

CRIMES DIGITAIS: UM ESTUDO DA LEGISLAÇÃO BRASILEIRA

Lisiane Rosa Magalhães ⁽¹⁾
(Sandresson Menezes) ⁽²⁾

RESUMO

Este artigo tem por objetivo, sem esgotar o tema, demonstrar a evolução e os desafios enfrentados pelo direito penal brasileiro em sua aplicação na área digital. Inicia-se por uma análise dos principais aspectos dos crimes digitais, formando uma visão geral dos conceitos necessários para o entendimento desse fenômeno recente da criminalidade. Faz-se uma apresentação das diversas abordagens no direito penal brasileiro e analisa-se mais detalhadamente a Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet. Logrou-se, deste modo, tratar de um tema atual e demonstrar sua importância no âmbito do Direito Penal. Por fim, para cumprir a formalidade científica e acadêmica, utilizou-se os métodos e práticas científicas adequadas ao caso real, portanto, esta pesquisa desenvolveu-se com base no método indutivo, utilizando-se a pesquisa bibliográfica e documental complementada e comparada com a observação da realidade concreta.

Palavras Chaves: Crimes digitais. Marco civil brasileiro.

1 INTRODUÇÃO

Com o advento da Revolução digital, as novas tecnologias alteram cada vez mais a forma com que o cotidiano se desenvolve na sociedade mundial. Desde as ações mais básicas, como a comunicação entre os cidadãos, até as mais complexas são constantemente alteradas pelo surgimento de alternativas tecnológicas para se realizar a mesma atividade.

A popularização do computador desencadeou o acesso à informática a um número maior de pessoas e conseqüentemente, à rede mundial de computadores. Novos hábitos surgiram e, com eles, novos valores e realidades modernizadas. Ressalta-se que todos os setores da sociedade foram drasticamente impactados e se tornaram dependentes das novas tecnologias, em especial dos programas de computadores.

¹ Acadêmica do Curso de Direito da UNI-RN

Email: lisiane.r.magalhaes@gmail.com

² Professor Orientador do Curso de Direito

Segundo Luiz Augusto Azevedo: os programas de computadores possibilitaram o desenvolvimento de inúmeros setores da economia mundial, além de permitir maior conforto e agilidade para o homem, sendo uma das mais relevantes criações no campo científico-tecnológico.

No âmbito do acesso e troca de informação, a internet tem um papel de suma importância, tornando-se uma das principais ferramentas que possibilitou as mudanças drásticas no cenário atual. Seu advento foi um dos principais fatores responsáveis pela reformulação cultural e estrutural da sociedade, seja em âmbito mundial, seja em âmbito nacional. A internet pode ser definida como um aglomerado de redes em escala mundial de milhões de dispositivos interligados pelo protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol*) que permite o acesso e a transferência de informações infinitas.

Com a evolução da interação entre tecnologia e sociedade, surge a concepção da sociedade da informação, onde essas novas relações virtualizadas e informatizadas criam a necessidade de que novas normas jurídicas sejam criadas a fim de proporcionar a devida regulamentação desse fenômeno social.

Assim, surgiu em meados dos anos 90, o Direito Eletrônico que através de estudos e correntes doutrinárias, visa a normatização jurídica das relações que envolvem a informática como fator primário e a regulamentação dos direitos e deveres consequentes dos meios de comunicação existentes na informática e no âmbito virtual. Por oportuno, apresenta-se a definição de Lobato Paiva para o direito digital:

“é a ciência que estuda a utilização dos elementos físicos, eletrônicos, como o computador, no Direito; isto é, a ajuda que este uso presta ao desenvolvimento e aplicação do Direito. Em outras palavras, é o instrumento necessário à utilização da informática no Direito”.

Ressalta-se que o direito digital é considerado um ramo autônomo atípico da ciência jurídica e pela sua relevância atual, outros ramos do Direito como o Direito constitucional, civil e penal se relacionam com o mesmo. Para o presente estudo, é de maior relevância a interação entre o Direito Penal e o Direito eletrônico.

Para Pinheiro (2009, p. 8):

“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.”

Não resta dúvida que com a ampliação da utilização da internet pela sociedade, a sua relevância social e econômica se tornou maior, e por conseguinte foram criadas novas formas de condutas criminosas. A importância da relação entre o Direito Penal e o direito eletrônico é tão grande que alguns acreditam, principalmente os doutrinadores de origem alemã, que exista uma subespécie do Direito Eletrônico que seria o Direito Penal Informático. Em se tratando da legislação pátria, percebe-se que essa relação ainda é escassa e evolui lentamente, deixando lacunas em vários parâmetros importantes, como exemplo, a jurisdição.

No entanto, o presente trabalho ressalta que já existiam suficientes tipificações para a maioria dos casos dos crimes digitais na legislação brasileira vigente, utilizando-se do entendimento que os crimes reais eram correlatos aos virtuais. Assim, para a caracterização dos crimes, a hermenêutica jurídica era utilizada a fim de possibilitar a interpretação e aplicação das normas legais já existentes, como exemplo, subtrair dados informáticos poderia ser considerado furto; invadir sistemas para obter vantagem econômica, estelionato, entre outros.

O que se objetiva é discutir sobre a necessidade de estudos e adequações que entendam o funcionamento das novas tecnologias e as alterações funcionais derivadas dessas constatações. Assim, em face das mudanças recentes na legislação específica aos crimes virtuais, e diante da realidade complexa da sociedade da informação, se faz necessária a discussão sobre o direito penal e sua adequação às novas condutas ilícitas praticadas no ambiente virtual, levando em conta o binômio liberdade-controle.

2. CRIMES DIGITAIS.

Segundo Alexandre DAOUN: O crime informático, é conceituado como uma ação típica, antijurídica e culpável, ao qual o termo “informático” consubstancia apenas um plus.

Já a definição de crime informático de Ivette Senise Ferreira explica que é: “toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão”. Ressalta-se que o crime informático pode ser denominado por várias nomenclaturas como crime virtual, cibernético, digital, cibercrime, entre outros.

Para uma melhor compreensão da evolução do crime digital, se faz necessário ter uma noção histórica do assunto. Através de uma breve análise da literatura científica internacional, verifica-se que os primeiros sinais da incidência desse tipo de crime foram registrados nos anos 60, na época dos estudos que levariam ao surgimento da internet, manifestando-se em sua maioria em casos de manipulação e sabotagem de computadores. Já nos anos 70, época em que o protocolo TCP/IP era utilizado por um número pequeno de usuários, surgiu a figura do *hacker* e por consequência, a ampliação da diversidade de crimes digitais, com o aparecimento da invasão de sistema e furto de software. A partir dos anos 80, através da difusão da internet pelo mundo, as ações criminosas virtuais se diversificaram e aumentaram na rede, com a manipulação de contas bancárias, pirataria digital, propagação de vírus, disseminação de conteúdos ligados a pornografia infantil, entre outros.

Logo, surgiu uma reação natural e esperada, a sociedade até então prejudicada gradativamente, reivindicou a punição das ações criminosas anteriormente citadas, surgindo concomitantemente a necessidade de proteção dos novos bens jurídicos criados pelo advento da informática. Assim, houve a criação do Direito Penal Informático, que passou a estudar a nova criminalidade bem como buscar formas para a sua prevenção.

Na legislação pátria, que é o foco principal desse trabalho, verifica-se que na Constituição Federal de 1988 é possível encontrar leis relativas à competência do Estado sobre questões de informática, porém a preocupação com a regulamentação

específica do âmbito virtual é recente. A legislação possui uma maior abrangência em termos de tipificação, no entanto possui uma grande escassez de regulamentação jurídica em outros aspectos como no inquérito, no processo e na jurisdição. Logo, se há lei mas não há aparelhamento e conhecimento necessários para amparar todo o processo investigatório, fica evidente que a aplicação da lei se torna ineficiente.

2.1 A CLASSIFICAÇÃO DOS CRIMES DIGITAIS:

Os crimes digitais, como já dito, podem receber diversas outras nomenclaturas como: crimes virtuais, cibernéticos, entre outros. A doutrina brasileira diverge quanto à nomenclatura de classificação desse tipo de crime, diferenciando em: crimes digitais próprios e impróprios, crimes digitais puros e impuros, entre outros.

Através da análise de jurisprudência recente e da doutrina, a classificação adotada nesse trabalho é a que divide crimes digitais próprios e impróprios.

Os crimes digitais próprios são aqueles em que o agente utiliza a informática como meio e fim da ação criminosa. A informática é o bem jurídico tutelado. Segundo Crespo:

“Os Crimes Virtuais Próprios figuram condutas delituosas dirigidas contra o próprio computador enquanto elemento físico, ou seja, são as condutas que acabam por ferir bens jurídicos inerentes à própria informática, que consistem contra dados, informações ou estruturas a ele interligados, e assim, os bens jurídicos tutelados são primordialmente os sistemas informatizados ou de telecomunicações ou dados.”

Como exemplos de crimes digitais cita-se os que atentam contra a inviolabilidade do hardware, software, banco de dados, sistemas operacionais, entre outros.

Os crimes digitais impróprios são aqueles comuns, que atualmente são cometidos por intermédio do computador. O detalhe a que deve se atentar na qualificação desse tipo de crime, é que o computador ou dispositivo conectado à internet foi utilizado apenas como meio de efetuar a ação criminosa. Os exemplos de crimes digitais impróprios são: crimes contra a honra, cyberbullying, envio de mensagens bancárias falsas através de e-mails, entre outros.

Por oportuno, colaciona-se ementa de jurisprudência recente:

recurso em sentido estrito. crimes contra a honra. civil em face de militar da ativa. crime de informática comum. declinação da competência. justiça federal. não ocorrência justiça militar da união. competência para julgar os crimes militares definidos em lei. previsão constitucional.

A Magna Carta, em seu art. 124, apesar de não especificar a matéria a ser julgada pela Justiça Castrense, prescreve que a ela compete processar e julgar os crimes militares definidos em lei, utilizando o critério *ratione legis*. Nesses termos, deixou ao alvedrio da legislação infraconstitucional a delimitação de sua jurisdição. A esta especializada Justiça não cabe julgar os integrantes das Forças Armadas, mas sim os agentes que tenham sido denunciados pela prática dos crimes militares definidos na legislação penal castrense, incluindo os civis. Trata-se de crime de informática impróprio ou comum, uma vez que os crimes de calúnia, difamação ou injúria podem ser praticados por qualquer meio, seja ele eletrônico ou não. In casu, a consumação do crime configurou-se no momento em que o Comandante da Base Aérea de Fortaleza e os demais militares tomaram conhecimento do conteúdo da mensagem postada eletronicamente, fato ocorrido no interior do aquartelamento. RECURSO PROVIDO. DECISÃO UNÂNIME. (GRIFEI)

(STM - RSE: 478920117100010 CE 0000047-89.2011.7.10.0010, Relator: Maria Elizabeth Guimarães Teixeira Rocha, Data de Julgamento: 11/12/2012, Data de Publicação: 06/02/2013 Vol: Veículo: DJE),”

Ressalta-se ainda a existência de classificação em crimes digitais mistos. São aqueles em que há a prática de crimes digitais próprios e impróprios na mesma conduta. Um exemplo desse tipo de crime, verifica-se no art. 72 do Código Eleitoral, que determina pena de cinco a dez anos de reclusão, ao agente que obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, com o objetivo de alterar a apuração ou contagem de votos.

Como ressalta o artigo 4º da Lei Orgânica dos Partidos Políticos: “A ação do partido será exercida, dentro de seu programa, em nome dos cidadãos que integram e sem vinculação com a ação de partidos ou governos estrangeiros”. (BRASIL, Lei nº4.740, de 15 de julho de 1965, 1965).

2.2 SUJEITOS DO CRIME DIGITAL:

2.2.1 Sujeito Ativo:

O Sujeito ativo do crime digital não difere daquele do crime comum, ou seja, é a pessoa que pratica a conduta típica e pode ser responsabilizada pelo crime em caso de conduta que também seja ilícita e culpável. Ressalta-se que a investigação da autoria do fato na realidade virtual é essencial, vez que o autor nesse tipo de crime pode se utilizar de várias artimanhas para encobrir sua real identidade, como clonagem ou invasão de contas e senhas.

Assim, no âmbito virtual, o sujeito ativo da ação criminosa possui características singulares. Não só por se tratar de um agente que geralmente possui um conhecimento técnico avançado, já que existem vários tipos de sistemas de segurança eletrônica. A identificação do agente se dá de forma diferenciada devido ao *modus operandi* ser necessariamente através de algum dispositivo ligado em rede. Portanto além da identificação visual, qualitativa, habitual nos crimes comuns, é necessário também a identificação numérica que formará o sujeito virtual, como por exemplo, o número do IP e *host*.

Nery (2003, pg. 50/62), diferencia os agentes de ações criminosas virtuais mais comuns pelos seus objetivos, eles são:

a) Hackers

Os Hackers são especialistas em informática, desde um administrador de sistemas até um adolescente, que se diverte acabando com a rede. Eles procuram defeitos nos sistemas operacionais e programas e quando os descobrem por vezes os avisam aos fabricantes. Eles não estão incluídos como criminosos digitais, mas muitas vezes sua imagem é distorcida pela mídia. Nery (2003, pg. 50/62)

b) Crakers

Os Crakers são criminosos, e agem normalmente em grupos, são movidos pela fama e pelo dinheiro. Procuram brechas para invadir redes e roubar dados, disseminam vírus, destroem sistemas e computadores, deformam páginas da Web, e escrevem códigos maliciosos para invasão automática (spyware). Normalmente são os mais temidos da rede. Nery (2003, pg. 50/62).

c) Carders

Criminosos solitários que causam o aumento do número de crimes por computador. Normalmente se especializam em criar programas que geram ou roubam números de cartões de crédito para conseguir dinheiro, comprar pela internet, ou até mesmo extorsão, mediante o nome e endereço das vítimas. Nery (2003, pg. 50/62)

d) Phreakers

Também são criminosos, só que especializados em telefonia. Entre as suas principais atividades estão incluídas as ligações gratuitas (locais e interurbanas), reprogramação de centrais telefônicas, instalação de escutas. Nery, David César; 2003. O prejuízo causado pelos phreakes no Brasil gira em torno de 2% do faturamento das operadoras de telefones móvel, algo em torno de US\$ 15 bilhões. Nery, David César; 2003 apud módulo 2004.

e) Insiders maliciosos

O Insider é uma pessoa que tem acesso a informações sigilosas em uma determinada organização. Portanto um insider malicioso é um aversário traiçoeiro e perigoso, pois já está dentro do sistema e pode ignorar defesas em torno dele. Muitas vezes corrompe o próprio sistema para o seu próprio fim. Conhece a estrutura organizacional (podendo ser um empregado, contratado ou um consultor) e sabe como seria conduzida uma investigação contra suas ações. Nery (2003, pg. 50/62)

f) Espionagem Industrial

Normalmente é motivada para obter vantagens sobre a concorrência, através do roubo de segredos profissionais dos concorrentes. A espionagem industrial começa onde a técnica de investigação passa a ser ilegal e a inteligência competitiva termina. Nery (2003, pg., David César; 2003)

2.2.2 Sujeito passivo:

O sujeito passivo do crime digital é quem sofre a lesão, o dano pela ação criminosa. Diante da evolução histórica dos crimes virtuais, fica evidente que com a disseminação da internet, houve uma grande diversificação das possíveis vítimas. Hoje em dia, não são só as pessoas físicas e jurídicas de direito privado que dependem da internet. O sistema judiciário brasileiro está em processo de plena informatização

visando a celeridade processual e a redução do consumo de papel e diversos outros órgãos públicos dependem de tecnologia, em especial da internet, para o funcionamento integral de suas atividades.

O processo judicial Eletrônico (PJe) pode ser considerado como um marco na implementação das novas tecnologias na máquina judiciária. Segundo informações do site oficial do CNJ:

“Desde o dia 3 de fevereiro de 2014, o Conselho Nacional de Justiça (CNJ) está utilizando exclusivamente o Processo Judicial Eletrônico (PJe) para o trâmite de novos processos. Este é o primeiro passo para a migração dos processos em andamento do sistema e-CNJ para o PJe, sistema desenvolvido pelo CNJ em parceria com os tribunais e a participação da Ordem dos Advogados do Brasil (OAB) para a automação do Judiciário. O objetivo principal do CNJ é manter um sistema de processo judicial eletrônico capaz de permitir a prática de atos processuais, assim como o acompanhamento desse processo judicial, independentemente de o processo tramitar na Justiça Federal, na Justiça dos Estados, na Justiça Militar dos Estados e na Justiça do Trabalho.”

Para a utilização do PJe é necessária a certificação digital de advogados, magistrados, servidores ou partes que precisarem atuar nos novos processos, tornando todos esses profissionais dependentes das novas tecnologias.

Em se tratando de outros órgãos brasileiros, a Receita Federal pode ser citada pela importância de seus sistemas eletrônicos e virtuais.

Para se ter uma noção de como os crimes digitais são corriqueiros no âmbito público, segundo um relatório publicado pela RSA, divisão de segurança da EMC (multinacional americana de tecnologia), sobre o assunto, o Brasil foi citado como um dos oito países com o maior número de corporações como vítimas de fraudes virtuais em fevereiro de 2013, junto a países como Reino Unido, Estados Unidos e Canadá, que possuem legislação específica e rigorosa contra os criminosos cibernéticos.

No campo do direito privado, destacam-se os sistemas virtuais disponibilizados pelos bancos aos seus clientes, que permitem a realização de várias operações exclusivamente pela internet como transferência de valores, contratação de empréstimos, entre outros, e todos são alvos constantes de crimes digitais.

Com relação á pessoas físicas, os crimes mais comuns são os que acontecem nas redes sociais e nos e-mails. As ofensas pessoais virtuais tomaram papel de destaque na mídia e tornaram-se o centro de discussões sobre o fenômeno denominado de cyberbullying ou bullying virtual. Para uma melhor compreensão sobre o tema, transcreve-se um trecho retirado de um site especializado:

“BULLYING virtual, ocorre nos meios eletrônicos, com mensagens difamatórias ou ameaçadoras circulando por emails, sites e blogs. É quase uma extensão do que ocorre na escola só que essas pessoas não estão cara a cara, dessa forma o anonimato pode aumentar a crueldade dos comentários e das ameaças e os efeitos podem ser tão graves, gerando na vítima sintomas psicológicos graves podendo levar a depressão ou suicídio. Esse tormento que a agressão pela internet faz com que a criança ou o adolescente humilhado não se sinta mais seguro em lugar algum, em momento algum. “

Outros exemplos de crimes digitais mais comuns são: Furto de dados, envio de spam, pirataria digital, entre outros.

Portanto, tomando como base a vulnerabilidade em que a sociedade se encontra e as graves consequências das ações criminosas virtuais, é necessário que o sistema penal brasileiro se adeque a nova realidade e cumpra seu papel de reduzir os danos em relação aos usuários através da busca da máxima eficácia de um sistema de garantias mínimas.

2.3 CRIMES DIGITAIS: JURISDIÇÃO E COMPETÊNCIA

Precipuamente utiliza-se a definição de jurisdição de Francesco Carnelutti: [...] é conceito oposto e complementar à ação; a ação é uma atividade que se desenvolve da periferia para o centro; a jurisdição, do centro para a periferia; a ação vai das partes ou, mais amplamente, até os cidadãos. A jurisdição penal é uma espécie da jurisdição em geral; é a jurisdição que se manifesta no processo penal mediante a comprovação do delito e a aplicação da pena.”

Assim a jurisdição é o poder que o Estado tem para impor as regras jurídicas, o direito, no caso concreto. A jurisdição é exercida através dos juizes e tribunais e a sua aplicação é limitada pela competência (material e funcional) de cada órgão jurisdicional.

Ressalta-se que a interferência na jurisdição de um Estado implica na interferência de sua soberania.

A análise da jurisdição e competência das leis brasileiras e suas delimitações em relação aos crimes digitais é de suma importância vez que, a utilização das novas tecnologias já abordadas ao longo desse trabalho revelam que os atos criminosos digitais, especialmente os virtuais, podem gerar consequências ao mesmo tempo em vários lugares diferentes do país e do mundo. Diante dessa característica de transnacionalidade dos crimes virtuais e do ciberespaço, há dificuldades em delimitar a jurisdição e a competência exatas de cada Estado e os limites da aplicação da lei penal no tempo e no espaço. Nesse sentido há a distinção entre os delitos que ocorrem em vários locais, mas inseridos apenas dentro do território brasileiro, esses são denominados de delitos plurilocais, já aqueles que ocorrem em países diferentes são denominados de crimes à distância.

Enquanto a jurisprudência não possui um consenso quanto à teoria aplicável para a fixação do foro, o entendimento acerca da competência da Justiça Federal para julgar os delitos informáticos é praticamente uniforme, restando a justiça Estadual a competência residual. Ressalta-se que o entendimento é que de acordo com o inciso V do artigo 109 da Constituição Federal, a competência é da Justiça Federal quando há a ofensa de bens, serviços ou interesses da União ou o delito esteja previsto em tratado ou convenção internacional, e não pelo modo ou meio como foi praticado, ou seja, não é porque foi praticado através internet que possui o âmbito internacional, veja-se:

PROCESSO PENAL. CRIME CONTRA A HONRA DE MENOR PRATICADO VIA INTERNET. ORKUT. PORNOGRAFIA INFANTOJUVENIL. ART. 16 DA CONVENÇÃO SOBRE OS DIREITOS DA CRIANÇA. DECRETO 99.710/1990. ART. 241-A DA LEI 8.069/1990. COMPETÊNCIA DA JUSTIÇA FEDERAL. ART. 109, INCISO V, DA CF/1988. RECURSO PROVIDO. I - A teor do disposto no art. 109, inciso V, da Constituição Federal/1988, compete aos juízes federais processar e julgar os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente. II - Tendo em vista ser o Brasil signatário da Convenção sobre os Direitos da Criança e diante da antevisão da transnacionalidade de crime praticado contra a honra de menor, consistente na veiculação, via internet, de fotografias contendo pornografia infantojuvenil, a competência para processar e julgar o presente feito é da Justiça Federal. Precedentes. III - Recurso em sentido

Em se tratando de território nacional há três teorias que são indicadas pela doutrina acerca do local do crime: a teoria da atividade, a teoria do resultado e a teoria mista ou da ubiqüidade.

A diferença entre as duas primeiras teorias é simples, vez que essas são excludentes entre si, ou seja, a teoria da atividade define que o lugar do crime é aquele em que ocorreu a ação ou omissão e ignora para a classificação, o lugar do resultado. Já a teoria do resultado, ignora o lugar da ação ou omissão e define o local do crime como aquele em que efetivamente ocorreu o resultado. No nosso ordenamento pátrio é a teoria da ubiqüidade ou mista que é aplicada, verificada no art. 6º do Código Penal: “Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado”, possibilitando que a legislação brasileira seja aplicável mesmo nos casos em que apenas um dos vários atos do delito, aconteça em território nacional.

Em se tratando dos crimes a distância, verifica-se que o art. 70 do Código de Processo Penal estabelece:

“§ 1º. Se, iniciada a execução no território nacional, a infração se consumir fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.

§ 2º. Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.

§ 3º. Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção.”

Logo, a legislação brasileira é responsável para tratar de todos os crimes ocorridos no solo nacional, mesmo que se tratando de iter criminis, atentando-se aos acordos e deliberações internacionais sobre o tema. Assim se o Brasil se tornasse signatário de uma convenção específica sobre crimes cibernéticos (como exemplo: a convenção de Budapeste), além da repercussão e destaque mundial no

desenvolvimento de políticas diplomáticas, seria um importante passo para dirimir os conflitos legislativos nos casos de crimes à distância. Sendo assim, evidencia-se que em termos de jurisdição e competência em questões que envolvem apenas o território nacional, as teorias aplicadas resolvem de maneira satisfatória os casos concretos, restando lacunas e carência de segurança jurídica nos casos que envolvam o Brasil e outros países.

3 OS CRIMES DIGITAIS E AS LEIS NO BRASIL.

3.1 O DIREITO PENAL INFORMÁTICO

No Brasil, o Direito penal informático é uma área em recente evolução, no ano de 2012, com a entrada em vigor das Leis 12.735 e 12.737 houve a regulamentação penal de normas específicas sobre os crimes digitais próprios e somente agora em 2014, foi sancionado o marco civil da internet, lei que estipulou regulamentações e aspectos importantes como os direitos considerados princípios da internet no Brasil, se tornando uma espécie de “Constituição da Internet”.

A seguir são explicitadas, de forma geral, as modificações trazidas pela legislação referente aos crimes digitais:

a) Lei no 9.296, de 24 de junho de 1996:

Regulamenta a interceptação de comunicações telefônicas, criminalizando a conduta consistente em realizar interceptação de comunicações telefônicas, de informática ou telemática ou quebra de segredo de justiça com pena de dois a quatro anos e multa.

b) Lei nº 9.609, de 19 de fevereiro de 1.998:

Dispõe sobre a propriedade intelectual de programa de computador e sua comercialização. Criminaliza a conduta consistente em violar direito do autor de programa de computador, atribuindo-lhe pena de seis meses a dois anos de detenção ou multa, e de um a quatro anos de reclusão e multa se a finalidade for comercial.

c) Lei no 9.983, de 14 de julho de 2000:

Legislação que altera dispositivos do Código Penal. Dentre aqueles ligados à informática, a norma criou o parágrafo 1º A, do artigo 153, criminalizando a divulgação de informações sigilosas ou reservadas, contidas ou não nos sistemas de informações ou bancos de dados da Administração Pública. Criou ainda os artigos 313, A e 313, B, que, respectivamente, criminalizam a inserção de dados falsos em sistema de informações e a modificação ou alteração não autorizada de sistema de informações. Acrescentou o parágrafo primeiro ao artigo 325 criminalizando, em seu primeiro inciso, a conduta de permitir ou facilitar mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, acesso de pessoas não autorizadas a sistemas de informação ou banco de dados da Administração Pública. No inciso seguinte pune também aquele que se utiliza do acesso restrito.

d) Lei no 11.829, de 25 de novembro de 2008:

Altera dispositivos do Estatuto da Criança e do Adolescente. Acrescenta o artigo 241-A que criminaliza oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo explícito ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

e) Lei nº 12.735, de 30 de novembro de 2012:

Originada pelo Projeto de Lei 84/1999 (PL 89/2003) e apelidada de Lei “Azeredo” por ter um projeto substitutivo do Senado Federal da antiga redação elaborado pelo então senador Eduardo Azeredo. Apesar do veto presidencial em grande parte da proposta, a lei em questão alterou o Código Penal e o Código Penal Militar, para tipificar condutas realizadas mediante sistema eletrônico, a legislação tratou de forma mais clara os atos de racismo por meio eletrônico, reforçando o Estatuto da Igualdade Racial e determinou a criação de setores especializados nas polícias civis dos estados e do DF para a investigação e combate aos crimes cibernéticos.

f) Lei nº 12.737, de 30 de novembro de 2012:

Originada de um Projeto de Lei em tramitação há muito tempo no Congresso Nacional, recebeu o apelido de “Lei Carolina Dickmann” por ter sua aprovação acelerada em virtude da repercussão na mídia de um caso em que a atriz em questão

alegou que algumas fotos íntimas foram roubadas de seu computador pessoal e espalhadas na internet. Essa lei forneceu a tipificação de vários delitos cometidos pela internet, foi publicada em novembro de 2012 e após 120 dias, período de vacatio legis, entrou em vigor. Destaca-se a inserção dos artigos 154-A a 154B ao Código Penal, inseridos nos crimes contra a liberdade individual, seção referente aos crimes contra a inviolabilidade dos segredos profissionais, criminalizando a invasão de um dispositivo eletrônico com a intenção de acesso, alteração ou destruição dos dados e informações protegidas. Assim a invasão de dados em computadores passou a ser considerada como um crime punível com multa e prisão. No entanto, para a invasão ser um crime, a lei estabelece que a invasão não deve ser autorizada, nem tacitamente e que por outro lado, é obrigação do titular dos dados a imposição de medidas protetivas de tais dados.

Ressalta-se que a maioria dos delitos tratados na lei já encontravam previsão em outros delitos presentes no Código Penal e já havia jurisprudência que consolidava as punições, entretanto essa não é a maior crítica da doutrina em relação a essa lei. Fato é que por se tratar de tecnologias novas, de complicadas definições técnicas, as expressões utilizadas na lei deram abertura para diversas interpretações. Além do mais verifica-se que as punições estipuladas seguiram o caminho oposto da tendência internacional, se tratando de punições leves e moderadas.

Ressalta-se, ainda, que os crimes digitais podem possuir o potencial de lesividade maior em relação aos crimes correlatos que se consumam no plano físico, pela extensão e rapidez com que as informações são trocadas no mundo virtual e pela dificuldade da total remoção dessas informação da rede.

Por fim, destaca-se que segundo a pesquisa “O Comportamento dos Usuários na Internet” realizada pela Fecomercio/SP no ano de 2014: 86,2% na cidade de São Paulo considera que a Lei nº 12.737/2012, não será suficiente para o combate aos crimes virtuais.

3.2 MARCO CIVIL DA INTERNET:

Em 24 de abril desse ano foi publicada a Lei nº 12.965, de 23 de abril de 2014, que instituiu o “marco civil da internet”. Proveniente do projeto de lei 84/99, que tratava das primeiras regulações sobre crimes praticados na internet, o qual foi rechaçado e apelidado à época de “AI 5 Digital”, logo foi alterado diversas vezes, resultando no projeto de lei 126/2011 que foi enviado pelo Executivo para apreciação do Legislativo em 2011. Desde então se manteve estagnado devido aos impasses entre oposição e governo. O deputado Alessandro Moron (PT-RJ) se tornou o relator do projeto de lei do Marco Civil. Assim, após anos de lentidão, voltou à tona após o vazamento de informações e provas que a agência norte-americana NSA está fazendo uma vigilância massiva aos estados-unidenses e também a diversos países do mundo e, em especial, ao Brasil. Em meio a esse cenário, após negociações políticas, pressão por parte da população e da então presidente Dilma Rouseff, alteração dos pontos mais controversos como a retirada da necessidade dos datacenters no Brasil e diminuição de interferência na questão da neutralidade de rede, o Marco Civil da Internet brasileiro, foi aprovado.

A importância do Marco Civil, Lei 12.965/2014, além da regulamentação de vários aspectos em seus 32 artigos, é de inserir o Brasil em posição de destaque positivo na regulamentação do âmbito virtual apesar de não ser signatário da convenção de Budapeste. A convenção de Budapeste, também conhecida como Convenção sobre o Cibercrime, é um tratado internacional que visa estabelecer uma política criminal e formas de persecução no ciberespaço comuns entre todos os países signatários. Para isso prega a adoção de legislação conforme os preceitos do tratado e cooperação internacional sistematizada. Atualmente os países mais influentes no cenário internacional, como os Estados Unidos, são signatários desse tratado.

O Marco Civil é um orientador sobre a forma de aplicação da legislação referente à internet tanto cível quanto penal, apresentando uma declaração de princípios e conceitos da rede, uma vez que a internet não segue os padrões usuais de regulação das telecomunicações. Destaca-se a importância de quatro parâmetros abordados no texto da lei: a neutralidade da rede, a privacidade do usuários, inimizabilidade da rede e a liberdade de expressão.

Através da neutralidade da rede foi estabelecida a proibição de venda de pacotes de conteúdo diferenciados na internet, proibindo a delimitação de conteúdo ao usuário por parte dos provedores, ou seja, é permitida apenas a comercialização do acesso a rede e em diferentes velocidades, respeitando um dos pilares da internet que é a neutralidade.

Em se tratando da privacidade do usuários, verifica-se que o direito foi garantido em diversos contextos, sendo garantida a inviolabilidade e o sigilo no fluxo de comunicações do usuário através da rede, assim como a Constituição Federal prevê o sigilo telefônico e de correspondências, salvo em caso de ordem judicial. No entanto há críticas da doutrina nesse ponto, pois faltam definições técnicas importantes como o conceito de dado pessoal, o que possibilita que a jurisprudência possa definir e portanto “legislar”, contribuindo para a insegurança jurídica.

Já no caso da inimizabilidade da rede, foi garantida a segurança jurídica para o empreendedorismo, vez que os provedores de acesso à Internet e empresas provedoras de aplicações não podem ser responsabilizados por conteúdos infringentes inseridos por usuários, constituindo-se exceção apenas os casos em que esses provedores não cumprirem ordem judicial para tornar indisponível determinado conteúdo. Verifica-se também nos artigos 18 a 20, a preocupação do legislador com relação aos casos que envolve divulgação de imagens, vídeos e conteúdos de nudez e atos de caráter privado, tornado obrigatória a retirada do ar do conteúdo de forma diligente após notificação pelo próprio participante ou representante legal.

A liberdade de expressão que se tratava de um dos assuntos mais polêmicos abordados pelo Marco Civil, foi assegurada de acordo com a Constituição Federal, sendo necessária a identificação do autor apenas quando há um ato ilícito previsto em lei.

Em contrapartida, o marco civil apresenta carência de definições técnicas e regulamentação prática da investigação criminal digital. Um dos pontos mais controversos diz respeito a criação de reserva de jurisdição para o acesso de dados de provedores da internet conforme previsão contida no artigo 17 do marco civil. De acordo com o Código de processo penal, artigo 6º, III, a autoridade deverá colher todas as

provas que servirem para o esclarecimento do fato e suas circunstâncias. O entendimento da doutrina é que se não houver reserva de jurisdição, o delegado deve usar o poder de requisitar informações mesmo se estiver em poder de terceiros, esse entendimento é compartilhado pela jurisprudência do STF. Ressalta-se ainda que a nova lei de organizações criminosas (lei 12.850/2013), no artigo 15 prevê:

“Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito.”

Através da análise superficial dos dados do cibercrime, fica evidente que as provas são mais voláteis no ambiente virtual, aliada a realidade da justiça brasileira que ainda é a morosidade processual percebe-se que retirar a prerrogativa da requisição direta de dados pelos delegados acabou por permitir um verdadeiro retrocesso para a investigação criminal no Brasil, que nessa área já é deficiente seja pela falta de recursos materiais, tecnologia de ponta, seja pela falta de recursos humanos especializado.

Por fim, falta a legislação complementar de caráter prática e aplicável ao cotidiano, uma vez que há princípios, garantias e tipificações suficientes, faltam leis e investimentos no aparato investigatório. É necessário priorizar a eficiência e garantir que as leis sejam aplicadas de fato para que a impunidade seja exceção e não a regra.

4 CONCLUSÕES.

Ao final deste trabalho, após a verificação da evolução histórica do cibercrime e do consequente surgimento de várias linhas de pensamento do direito digital, se torna evidente que com o avanço tecnológico novos tipos de interações surgiram e consequentemente novas modalidades delitivas.

Vivemos na era digital e os comportamentos sociais que antes eram vistos apenas na sociedade física manifestam-se cada vez mais no mundo virtual. A cada dia o limite entre vida biológica e virtual se torna mais tênue. Com isso surge a necessidade que o Direito se adeque e regule tanto as relações tradicionais quanto as atuais.

Vislumbra-se através da cronologia das leis brasileiras que a internet nunca foi uma terra sem lei, sendo utilizada a hermenêutica jurídica afim de inibir as condutas impróprias e delitos na rede mundial de computadores.

Contudo, a legislação brasileira ainda está em fase de desenvolvimento, assim como o entendimento das novas tecnologias por parte do legislador. O caminho para a obtenção da plena segurança jurídica digital é longo mas vem sendo trilhado respeitando os direitos e garantias já expressos na Carta Magna, como se verifica no Marco Civil, não obstante, ainda que com seus acertos e indiscutíveis avanços, se conclui que essa lei especificamente se trata mais de um marco orientador sobre a forma de aplicação da legislação existente e norteador de princípios e deveres do que uma lei disciplinadora de procedimentos e conteúdo técnico avançado.

Por fim, evidencia-se a necessidade de prosseguimento do avanço no Brasil de legislação especializada, de jurisprudência unificada sobre alguns pontos referentes a jurisdição e competência, de participação em tratados internacionais sobre o assunto e de investimento e avanço na área da investigação criminal virtual, vez que só a letra da lei pura não confere resultados e não inibe as práticas delitivas.

REFERÊNCIAS BIBLIOGRÁFICAS

Análise da Lei carolina dickmann por carlos eduardo Miguel Sobral. disponível em <http://www.emersonwendt.com.br> acesso em 10 abr 14.

CARNELUTTI, Francesco. **Lições sobre o Processo Penal**. Vol.II. Campinas: Bookseller, 2004, p. 147.

Competencia-no-caso-de-crimes-cometidos.html disponível em: <http://www.dizerodireito.com.br/2012/12/> acesso em 23 abr 14.

COSTA, Fernando José da. **Locus Delicti nos crimes informáticos**. Faculdade de Direito da USP. SÃO PAULO. 2011

CRESPO, M. X. F. **Crimes Digitais**. 1 ed. São Paulo: Saraiva, 2011.

Da Persecução Penal dos Crimes Virtuais. Disponível em: http://www.jurisway.org.br/monografias/monografia.asp?id_dh=9903. acesso em 23 abr 14.

DAOUN, Alexandre Jean. **Crimes informáticos**. In: BLUM, Renato M. S. Opice et al. (Coord.). op. cit., p. 203.

FERREIRA, Ivette Senise. **A criminalidade informática**. In: DE LUCCA, Newton; Simão Filho, Adalberto (Coords.). op. cit., v. 2, p. 210.

Nery, David César de Jesus. **A importância do escritório sem papel na segurança da informação**. MBIS 2003, Pag 50 a 62.

<http://www.cnj.jus.br/programas-de-a-a-z/sistemas/processo-judicial-eletronico-pje> acesso em 03 abr 14.

<http://psicologiajuridicaecriminal.blogspot.com.br/> acesso em 03 abr 14.

http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegracodteor=912989&filenome=PL@126/201 acesso em 20 abr 14.

<http://www.conjur.com.br/2012-dez-09/especialistas-lei-crimes-internet-positiva-redundante> acesso em 11 abr 14.

<http://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lei-n-12737-12-art-154-a-do-codigo-penal> acesso em 16 abr de 2014.

Brasil está no TOP 5 das corporações vítimas de fraude digital. Convergência Digital. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=33194&sid=18>>. Acesso em: 12 de abr 14.

<http://congressoemfoco.uol.com.br/noticias/a-importancia-da-lei-de-ciber Crimes/> acesso em 08 abr 14.

<http://josemilagre.com.br/blog/2012/12/03/o-que-muda-com-a-aprovacao-das-leis-de-crimes-informaticos-lei-12-735-e-12-7372012/#more-1803> acesso em 3 abr 14.

<http://www.comunicacaoepolitica.com.br/blog/2014/03/o-marco-civil-e-a-comunicacao-politica-um-historico-de-diferentes-disputas-politicas-e-simbolicas/> acesso em 03 mai 14.

http://pt.wikipedia.org/wiki/Conven%C3%A7%C3%A3o_sobre_o_Cibercrime acesso em 05 mai 14.

<http://trf-1.jusbrasil.com.br/jurisprudencia/24259376/recurso-em-sentido-estrito-rse-440102320124013500-go-0044010-2320124013500-trf1> acesso em 10 abr 14

<http://pt.slideshare.net/tutufischer/vi-congresso-fecomercio-de-crimes-eletrnicos-19052014-apresentao-de-dav-bettspesquisa-crimes-eletrnicos-2014> acesso em 2 abr 14.

<http://www.conjur.com.br/2014-abr-17/marcelo-tostes-marco-civil-internet-traz-avancos-demanda-cautela> acesso em 01 jun 14.

OLIVEIRA, Jôline Cristina de. **O cibercrime e as leis 12.735 e 12.737/2012** disponível em <http://www.conteudojuridico.com.br/pdf/cj045489.pdf>. Acesso em 16 abr 14.

PAIVA, Mário Antônio Lobato de. Primeiras linhas em Direito Eletrônico. In: **Âmbito Jurídico**, Rio Grande, III, n. 11, nov 2002. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=4960>. Acesso em 05 abr 14.

PINHEIRO, Emeline Piva. **Crimes virtuais: uma análise de criminalidade informática e da resposta estatal**. Disponível em: <www.mail.google.com> acesso em 2 abr 14.

SETTE, Luiz Augusto Azevedo. **Dados sobre a proteção jurídica do software no Brasil**. In: BLUM, Renato M. S. Opice et al. (Coord.). **Direito eletrônico: a internet e os tribunais**. Bauru, SP: EDIPRO, 2001. p. 627.

VARGAS, Aline do Vale e RICCI, Camila Milazotto. **Da tipificação dos crimes virtuais**, Disponível em: <http://www.fag.edu.br/> acesso em 10 abr 14.