Penal Esquematizado: Parte Geral**. Coord. Pedro Lenza. São Paulo : Saraiva, 2012.

FERREIRA, Ivette Senise. A criminalidade informática. In: LUCCA, N.; SIMÃO FILHO, A. (coord.). **Direito e internet: aspectos jurídicos relevantes**. Bauru: Edipro, 2000.

FILHO, Demócrito Reinaldo. O projeto de lei sobre crimes tecnológicos (Pl nº 84/99). Disponível em: <<http://jus.com.br/revista/texto/5447/o-projeto-de-lei-sobre-crimes-tecnologicos-pl-no-84-99>> Acesso em: out. 2017.

GOMES, Helton Simões. G1. **Pela 1ª vez, acesso à Internet chega a 50% das casas no Brasil, diz pesquisa**. Set/2015. Disponível em: <<http://g1.globo.com/tecnologia/noticia/2015/09/pela-1-vez-acesso-internet-chega-50-das-casas-no-brasil-diz-pesquisa.html>> Acesso em agosto de 2017.

INELLAS, Gabriel Cesar Zaccaria. Crimes na internet. São Paulo: Editora Juarez de Oliveira, 2004.

LOPES JR, Aury. Violência urbana e tolerância zero: Verdades e mentira. In: Âmbito Jurídico, Rio Grande, II, n. 5, maio 2001. Disponível em: <<http://www.ambito->

juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=5805>. Acesso em outubro de 2017.

MÁYNEZ, Eduardo García. **Introducción al Estudio del Derecho**. 12ª Edição. México: Editorial Porrúa S.A, 1964.

MORAES, Alexandre de. **Direitos Humanos Fundamentais: Teoria geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência**. 8ª Ed. São Paulo: Saraiva, 2007.

NADER, Paulo. **Introdução ao Estudo do Direito**. 36ª Edição. Rio de Janeiro: Editora Forense, 2014.

OLIVEIRA, Aparecida do Carmo Prezotti de. **Teoria das janelas quebradas**. Revista Vinna Jr. mar. de 2014. Disponível em: <http://www.viannajr.edu.br/files/uploads/20140502_172228.pdf>. Acesso em: 24 de maio de 2017.

PAESANI, Liliana Minardi. **Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil**. 6ª Edição. São Paulo: Atlas, 2013.

RECURSO EM SENTIDO ESTRITO nº 0018910-29.2009.8.26.0077; Comarca: BIRIGÜÍ - (Processo nº 077.01.2009.018910-6/000000-000); Juízo de Origem: 2ª Vara Criminal; Órgão Julgador: 4ª Câmara de Direito Criminal; Recorrente: Ministério Público do Estado de São Paulo; Recorrido: Delmiro Francisco Nogueira.

ROSA, Fabrizio. **Crimes de Informática**. 2ª edição. Campinas: Bookseller, 2006.

SYSMANTEC. **Relatórios de Crimes Cibernéticos NORTON: O impacto humano**. Disponível em: http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_Portuguese-Human%20Impact-A4_Aug18.pdf

TJSP – RSE 0018910-29.2009.8.26.0077, Rel. Des. Euvaldo Chaib, DJ. 22.02.2011.

STF - HC: 76689 PB, Relator: SEPÚLVEDA PERTENCE, Data de Julgamento: 22/09/1998, Primeira Turma, Data de Publicação: DJ 06-11-1998 PP-00003 EMENT VOL-01930-01 PP-00070.

STJ- Sexta Turma- REsp 4 76.315- Rei. Ministro Celso Limongi (des. convocado)- DJe 22/02/2010.