UNIVERSIDADE PAULISTA
DIREITO

GABRIELA NASCIMENTO OLIVEIRA PEREIRA

CRIMES CIBERNÉTICOS: Uma análise sobre a dificuldade de identificação do criminoso.

São Paulo
2019

GABRIELA NASCIMENTO OLIVEIRA PEREIRA

CRIMES CIBERNÉTICOS: Uma análise sobre a dificuldade de identificação do criminoso.

Trabalho de conclusão de curso para obtenção do título de graduação em Direito, apresentado à Universidade Paulista - UNIP.

Orientador: Prof. Vitor Kundrat

São Paulo
2019

GABRIELA NASCIMENTO OLIVEIRA PEREIRA

CRIMES CIBERNÉTICOS: Uma análise sobre a dificuldade de identificação do criminoso.

Trabalho de conclusão de curso para obtenção do título de graduação em Direito, apresentado à Universidade Paulista - UNIP.

São Paulo, 11 de Novembro de 2019

BANCA EXAMINADORA

Prof. Dr. .....
Universidade .....

Prof. Dr. .....
Universidade .....

Prof. Dr. .....
Universidade .....

Dedico este trabalho ao meu marido, Eduardo, e aos meus filhos, Sophia e Valentim, que são a minha base e não me deixam desistir. Dedico também aos meus pais e a minha avó que foram imprecindíveis na minha criação e me tornou quem eu sou hoje.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus por me capacitar e me dar provisão para a conclusão deste curso;

À minha família, por acreditar em minhas escolhas, apoiando-me e esforçando-se junto a mim, para que eu suprisse todas elas;

E aos meus professores, pela dedicação e incentivo para que eu pudesse desenvolver este trabalho.

"Quanto maior o poder, mais perigoso é o abuso." (Edmund Burke)

RESUMO

Este trabalho tem como propósito apresentar a maneira com que a internet se tornou parte da vida das pessoas e também uma arma na mão dos criminosos. Analisar o conceito dos crimes informáticos e a dificuldade em lidar com eles no âmbito do Direito Penal. Expor exemplos de crimes cibernéticos, alguns já previstos no Código Penal, entretanto, sendo a internet e os dispositivos informáticos um meio para o seu cometimento e, também dividindo-os em crimes informáticos puros, comuns e mistos e próprios e impróprios. Analisar questões processuais inerentes a esse novo tipo de crime e as suas respectivas peculiaridades. Apresentar diferentes interpretações as leis específicas e as suas fragilidades. Expor algumas visões doutrinárias quanto ao conceito de crime cibernético e a necessidade de legislação específica, com foco, especificamente, em sanar/diminuir a dificuldade de apuração da autoria do crime.

Palavras-chave: crimes informáticos; crimes cibernéticos; direito penal; internet; processo penal; lei carolina dieckmann; marco civil da internet

ABSTRACT

This paper aims to present the way the internet has become part of people's lives and also a weapon for criminals. Analyze the concept of computer crimes and the difficulty in dealing with them under criminal law. Expose examples of cyber crimes, some already provided for in the Penal Code, however, with the internet and computer devices being a means to commit them and also dividing them into pure, common and mixed and proper and inappropriate computer crimes. Analyze procedural issues inherent in this new type of crime and its respective peculiarities. Present different interpretations of specific laws and their weaknesses. Expose some doctrinal views on the concept of cyber crime and the need for specific legislation, focusing specifically on remedying / reducing the difficulty of ascertaining the authorship of crime.

Keywords: computer crimes; cyber crimes; criminal law; Internet; criminal proceedings; carolina dieckmann law; internet milestone

SUMÁRIO

1 **INTRODUÇÃO**

A internet, inicialmente uma ferramenta de comunicação militar, evoluiu de maneira global. Hoje, inclusive, é indispensável para determinadas atividades e transformou, por meio de suas facilidades, a vida cotidiana. Muitas das atividades humanas foram englobadas pela automatização em vários setores de produção. A evolução exagerada da internet e dos computadores culminou no surgimento de um universo paralelo e instantâneo: o cyber espaço. Essa facilidade e agilidade trazida por esse novo universo fez com que as redes computacionais se tornassem meio de efetivação de negócios envolvendo valores cada vez maiores. Não só valores monetários, a informação se tornou a verdadeira riqueza.

Essa troca ininterrupta de informação atrai também a criminalidade, pois, a ausência de uma regulamentação e o falso anonimato proporcionado pela grande rede de computadores trouxe consequências negativas. O estudo que aqui será demonstrado tem como objetivo apresentar algumas dificuldades que o legislador encontra acerca dos crimes na internet, assunto atual e que, infelizmente, vem crescendo cada vez mais devido à facilidade de se praticar atos ilícitos nesses meios, sendo acobertado pela dificuldade em identificar a autoria do delito e enquadrar os agentes que o cometem na devida tipificação legal.

Tendo isto em mente, podemos trazer outro ponto, a forma atual de fácil acesso à internet a muitas pessoas leigas e inocentes acessando essas redes, pessoas essas que acabam se descuidando, achando que estão seguras pelo fato de se encontrarem em suas casas, em frente aos seus computadores.

Os ilícitos virtuais não se prendem apenas ao furto ou invasão de privacidade, existem muitos outros crimes na internet, entre esses crimes podemos destacar o comércio sexual, a pedofilia, tráfico, calúnia, difamação, que quando não são cometidos unicamente no meio virtual, são preparados por ele.

É visível o crescente “mercado do incorreto” que vem surgindo na rede mundial de computadores, por isso se faz necessária uma melhor regulamentação desses fatos que em diversos casos são tidos como atípicos. São analisados com dificuldade por conta da falta de transparência em nossa legislação, falta essa compreensível, este moderno uso da internet era impossível de ser previsto à época dos legisladores que promulgaram nosso Código Penal, Constituição Federal e Código de Processo Penal, dificultando uma regulamentação daquilo que não se conhecia à época.

2 **BREVE RELATO SOBRE COMO SURGIU E QUAL A FUNÇÃO DA INTERNET**

A internet surgiu no ano de 1969, nos Estados Unidos, no auge da Guerra Fria. O Departamento de Defesa Americano tinha a intenção de criar uma rede de comunicação entre computadores em pontos estratégicos, a função era interligar laboratórios de pesquisas, descentralizando informações importantes de forma que não fossem destruídas por bombardeiros se estivessem localizadas em apenas um servidor. Naquele ano, foi enviado o primeiro email da história, através de um professor da Universidade da Califórnia para um amigo em Stanford.

Uma subdivisão do Departamento de Defesa, a ARPA - Advanced Research Projects Agency, criou uma rede que possuia estruturas capazes de manipular grandes volumes de informações, conhecidas como "backbone", essa estrutura passava por debaixo da terra dificultando assim sua destruição, essa rede foi chamada de ARPANET.

Os EUA, por temerem o mau uso da tecnologia por civis e países não aliados, no início, restringiu a ARPANET a militares e pesquisadores. Em meados de 1982, o uso da ARPANET tornou-se maior na área acadêmica, depois se expandiu para outros países, como por exemplo, Dinamarca, Suécia e Holanda. A partir dessa expansão, a ARPANET passou a ser chamada de INTERNET, sendo liberado seu uso comercialmente nos EUA no ano de 1987.

Em 1992, com o surgimento de diversas empresas provedoras de acesso a internet, o Laboratório Europeu de Física de Partículas (CERN) criou a WORLD WIDE WEB, conhecida como WWW, que tinha a função de colocar informações ao alcance de qualquer usuário que acessasse a internet.

No Brasil, a internet começou a ser comercializada no ano de 1995, ficando a cargo da iniciativa privida a exploração dos serviços.

Há várias maneiras de trocar e obter informações através da internet, tais como: WWW (World Wide Web), mecanismos de busca, e-mail (correio eletrônico), IRC (Internet Relay Chat), listas de discussão, bate-papos, VoIP (voz sobre IP), mensagens instântaneas e etc. A rede de internet é acessada através de diversos meios, proporcionando a facilidade no processo de troca de comunicação.

A Lei 12.965 de 2014, conhecida como Lei do Marco Civil, a qual será comentada nos próximos tópicos, define internet como:

> Art. 5º Para os efeitos desta Lei, considera-se:
>
> I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

Fabrizio Rosa (2006, pág. 35), conceitua a internet como um conjunto de redes de computadores interligadas pelo mundo inteiro, que têm em comum um conjunto de protocolos e serviços, possuindo a peculiaridade de funcionar pelo sistema de troca de pacotes, ou seja, as mensagens dividem-se em pacotes e cada pacote pode seguir uma rota distinta para chegar ao mesmo ponto.

Por fim, a Internet hoje, é a ferramenta mais utilizada para a comunicação entre pessoas. Ela é usada de diferentes formas: para trabalho, compras, movimentação de contas bancárias, agendamento de viagens e até mesmo para cometer crimes, tema este que será abordado no decorrer deste trabalho.

3 **LIBERDADE DE EXPRESSÃO E ÉTICA NA INTERNET**

A liberdade de expressão na internet é um assunto polêmico onde diferentes posições divergem. Muitos defendem a tese de que a lei não se aplica à internet, e são contra a regulamentação, já outros discutem a inviabilidade da aplicação de qualquer norma ou princípio do Direito e, dizem que a rede é envolvida por um indulto de impunidade, porém, expressam que há dificuldade na eficácia da aplicação de sanções.

No Brasil, a Constituição Federal em seu artigo 5º e 220º, veda expressamente toda e qualquer censura:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
>
> Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.
> § 2º É vedada toda e qualquer censura de natureza política, ideológica e artística.

Sendo assim, a internet é um campo livre para a manifestação de pensamentos, atividades e etc. No entanto, a liberdade da manifestação de pensamento, protegida constitucionalmente, tem seu ônus, uma vez que a própria Constituição, em seu artigo 5º inciso IV, veda o anonimato

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> IV - é livre a manifestação do pensamento, sendo vedado o anonimato;

É necessário que o manifestante se identifique e assuma a autoria do seus atos na internet para que, sendo o caso, seja responsabilizado por eventuais danos causados a terceiros. Porém, é neste ponto que, na maioria das vezes, entra a dificuldade de responsabilização na internet, uma vez que muitos dos atos criminosos são anônimos, sendo difícil a identificação do autor e a aplicação da sanção.

É sabido que, quanto mais atrativo for a atividade criminosa, mais crimes serão cometidos, acredita-se que para combater a criminalidade virtual, é importante que se reduza essa atratividade, ou seja, dificultar o crime aumentando os mecanismos de segurança e difundindo uma formação ética entre os usuários que acessam a internet e, também entre os especialistas do ramo.

Com relação a regulamentação, tendo como ponto de vista essa vulnerabilidade da rede, é necessário estabelecer novas categorias para que haja a possibilidade de diminuição dos crimes e/ou a identificação do autor. É fundamental que o legislador torne mais transparente a responsabilização penal, estabeleça um padrão ético de comportamento para essa ferramenta e, os fornecedores, provedores e etc. invistam em segurança para que haja, ao menos, a possibilidade de identificação da autoria.

Sendo assim, concluímos que é necessário tornar o ambiente informático menos atraente para o crime, para isso a função da ética, transparência na legislação e segurança são imprescindíveis. De acordo com Fabrizio Rosa (2006, pág. 44), algumas regras simples como evitar danos a terceiros; honrar a propriedade; zelar pela privacidade dos outros e etc., podem, ao longo do tempo, contribuir para que haja uma formação cultural e ética, construída pouco a pouco. No entanto, em nosso atual cenário é necessário que as normas jurídicas do "mundo real", sejam também aplicadas ao "mundo virtual".

4 **CRIMES CIBERNÉTICOS**

A OECD - Organização de Cooperação e Desenvolvimento Econômico, em 1983, iniciou uma pesquisa sobre a possibilidade de aplicação de leis em plano internacional, contra os abusos e uso indevido de programas de computadores. Fruto desse estudo surgiu o conceito de crime de informática como sendo "qualquer conduta ilegal não-ética, ou não autorizada que envolva processamento automático de dados e/ou transmissão de dados."[1].

De acordo com o artigo da ECOIT, crime cibernético são:

> atividades ilegais praticadas em ambiente virtual que vão além do roubo de informações financeiras. Utilizam-se de computadores e internet para atingir os mais variados objetivos, seja por meio de uma rede pública, privada ou doméstica.
> A grande diversidade de crimes cometidos engloba infrações que podem atingir um único usuário ou não, assim como podem causar apenas danos em um ou mais computadores.
> Com isso, é possível entender que essas infrações podem ocorrer em um destino isolado ou em vários destinos simultaneamente, o que é muito comum.

Fabrízio Rosa (2006, pág. 58), conceitua crimes cibernéticos com facilidade quando diz que:

> Pode se definir o "crime de informática" como sendo aquela conduta típica, ilícita e culpável, praticada sempre com a utilização de dispositivos de sistemas de processamento ou comunicação de dados, da qual poderá ou não suceder a obtenção de uma vantagem indevida e ilícita.

De uma forma simples e resumida, crimes cibernéticos são crimes reais cometidos no ambiente virtual, através de máquinas/computadores para sua concretização e, que podem ter ou não vantagem ilícita, porém, mesmo com todas as definições e as diferentes abordagens dos doutrinadores quanto ao conceito de crime informático, percebe-se o seguinte consenso: ora o computador é o instrumento do crime, ora o seu objeto.

4.1 EXEMPLO DE CRIMES CIBERNÉTICOS

Conforme mencionado, o computador pode ser tanto o instrumento para o cometimento de crimes, quanto o objeto de um crime, nesse caso, os programas, informações e dados nele contidos. A fim de elucidar melhor o tema sobre crimes cibernéticos, a seguir exemplos de crimes cometidos no âmbito virtual:

---

1 Apud FERREIRA, Ivete Senise. Os crimes de informática. In: BARRA, Rubens Prestes & ANDREUCCI, Ricardo Antunes. Estudos Jurídicos em Homenagem a Manoel Pedro Pimentel. São Paulo: RT, 1992.

a. Danos afetando dados ou programas: Deteriorar, danificar ou suprimir dados e programas, são também bastante conhecidos como vírus;
b. Pichação: Implantar fotos, imagens ou informações indevidas em site de terceiros, sem a autorização;
c. Sabotagem: Interrupção danosa do sistema com o intuito de alterar, entrar, apagar ou suprimir dados;
d. Interceptação não autorizada: Interceptação não autorizada de um sistema ou rede informática;
e. Pirataria: Cópia ilegal de software, reprodução, difusão ou comunicação ao público, sem autorização. O produto, neste caso, é protegido legalmente e, tal conduta já se encontra tipificada no artigo 12 da Lei 9.609/1998;
f. Estelionato: O art. 171 do Código Penal conceitua o crime de estelionato como quando o agente obtém, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento
g. Furto: Cópia ilegal ou criptografia de informações, normalmente com a intenção de obter vantagem pecuniária ilícita. Tipo penal já previsto pelo nosso Código e que tem grande ocorrência no mundo informático devido às inúmeras formas e possibilidades que a internet proporciona. Previsto no art. 155, tem como conduta central a de subtrair para si ou para outrem, coisa alheia móvel.
h. Invasão de dispositivo informático: Crime propriamente informático, o art. 154-A do Código Penal, inserido pela Lei 12.737 de 2012, define como invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
i. Spam: Envio, de forma sistemática, de mensagens não solicitadas por correio eletrônico, que de alguma forma possam causar danos;
j. Divulgação de informações sem autorização: Divulgação de informação, sem justa causa, sem autorização de autoridade competente ou de pessoa interessada. É o famoso caso de divulgação indevida que deu origem a lei conhecida como Lei Carolina Dieckman.

Esse são alguns comportamentos delituosos cometidos no ambiente informático.

4.2 FORMAS DE ATAQUE: MÉTODOS

Fabrízio Rosa (2006, pág: 69) em sua obra "Crimes de informática" cita alguns dos métodos utilizados para a invasão de computadores ou sistemas de informática:

a. Chave Mestra: Uso não autorizado de programas que tendo acesso ao ambiente virtual da vítima modifica, destrói, copia, insere, utiliza ou impede o uso de dados arquivados no sistema.
b. Sniffers: Programas que interceptam informações que circulam pela rede.
c. Cavalo de tróia: Um programa inicialmente útil e ingênuo, mas inclui recursos maliciosos escondidos. Induz a vítima a baixar o programa e após concluído sabotam o sistema.
d. Vírus: Um segmento de programa capaz de mudar a estrutura do software do sistema, destrói e altera dados ou programas.
e. Keylogger: Uma forma de software espião que registra cada batida no teclado ou outra atividade realizada em um sistema, coletando, sem autorização, os dados da vitima.
f. Backdoor: Vulnerabilidade na segurança instalada por um vírus ou cavalo de troia, facilitando o acesso do invasor.

Essas são apenas algumas técnicas e golpes de invasão utilizadas pelos criminosos, desses métodos pode se originar diversos crimes com enquandramento na legislação vigente. É importante salientar que deve ser levado em consideração o dolo, a intenção e a vontade do agente.

4.3 CLASSIFICAÇÕES DOS CRIMES CIBERNÉTICOS

Devido à característica dinâmica dos crimes cibernéticos e da própria internet, as classificações dos crimes cibernéticos devem sempre estar se ajustando às mudanças que tal prática delitiva apresenta no meio virtual. Em que pese a dinamicidade dos crimes virtuais, algumas classificação tendem a se mostram adequadas ao tema em questão, tal como a sugerida por Ivette Senise Ferreira (2005, p. 261), a qual traz a seguinte classificação:

Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as

infrações contra a propriedade imaterial.

Outras duas classificações também despontam na doutrina. A primeira classifica os crimes cibernéticos em puros, mistos e comum, enquanto a segunda divide os crimes de informática em próprios e impróprios.

4.3.1 **CRIMES CIBERNÉTICOS PUROS, MISTOS E COMUM**

Os crimes cibernéticos puros, segundo Costa (1997, p. 03), seriam “toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas.”

No caso acima, o agente visa a atingir especificamente o sistema de informática ou os dados armazenados no referido sistema, tais como as condutas praticadas por crackers, pessoas que utilizam de seu vasto conhecimento informático para invadir sistema com a intenção de causar danos aos sistemas informatizados.

Por outro lado, os crimes cibernéticos mistos, na lição trazida por Pinheiro (2000), “são aqueles em que o uso da internet ou sistema informático é condição sine qua non para a efetivação da conduta, embora o bem jurídico visado seja diverso ao informático.”

Nessa modalidade, o agente não tem como objeto do crime o sistema informatizado ou seus dados, mas se utiliza daquele como instrumento indispensável para a perpetração de sua conduta ilícita, tais como as transferências ilegais por meio do sistema internet-banking.

Por fim, os crimes cibernéticos comuns seriam aqueles em que o objetivo do agente é se utilizar da internet ou sistema de informática para atingir um bem já tutelado penal. Ou seja, a informática é mero instrumento, não indispensável, para a prática delitiva objetivada pelo agente.

4.3.2 **CRIMES CIBERNÉTICOS PRÓPRIOS E IMPRÓPRIOS**

Consoante a lição de Damásio de Jesus (apud ARAS, 2001), crimes cibernéticos próprios ou puros são “aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.”

Segundo tal classificação, os crimes cibernéticos próprios ou puros seriam aqueles em que a utilização do sistema de informática é o meio necessariamente

utilizado para a prática delitiva, a qual, também, necessariamente, objetiva a informática ou seus componentes, sendo estes o objeto jurídico a ser tutelado.

Nessa modalidade, incluem-se os crimes de invasão de sistemas de informação, com o objetivo de danificá-los ou alterá-los, bem como a prática de inserir dados faltos em sistema de dados de informações.

Já os crimes cibernéticos impuros ou impróprios, ainda sob os ensinamentos de Damásio de Jesus (apud ARAS, 2001), são “[..] aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.”

Em suma, os crimes cibernéticos impróprios ou impuros seriam aqueles em que a utilização do sistema de informática trata-se apenas de um novo modus operandi, ou seja, um novo meio de execução, com o qual o agente visa atingir um bem já tutelado penalmente, diverso do sistema de dados ou informação.

São exemplos os crimes contra o patrimônio, como o furto e o estelionato praticados com o uso da internet. Assim, o agente se utiliza de um computador ou assemelhado para atingir um bem que se encontra no mundo físico, do qual de originará um resultado naturalístico.

5 **LEGISLAÇÃO BRASILEIRA E O CRIME CIBERNÉTICO**

Outra dificuldade na qual se esbaram os investigadores é em relação à legislação aplicável aos casos de crimes cibernéticos, que em muitas vezes são inexistentes, ou quando existem, pecam pela falta técnica, dando margem a interpretações dúbias, o que dificultam a sua aplicabilidade.

5.1 DECRETO-LEI 2.848/1940 - CÓDIGO PENAL

Hoje em nosso Código Penal não encontramos nenhum artigo onde se enquadre o sujeito que comete uma infração por meio de computador. Geralmente punem-se esses criminosos no enquadramento de outros artigos, como estelionato, formação de quadrilha, entre outros.

Sendo assim, muito se fala em analogia para casos inéditos como os de crimes na internet, contudo, no Direito Penal, a analogia só é aplicada em benefício do réu, o conceito de in dúbio pro réu (em caso de dúvidas, beneficia-se o réu) prevalece em nosso ordenamento, sendo assim, muitas das vezes, em caso de dúvidas se entende de forma benéfica ao réu, tudo isto devido à ineficiência e defasagem de nossa legislação penal.

Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal, preceitos previstos nos incisos II e XXXIX do art. 5º da CF/88, respectivamente, base de todo nosso regime jurídico, sendo assim é inviável o funcionamento atual ser controverso a esse posicionamento, mesmo que algumas decisões já sejam tomadas direcionadas a esse ponto, não é totalmente efetivo o combate a esses delitos.

Com o advento da era digital e o avanço exacerbado da internet e dos dispositivos informáticos, novos crimes e novas formas de execução foram sendo criadas e aperfeiçoadas nos crimes informáticos, de maneira que, cada vez mais, dificultou-se precisar quando o crime foi cometido, em que lugar se deu, quem seria competente para julgar crimes plurilocais e outras tantas questões penais que se tornaram cada vez mais controvertidas. Discorrer-se-á, a seguir, sobre algumas questões penais importantes e a sua aplicabilidade com relação aos crimes informáticos.

1. Tempo do crime

A fixação do instante em que o crime foi praticado é importante sob vários aspectos, mormente para, entre outras hipóteses legais, determinar a lei vigente no momento que o delito se consumou, no caso de sucessão de leis penais, para aferir

a inimputabilidade penal, ou seja, se o agente tinha 18 anos na ocasião da consumação, ou se ao tempo da ação ou omissão era inteiramente incapaz de entender o caráter ilícito do fato ou ao menos se

determinar de acordo com esse entendimento, além do exame das circunstâncias do crime e aplicação de eventual anistia condicionada no tempo.

Para Andreucci (2010, p. 102) “a questão referente ao tempo do crime apresenta particular interesse quando, após realizada a atividade executiva e antes de produzido o resultado, entra em vigor nova lei, alterando os dispositivos sobre conduta punível”. Nesse mister, o autor levanta o seguinte questionamento: “Qual a lei deve ser aplicada ao criminoso: a do tempo da atividade ou aquela em vigor por ocasião da produção do resultado?”, assim apresenta três teorias a respeito:

a. Teoria da atividade, segundo o qual se considera praticado o delito no momento da ação ou omissão, aplicando-se ao fato a lei em vigor nessa oportunidade;

b. Teoria do resultado, segundo o qual se considera praticado o delito no momento da produção do resultado, aplicando-se ao fato a lei em vigor nessa oportunidade;

c. Teoria mista ou ubiquidade, segundo o qual o tempo do crime é indiferentemente o momento da ação ou do resultado, aplicando-se qualquer uma das leis em vigor nessas oportunidades. (ANDREUCCI, 2010, p. 102)

Assim, o nosso Código Penal adotou a teoria da atividade no seu art. 4.º, que diz: “Art. 4.º Considera-se praticado o crime no momento da ação ou omissão, ainda que outro seja o momento do resultado.” Portanto, considera-se tempo do crime o momento da ação ou omissão do agente, ou seja, no momento da prática da conduta prevista da norma penal incriminadora.

Sendo assim, com relação aos crimes informáticos, o tempo do crime é de suma importância, pois o agente pode ter cometido algum ato delituoso não previsto, na época, em nossa Lei Penal. Isso torna-se uma tarefa árdua aos julgadores, visto que, atualmente, tem-se pouca matéria tipificada sobre crimes informáticos enquanto há um universo de possibilidades para os agentes que cometem esse tipo de crime.

1. Local do crime

A fixação do lugar do crime é importante para fins de delimitar a competência do órgão jurisdicional para julgar o caso. Novamente Andreucci (2010, p. 112) nos traz três teorias que procuram solucionar o problema:

a. Teoria da atividade, segundo a qual o local do crime é aquele onde é praticada a conduta criminosa (ação ou omissão);

b. Teoria do resultado, segundo a qual o local do crime é aquele onde ocorre o resultado; e

c. Teoria mista ou da ubiquidade, também conhecida por teoria da unidade, segundo a qual o local do crime é aquele onde ocorreu tanto a conduta quanto o resultado, ou seja, qualquer etapa do iter criminis.

O legislador adotou em nosso Código Penal a teoria da ubiquidade, de maneira que se considera “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”.[9]

A importância de se definir o lugar do crime ganha destaque nos casos de tentativa, em que, iniciada a execução do crime, este não se consuma por circunstâncias alheias à vontade do agente, bem como na hipótese de crimes a distância, naquelas infrações em que a ação ou omissão se dá em um país e o resultado em outro, situação muito comum quando se trata de crimes informáticos.

Interpretando a norma trazida, desde que no Brasil tenham sido praticados atos de execução, no todo ou em parte, ou aqui se tenha produzido o resultado do comportamento ilícito, é de aplicar-se a legislação pátria. Numa abordagem de questões de jurisdição e territorialidade nos crimes praticados por meio da internet, Valin (2000, p. 116) aponta problema para análise do caso quanto a situação compreender a segunda figura da norma comentada, ou seja, quando se considerar praticado o crime onde se produziu ou deveria produzir-se o resultado, “principalmente com o que diz respeito aos crimes que

podem ser cometidos com a divulgação de informações, o ataque a servidores e furto de dados”.

O mesmo autor exemplifica levantando a hipótese de um ataque estrangeiro que acabe por retirar do ar um servidor de renome como o Yahoo, fisicamente não presente no território nacional, de forma que não permite que um usuário brasileiro possa acessá-lo no período.

Nessa hipótese, em que o crime realmente surtiu os seus efeitos e lesionou um bem juridicamente protegido de um cidadão brasileiro, qual seja, o direito de acesso à informação[10], pela análise fria da legislação, poderia ser julgado pelo Direito pátrio, ainda que o autor do delito e o portal Yahoo, vítima principal, não estejam fisicamente no território nacional. Porém, Valin (2000, p. 116-117) questiona se seria eficaz o julgamento realizado no Brasil, até por uma questão de aplicabilidade da lei penal.

Propõe o autor a revisão da matéria por meio de regras estabelecidas em tratado internacional, sendo adotado, para os crimes praticados por meio da internet, “algo semelhante à teoria da atividade que determina como sendo o local do crime aquele em que o agente praticou o delito”, definindo-se qual o local efetivo da prática do ato, “se é o local onde se encontra o autor, ou se é o local em que as ofensas foram publicadas” (VALIN, 2000, p. 116-117).

Na opinião do autor, a melhor solução seria considerar como local do crime “aquele em que está o autor da infração”. Justifica sua posição por considerar o país de domicílio do réu o melhor para aplicar eventual pena, além de evitar o processo de extradição, sempre moroso, bem como por ser o país do local da publicação o único com poder legal para retirar a página da rede, o que eventualmente poderá ser feito por meio de outro processo, independente do criminal.

1. Competência para julgar crimes plurilocais

A doutrina definiu crimes plurilocais como sendo “aqueles em que a ação ou a omissão se deu em um determinado local e o resultado em outro, mas dentro do território nacional (NUCCI, 2005). Tendo em vista as peculiaridades, é justamente dentro do conceito de crimes plurilocais que se insere a maior gama dos crimes praticados por meio da internet, como o furto mediante fraude, por exemplo.

Se imaginarmos a situação hipotética em que, após ter feito emprego de um keylog e subtrair dados da vítima, o agente conecta-se a um provedor de banda larga de Foz do Iguaçu – PR, acessa a home banking de uma instituição financeira particular de Marília – SP, onde fornece o número da conta corrente e a senha do cliente, e efetua a transferência de um valor razoável da conta bancária até a conta de um terceiro, situada em uma agência de Balneário Camboriú – SC. A vítima somente percebe a subtração no dia seguinte, quando o agente já providenciou o saque do valor respectivo da conta corrente do terceiro, para onde o valor tinha sido transferido de forma fraudulenta.

Percebe-se no exemplo trazido que o iter criminis se iniciou em Foz do Iguaçu – PR, passou por Marília – SP e se consumou em Balneário Camboriú – SC. Assim, como se delimita a competência no caso em tela? É de suma importância saber precisar a competência nesse caso, pois, como já dito, a maioria dos crimes cometidos pela internet tem essa característica.

Levando em consideração a regra geral de competência em razão do foro, prevista no art. 70 do Código de Processo Penal, o juízo da Comarca de Marília – SP é que deve conhecer e julgar o processo. Conforme abordado anteriormente, o furto é um crime material cuja consumação se verifica com a produção do resultado naturalístico. Segundo Nucci (2005, p. 223), “tal regra somente tem pertinência aos crimes materiais, isto é, aqueles que possuem resultado naturalístico e pode haver clara dissociação entre ação, omissão e resultado”. Portanto, fica afastada essa regra nos casos de crimes formais ou de mera conduta, cuja consumação se dá com ação de omissão.

Essa questão não é pacífica na doutrina, tanto é que Inellas (2004) defende a tese de que os crimes praticados por meio da internet são crimes formais. Para o autor, tais delitos se consumam no “local onde foi realizada a ação” (INELLAS, 2004,

p. 85). Outros autores como Furlaneto Neto (2003) discordam desse posicionamento: “é verdade que a grande rede mundial de computadores trouxe a necessidade de algumas reflexões nos campos de

Direito Penal e Processual Penal, porém, por si só, não teve o condão de modificar alguns institutos jurídicos.”

Nesse contexto, como já abordado ao apresentar a classificação dos crimes informáticos, há crimes já tipificados pela legislação e que não sofreram nenhuma alteração com o surgimento da internet, apenas tivemos a modificação do seu modus operandi. É sabido que algumas condutas necessitam ser reexaminadas, tais como, a título de exemplo, o furto de tempo[11], cuja ação, no entendimento de Inellas (2004), se amolda por equiparação ao furto de energia elétrica, bem como o dano perpetrado pela disseminação de vírus, porém, assim como o tipo penal do homicídio não precisou ser modificado com o surgimento da arma de fogo, não se faz necessária a alteração de inúmeros crimes já tipificados pelo nosso Código e leis extravagantes com o fundamento no surgimento da internet.

Tendo em vista a dupla subjetividade passiva do crime de furto mediante fraude praticado por meio da internet, se o dinheiro subtraído estivesse depositado em uma agência da Caixa Econômica Federal, por se tratar de uma empresa pública, a competência para conhecer e julgar o crime seria da Justiça Federal, conforme entendimento do STJ:

CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSO PENAL. FRAUDE ELETRÔNICA NA INTERNET. TRANSFERÊNCIA DE NUMERÁRIO DE CONTA DA CAIXA ECONÔMICA FEDERAL. FURTO MEDIANTE FRAUDE QUE NÃO SE CONFUNDE COM ESTELIONATO. CONSUMAÇÃO. SUBTRAÇÃO DO BEM. APLICAÇÃO DO ART. 70 DO CPP. COMPETÊNCIA DA JUSTIÇA FEDERAL PARANAENSE. (...) 2. Hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de dois mil e quinhentos reais de conta bancária, por meio da "Internet Banking" da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima, o Banco. (...) No caso em apreço, o desapossamento que gerou o prejuízo, embora tenha se efetivado em sistema digital de dados, ocorreu em conta corrente da Agência Campo Mourão/PR, que se localiza na cidade de mesmo nome. Aplicação do art. 70 do Código de Processo Penal. 5. Conflito conhecido para declarar competente o Juízo Federal de Campo Mourão -

SJ/PR. (STJ, CC nº 200601661530 (67343), GO, 3ª S., Relatora Min. Laurita Vaz)

Tendo como base a ementa supracitada e o entendimento utilizado pela Relatora Min. Laurita Vaz, no caso do furto mediante fraude exemplificado anteriormente, por se tratar de instituição financeira particular, a competência seria da Justiça Comum de Marília – SP, local onde se situa a agência bancária.

Nesse sentido, há também entendimento do TRF da 4ª Região:

PROCESSO PENAL. COMPETÊNCIA. TRANFERÊNCIA FRAUDULENTA PRATICADA PELA INTERNET. SUBTRAÇÃO DE VALORES DEPOSITADOS EM BANCO. FURTO MEDIANTE FRAUDE. COMPETÊNCIA. LOCAL DA SUBSTRAÇÃO. 1. Em que pese a existência de recentes julgados desta Corte entendendo tratar-se de estelionato (com a divergência deste Relator) firmou-se a jurisprudência do Superior Tribunal de Justiça no sentido de que a hipótese de subtração, por meio eletrônico, de valores depositados em instituição bancária configura o crime de furto mediante fraude. 2. Modificada a orientação da 4ª Seção para, com base nos precedentes citados, declarar competente a Subseção Judiciária onde está situada a agência que mantém a conta corrente da qual os valores foram subtraídos. (TRF 4ª R., SER 2007.71.00.000608-6, 8ª T., Rel. Des. Fed. Luiz Fernando Wowk Penteado, DJe de 21.11.2007)

Importante salientar que as demais regras de competência previstas no CPP devem ser aplicadas à criminalidade informática, conforme o

entendimento de Castro (2003) e todas elas auxiliam no sentido de esmiuçar a complexidade que se percebe em alguns delitos informáticos, tanto pela sua complexidade técnica, quanto pela complexidade jurídica.

Na tentativa de sanar a lacuna existente na legislação penal com relação aos crimes informáticos, o legislador, por meio da Lei 12.737, cria um novo tipo penal “invadir dispositivo informático” e, assim, inúmeras questões surgem em torno dessa nova modalidade. O objetivo do capítulo a seguir é apresentar, de uma forma geral, porém abrangente, essa alteração feita pelo legislador e as inúmeras consequências que dela se originam.

5.2 LEI 11.829/2008 - ESTATUTO DA CRIANÇA E DO ADOLESCENTE

A Lei nº 11.829, de 25 de novembro de 2008, que alterou o Estado da Criança e do Adolescente foi um dos primeiros passos dados pelo Legislativo com o intuito de combater os crimes virtuais, uma vez que a referida lei definiu algumas condutas específicas relacionadas à prática de crimes de pornografia infantil no ambiente virtual, suprindo a lacuna legislativa que deixava criminalmente impunes aqueles que tinham armazenados em seus computadores vídeos e fotos relacionados à pornografia infantil.

5.3 LEI 12.737/2012 - LEI CAROLINA DIECKMANN

Como já visto anteriormente, muitos criminosos informáticos não são

devidamente repreendidos, por conta de ausência de legislação que regule o comportamento do agente a fim de punir atividades ilícitas na internet ou contra dispositivos informáticos. Sendo assim, cada vez mais se faz necessária a presença de uma legislação ampla e abrangente, de maneira a não deixar lacunas e tentar preencher o máximo todas as possibilidades já encontradas de crimes informáticos. Vale lembrar que existem os crimes informáticos impróprios que já estão previstos no nosso Código Penal e não é sobre eles que há necessidade de legislar, mas sim sobre os crimes informáticos próprios, aqueles em que a internet, o computador e os dispositivos informáticos são alvos do agente criminoso.

Foi com esse objetivo que, em 2012, entrou em vigor a Lei 12.737 que altera o Código Penal e dá outras providências. Tida como novidade no âmbito jurídico, a Lei Carolina Dieckmann, como é conhecida pela imprensa, tenta exaurir essa lacuna existente na legislação penal quanto aos crimes informáticos.

A Lei vem merecendo críticas de juristas, peritos, especialistas e profissionais de segurança da informação, como por exemplo, em seu artigo 154-A trata sobre invasão de dispositivo informático alheio, porém a lei traz uma redação ampla, confusa e que pode gerar dupla interpretação, ou mesmo interpretação subjetiva, o que pode ser utilizado para enquadramento criminal de condutas triviais ou mesmo para a defesa e respaldo de infratores cibernéticos, o que tornaria a lei injusta e ineficaz. Para outra corrente, ainda, as penas são pouco inibidoras, sendo muitas situações enquadráveis nos procedimentos dos Juizados Especiais, o que poderia contribuir para a não eficiência no combate ao crime cibernético no Brasil.

5.4 LEI 12.965/2014 - LEI DO MARCO CIVIL DA INTERNET

A lei 12.965, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

O Marco Civil da Internet, como é conhecida, é a lei que regula o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado.

A ideia da lei, surgiu em 2007, foi adotada pelo governo federal em função da resistência social ao projeto de lei de cibercrimes, conhecido como Lei Azeredo (em alusão ao seu autor, Eduardo Azeredo), muito criticado sob a alcunha de AI-5 digital.

É aspecto intrigante do Marco Civil da Internet a ingenuidade do legislador brasileiro de manter a pretensão de solução de problema de escala mundial, com efeitos extraterritoriais, por meio de uma lei nacional. A própria estrutura da internet permite que as violações dos direitos das pessoas ocorram em qualquer parte do

mundo, passando ao largo da jurisdição brasileira. Parece confessar essa dificuldade, ao afirmar-se, no art.2º, I, do Marco Civil da Internet, que um dos fundamentos da disciplina do uso da internet é o "reconhecimento da escala mundial da rede". Na tentativa de frear violações de privacidade por meio de coleta, armazenamento e tratamento de registros, dados pessoais ou comunicações, por meio do art.11, caput, §§1º e 2º, estabeleceu-se que o Marco Civil da Internet se aplica quando, pelo menos, um dos atos realizar-se no Brasil ou quando um dos terminais estiver no Brasil e que pessoas jurídicas com sede no exterior devem sujeitar-se à lei brasileira quando tiverem, pelo menos, uma integrante do mesmo grupo econômico com estabelecimento no Brasil. A despeito da boa intenção, a violação pode não acontecer no Brasil, mas poderá acontecer na outra ponta da transmissão de dados no exterior. Mesmo com a previsão das sanções contidas no art.12 do Marco Civil da Internet, entre os quais, advertência, multa de 10% do faturamento do grupo econômico no Brasil em seu último exercício, suspensão temporária de atividades ou proibição de exercício de atividades - sendo esta última medida possivelmente inconstitucional nos termos do art.170 da Constituição Federal - tais medidas serão inócuas, já que o Brasil não tem jurisdição para controlar as atividades dessas grandes empresas em suas sedes no exterior.

Devido a todas essas dificuldades naturais de gerenciamento de uma rede mundial de computadores, deixou-se de lado a polêmica exigência de instalação de datacenters para fins de provisão de aplicações de internet no Brasil, nos termos do art.24, VII, uma vez que a informação que circula na internet não é física e de pouco adiantaria seu armazenamento no Brasil, se esta pode ser replicada indefinidamente para qualquer parte do mundo. Não é impossível que, no envio de um e-mail para o computador do lado, esses dados circulem em outros países pelo próprio tráfego da rede. A proposta de nacionalização de datacenters é prova do desconhecimento do funcionamento da internet, imaginando-a como uma biblioteca física localizada em determinado território, sem qualquer conexão ou interferência com a estrutura física de internet dos demais países.

Um aspecto positivo do marco civil, consiste na regulamentação dos procedimentos judiciais específicos para obtenção dos registros de navegação para fins de instrução processual civil e penal. O projeto inicial do Marco Civil da Internet não tratava da interceptação de dados transmitidos pela internet ou o acesso dessas informações por terceiros, tampouco afirmava a ilegalidade dessas práticas, limitando-se apenas ao que está armazenado nos servidores e não no que está circulando entre eles. Apesar disso, não se trata de grande inovação, pelo fato de que se poderiam usar as regras atuais contidas nos Códigos de Processo Civil e Penal, bem como as delegacias especiais de combate a crimes virtuais há mais de

uma década já fazem a requisição desses dados pelo uso dos mesmos procedimentos comuns aos demais crimes.

Outro aspecto positivo foi a disciplina dos chamados cookies, arquivos instalados nos computadores ou telefones para registrar informações e preferências dos usuários quando acessam determinada página na internet, conforme o art.7°, VIII. Essas normas também não estavam presentes no projeto inicial. Dessa maneira, as páginas de internet terão que informar logo no primeiro acesso do usuário que pretendem coletar tais informações. Afinal, é violação da privacidade quando a pessoa acessa determinada informação e receber ofertas de produtos e serviços relacionados. No mesmo sentido, não parece correto que o Estado ou terceiros soubessem que o leitor leu esse texto e, tempos depois, indagá-lo por que se interessou por esse assunto. Com efeito, são situações reais e preocupantes, porque essas grandes empresas de internet já conhecem quase todos os hábitos de determinada pessoa, tornando-se um verdadeiro "big brother". Mesmo assim, poder-se-ia obrigar a solicitação de concordância com a coleta desses dados, tal como ocorre em páginas da internet de países europeus, em vez de apenas informar o usuário sobre esse fato. Completando essa ideia, foi importante o reconhecimento no art.7º, VII, da proibição de fornecimento a terceiros dos dados pessoais, inclusive registros de conexão e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei.

Importante destacar o art.18, que, acertadamente, declarou a irresponsabilidade civil do provedor de conexão à internet por atos ilícitos praticados pelos usuários. Tal providência faz todo sentido, porque essa atividade consiste apenas em promover a conexão dos computadores e telefones celulares das pessoas à internet. Implica dizer que não há nexo causal entre a realização de tal atividade e os danos sofridos por terceiros. Exemplo disso deu-se com a publicação de vídeo no site Youtube.com em 2006, quando este site ainda não era tão popular quanto nos dias atuais, em que a atriz Daniela Cicarelli foi registrada na Espanha praticando atos sexuais no mar. Sentindo-se ofendida em sua honra, imagem e privacidade, ela ingressou com ação para que o material fosse retirado do site, o que foi deferido pelo Tribunal de Justiça do Estado de São Paulo. Pelo fato de que esse material estava hospedado em servidores nos Estados Unidos e a ordem para retirada do material foi dada aos provedores de acesso brasileiros, não restou alternativa que não fosse o bloqueio de todos os usuários brasileiros ao site Youtube.com (Folha de S.Paulo, 2007a, p.C7) o que fez o Tribunal de Justiça do Estado de São Paulo rever o equívoco da ordem judicial quanto a seus efeitos (Folha de S.Paulo, 2007b, p.C5).

No entanto, são muitas as deficiências e insuficiências do Marco Civil da

Internet, mesmo depois da revisão do projeto inicial por meio da aprovação do texto substitutivo. Afinal, toda lei aprovada tem a finalidade de inovar o ordenamento jurídico, acrescentando normas necessárias à regulação dos comportamentos, eliminando aquelas que não mais atendem às necessidades sociais. O primeiro ponto a ser observado é a redundância de várias de suas disposições, que repetem, com insuficiência, o que já consta na Constituição Federal. Nenhuma "ginástica hermenêutica" é capaz de permitir ao operador do direito a obtenção de significado adicional. Por exemplo: o art.5º, X, da Constituição Federal dispõe que: "X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação", e o art.7°, I, do Marco Civil da Internet dispõe que é direito dos usuários da internet a: "I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano moral e material decorrente de sua violação".

É dispensável afirmar que é princípio do uso da Internet a "proteção da privacidade" e a "proteção dos dados pessoais, na forma da lei', por repetir o que já dispõe a Constituição Federal. Também o art.3º, parágrafo único, dispõe que "os princípios expressos nessa Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte", quando o art.5º, §2º, da Constituição Federal dispõe que "§2º - Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte".

O art.9º, §2°, I, do Marco Civil da Internet é desnecessário pela sua obviedade. Ao estabelecer que, em caso de discriminação ou de degradação do tráfego na internet, o responsável deve "abster-se de causar danos aos usuários, na forma do art.927 da Lei n.10.406, de 10 de janeiro de 2002 - Código Civil", simplesmente se dispôs o seguinte: cumpra-se a lei! Retomando o que já se mencionou acima, o art.3º, parágrafo único, ao estabelecer que "os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria..." simplesmente dispõe sobre o óbvio, que é o de que o ordenamento jurídico é composto por diversas normas e que a disciplina jurídica de determinado assunto não se encerra em um único texto de lei.

Outra obviedade é o disposto no art.7°, XIII, segundo o qual se estabelece como direito dos usuários da Internet a "XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na Internet", ou, em outras palavras: aplica-se o Código de Defesa do Consumidor às relações de consumo! Do mesmo modo, o art.7°, V, do Marco Civil da Internet, segundo o qual é direito do usuário a "manutenção da qualidade contratada da conexão à Internet",

como se fosse logicamente possível qualquer disposição em contrário. Afinal, já é muito antiga a ideia de que os contratos devem ser cumpridos ("pacta sunt servanda") e que se deve entregar exatamente o que se obrigou a tanto. Tanto que o art.313 do Código Civil estabelece que "o credor não é obrigado a receber prestação diversa da que lhe é devida, ainda que mais valiosa".

Igualmente despicienda é a norma do art.8°, I, segundo a qual prevê a nulidade de pleno direito de cláusulas que "impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela Internet". Nesse caso, tal cláusula seria não apenas inconstitucional, como também ilegal e inválida, nos termos do art.166, II e VI, do Código Civil. Ainda, a previsão do art.3º, VI, da "responsabilização dos agentes de acordo com suas atividades, nos termos da lei" é irrelevante, porque é ilógico pensar em irresponsabilidade dos agentes por seus atos. Desnecessária também é a regra do art.8º, II, segundo a qual se estabelece que, em contratos de adesão, é nula a cláusula que não oferece alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil. Tal direito é garantido pelo art.5º, XXXV, da Constituição Federal, segundo o qual "a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito" e também pelo art.101 do Código de Defesa do Consumidor, segundo o qual "Na ação de responsabilidade civil do fornecedor de produtos e serviços, sem prejuízo do disposto nos Capítulos I e II deste título, serão observadas as seguintes normas: I - a ação pode ser proposta no domicílio do autor".

O texto do Marco Civil da Internet trouxe normas vazias de conteúdo. Por exemplo, o art.2º, IV, segundo o qual prevê como fundamento da disciplina do uso da internet a "abertura e a colaboração". Há que perguntar de que abertura se trata e que colaboração se pretende. O art.5º do Marco Civil da Internet, que apresenta definições para fins de interpretação, deixou de definir "provedor de conexão à Internet", "provedor de aplicações de Internet", "provedor responsável pela guarda dos registros" e "responsável pela transmissão, comutação e roteamento". Não se trata de definições de menor importância, já que são estes os principais destinatários dos deveres reflexos previstos na declaração dos direitos dos usuários da internet.

Não há critério em estabelecer-se o prazo de um ano para armazenamento dos registros de conexão, nos termos do art.13 e o prazo de seis meses para armazenamento dos registros de acesso a aplicações de internet, nos termos do art.15. Também silenciou sobre o estímulo à criptografia como forma de resguardo da privacidade das pessoas em suas comunicações.

Quanto à proteção dos usuários da internet, o Marco Civil diminuiu a responsabilidade dos provedores de aplicações de internet. Nos termos do direito então vigente, o art.942 do Código Civil estabelece a solidariedade ex delito. Dessa

maneira, basta a ocorrência do dano para que a vítima pudesse acionar judicialmente tanto o usuário violador, quanto o provedor de aplicações de internet ou ambos, simultaneamente. Esse sistema de proteção impunha o dever de vigilância dos provedores de aplicações de internet, ante a possibilidade de responder diretamente pelos atos dos usuários, pelo menos mediante o oferecimento de canais de denúncia para que se formulasse o pedido de retirada do conteúdo.

O Marco Civil da Internet, estabeleceu-se a responsabilidade subsidiária dos provedores, dispensando-os desse dever de diligência, o que facilitará a prática de delitos. Dessa maneira, o primeiro responsável é o usuário que causou o dano. Os provedores de aplicações de internet somente respondem quando se recusarem a cumprir ordem judicial para retirada do conteúdo violador dos direitos da personalidade. Apenas se exige a retirada do material quando o material envolver conteúdo sexual.

6 **DIFICULDADE EM IDENTIFICAR A AUTORIA DO CRIME CIBERNÉTICO**

O primeiro problema que é encontrado ao se enfrentar os crimes cibernéticos é a determinação da autoria. Raramente, a pessoa que pretende cometer uma infração penal utiliza sua identificação pessoal verdadeira. Há casos em que o criminoso se faz passar por outra pessoa, mediante o uso indevido de suas senhas pessoais.

Nas redes de computadores, não é possível identificar o usuário visualmente ou através de documentos, mas é possível identificar o endereço da máquina que envia as informações à rede. Ou seja, o IP da máquina.

O número IP é uma identificação que todos os computadores que acessam a Internet possuem; ele aparece no formato A. B. C. D, onde A, B, C e D são números que variam de 0 a 255 (por exemplo, 200.158.4.65).

Daí vem a importância da cooperação dos provedores de acesso nesse tipo de investigação. Como visto acima, o provedor é o computador que providencia acesso à rede e é responsável por fornecer aos clientes um número de IP para que este se conecte. Portanto, após se conseguir o número de IP utilizado na realização de uma conduta criminosa, é necessário requisitar ao provedor de acesso informações sobre o usuário daquele IP.

Entretanto, a maioria dos serviços de conexão adota o sistema de IP dinâmico. Isso quer dizer que cada vez que uma máquina se conecta a Internet, recebe um IP diferente de seu provedor. Por isso, além de possuir o número de IP utilizado para a prática criminosa, também é necessário a data, a hora exata da conexão ou comunicação e o fuso horário do sistema.

Como a Internet é uma rede mundial de computadores, os registros indicam a hora local e a referência à hora GMT. Às vezes, é feita apenas a menção à hora GMT (por exemplo, “Tue, 09 Mar 2004 00:24:28 GMT”).

Cada IP está vinculado à uma provedora de acesso. Há sites de registro destinados à identificar a provedora de acesso responsável por cada IP. Uma vez identificada a provedora de acesso deve-se requisitar informações a respeito do cliente que utilizou aquele IP durante aquele momento.

Nos pedidos feitos aos provedores de acesso e às companhias telefônicas, é imprescindível que haja, no mínimo, a menção a esses três indicadores: a) o número IP; b) a data da comunicação; e c) o horário indicando o fuso horário utilizado – GMT ou UTC. Sem eles, não será possível fazer a quebra do sigilo de dados telemáticos.

Importa ressaltar que não podemos confundir interceptação de dados telemáticos com quebra de sigilo dos dados de conexão e de usuário.

A quebra do sigilo dos dados de conexão de usuário, trata-se somente da

disponibilização por parte das empresas, em um primeiro momento, de qual teria sido o IP utilizado e o horário (incluindo informações de fuso horário) de determinada ação criminosa realizada em um serviço de Internet, como redes sociais, contas de e-mail, programas de mensagens instantâneas, dentre outros e em um segundo momento das informações do usuário que efetivamente utilizou aquele IP de determinado provedor, ou seja, qual teria sido, supostamente, o endereço físico no "mundo real" em que o computador ou outro equipamento informático com acesso à Internet estaria instalado no momento da conduta criminosa.

Já a interceptação de dados telemáticos diz respeito ao recebimento por parte da Autoridade Policial de todos os acessos e conexões realizados pelo investigado em ambiente de Internet. Se equipara, em todas as questões legais, à interceptação telefônica, devendo, portanto, ser realizada em sede de Inquérito Policial, sendo necessária, portanto, a provocação do Poder Judiciário e Ministério Público, por meio de Representação, a fim de obtermos a autorização judicial, nos moldes da legislação vigente, em especial a Lei 9.296/96, a Lei de Interceptações Telefônicas.

A análise dos dados constantes dos cadastros de clientes dos provedores de acesso não caracteriza interceptação do fluxo de comunicações em sistemas de informática, sendo certo que a requisição judicial não é necessária.

Algumas empresas que prestam serviços na Internet somente divulgam os dados de conexão com decisão judicial. Costumam criar embaraços para informar à Autoridade Policial as informações que são necessárias à investigação de crimes que tenham sido cometidos em seus serviços.

Outro problema enfrentado, é o tempo de armazenamento dos logs (registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado) de acesso. Não há na legislação nenhuma previsão de por quanto tempo os servidores devem armazenar essas informações.

Em Julho de 2008, o Ministério Público Federal conseguiu com que a Google assinasse Termo de Ajustamento de Conduta, que entrou em vigor imediatamente, prevendo a preservação de todos os dados necessários às investigações pelo prazo mínimo de seis meses e o fornecimento desses dados a polícia brasileira, mediante autorização judicial. Tal acordo foi procedido por inúmeros nos mesmos moldes. Entretanto, tal prazo ainda é incompatível com a conclusão das perícias informáticas e andamento dos inquéritos policiais, sendo a investigação obstaculizada pela perda dessas informações.

No entanto, a situação pode ser ainda mais complicada. Como identificar o agente? Para termos uma ideia das dificuldades e da complexidade que o tema dos

controles assume, por exemplo, na Internet, basta mencionar que podem existir serviços que poderiam ser denominados de serviço de máscara.

Esses serviços de máscara seriam os denominados proxys (um servidor - um sistema de computador ou uma aplicação - que age como um intermediário para requisições de clientes solicitando recursos de outros servidores.) de anonimato. Muitas vezes, é utilizada uma cadeia de proxys, tornando a identificação da máquina de origem das ações virtualmente irrastreável.

6.1 FALTA DE MATERIALIDADE

Em regra, pode-se dizer que as evidências dos crimes cibernéticos são extremamente voláteis. Podem ser apagadas em segundos ou perdidas facilmente. Além disso, possuem formato complexo e costumam estar misturadas a uma grande quantidade de dados legítimos, demandando uma análise apurada pelos técnicos e peritos que participam da persecução penal.

Muitas vezes, para a devida comprovação da materialidade do delito se faz necessária a interceptação do fluxo de comunicações realizadas através de um computador. Tais interceptações, como exposto acima, somente podem ser feitas mediante autorização judicial.

Em relação à inviolabilidade do sigilo das comunicações, Ada Pellegrini Grinover ensina:

> “A garantia constitucional pode sofrer limitações, não devendo prestar-se para a proteção de atividade ilícitas ou criminosas. É assim que através de uma ponderada apreciação judiciária, que obedeça os limites legais, pode ser determinada a interceptação das comunicações telefônicas.”

Observe-se que de acordo com o parágrafo único do art. 1º da Lei nº 9.296/96, estendeu-se a normatização das interceptações telefônicas ás informáticas e telemáticas. Segundo João Roberto Parizatto:

> “o que o dispositivo em apreço quer, é estender a aplicação das hipóteses de interceptação de comunicações telefônicas, a qualquer espécie de comunicação, ainda que realizada através de sistemas de informática, existentes ou que venham a ser criados.”

A maioria dos crimes cibernéticos exige perícia para sua perfeita prova. Uma vez identificado o endereço real do criminoso, e determinada a busca e apreensão de seu computador e, quaisquer mídias que possam conter indícios da materialidade será procedido o exame de corpo de delito.

De início, é feita uma duplicação das mídias do exame, e a perícia deverá ser realizada nas cópias. Isso porquê, além da preservação dos originais, o simples fato de se abrir um arquivo de computador já altera seu estado.

As evidências dos crimes cibernéticos, em um computador, podem ser classificadas como evidências do usuário e evidências do sistema. As evidências do usuário são aquelas produzidas pelo próprio sujeito ativo, em arquivos de texto, imagem ou qualquer outro tipo. Já as evidências do sistema são as produzidas pelo sistema operacional, em função da ação do sujeito ativo. Pode-se citar os arquivos temporários da Internet, o cache da memória ou os cookies dos sites visitados.

6.2 ACERCA DA LOCALIZAÇÃO DA ORIGEM DA CONDUTA DELITUOSA NA REDE

Como já exposto no presente trabalho, em regra, ao se obter o endereço IP utilizado na prática da conduta criminosa, teria-se a localização do agente criminoso e sua consequente identificação. Porém, há diversas formas de se burlar esse tipo de evidência, tais como a utilização dos servidores proxys, das redes Wi-Fi abertas, bem como o acesso por meio das denominadas lan houses ou cyber cafés.

As redes Wi-Fi abertas consistem em locais que dão acesso gratuito à internet, criadas muito em função da crescente onda de utilização de smartphones e outros dispositivos de informáticas portáteis. Contudo, por terem a característica de serem de acesso gratuito e de acesso ao público em geral, estas redes permitem o uso de pessoas não identificadas, apresentando-se aos cibercriminosos como um leque de oportunidades para a práticas de atividades com fins maliciosos, pois, em razão de ser possível ser acessada por qualquer pessoa, dificulta a localização de seus usuários, propiciando uma maior probabilidade de o agente criminoso sair impune pelo delito praticado.

Uma outra dificuldade encontrada é relacionada à falta de registro de usuários que se utilizam dos serviços de internet disponibilizados pela denominadas lan houses e cyber cafés, quando muito raramente exije-se o cadastro, o uso de documento falso é utilizado, permitindo-se que os criminosos utilizem-se de tais locais para práticas de suas condutas ilícitas, o que dificulta que seja possível a obtenção da autoria, uma vez que tais locais são abertos a qualquer pessoa e os estabelecimentos não mantém registros de seus usuários. As lan houses e cyber cafés são principalmente usadas nos grandes centros urbanos, disponibilizando o serviço de acesso à internet vinte e quatro horas por dia.

Com a utilização dos proxys, o endereço IP do servidor proxy foi o que acessou aquele conteúdo disponibilizado na internet e não o do usuário que o efetivamente acessou.

Os servidores proxys não se destinam exclusivamente à prática de atividades maliciosas. Pelo contrário, foram criados justamente para esconder o endereço IP do

usuário a fim de protegê-lo de ataques maliciosos na rede, bem como contra o roubo de dados. Contudo, há aqueles destinados a esconder a identificação dos usuários com o fim exclusivo de dificultar a identificação do agente delinquente e a obter, como consequência, a impunidade pelo crime praticado.

Esta modalidade é chamada de proxy anônimo, sendo este uma ferramenta que se destina a propiciar a prática de atividades na internet sem com que se deixe vestígios, ou seja, acessa a internet em favor do usuário, protegendo-se as suas informações pessoais ao ocultar o endereço IP que o identificaria, assim previne que haja a publicidade das informações de identificação do computador que deu origem a um evento na internet.

Como se não bastasse, o usuário pode se utilizar de uma cadeia de diferentes proxys. Assim, se um dos proxys que fazem parte da cadeia não colaborar com os outros integrantes e não guardar as informações dos usuários, torna-se impossível identificar o usuário através do número IP.

6.3 PROCEDIMENTOS INVESTIGATIVOS NOS CRIMES CIBERNÉTICOS

As tecnologias de informação possuem uma praticidade sem igual, motivo pelo qual os crimes cibernéticos podem ser praticados de inúmeras formas dentro do mundo virtual. É por esse motivo que a polícia investigativa, ao tomar conhecimento da prática de um delito virtual, deve primeiramente identificar o meio utilizado pelo criminoso para a prática do ilícito penal.

Como já comentado, são vários os meios utilizados para a consumação da conduta ilícita pelo agente, tais como websites, e-mails, redes sociais, malwares, sites falsos de comércio eletrônico ou de instituições bancárias, dentre tantas outras possibilidades. Esse é um fator extremamente importante para os próximos passos a serem dados pelo investigador responsável pelo caso, pois conforme for o meio adotado pelo cibercriminoso, diferentes serão as técnicas a serem utilizadas para a obtenção da identificação da autoria do delito.

Além de identificar o meio utilizado, o investigador deve observar as peculiaridades que destacam os indícios de tal modalidade delitiva. De modo geral, as evidências deixadas pelos crimes cibernéticos são extremamente instáveis, motivo pelo qual, em razão de seu caráter volátil, podem ser facilmente apagadas, alteradas ou perdidas, devendo o investigador agir com cautela para não corromper evidência alguma que possa ser relevante para a solução da investigação.

Normalmente, tais informações são complexas, exigindo-se uma maior capacidade técnica dos agentes investigativos para a correta coleta e compreensão das evidências dos crimes desta natureza.

Tais informações costumam aparecer envolvidas por uma enorme quantidade de dados legítimos, que não possuem relevo para a investigação, exigindo-se, desta forma, que os técnicos responsáveis pela sua coleta realizem uma análise apurada dos dados ali encontrados, separando os dados necessários à persecução penal.

Devido a praticidade da tecnologia de informações, muitas são as dificuldades enfrentadas pelos investigadores no processo de investigação dos crimes cibernéticos. Todavia, muitas soluções estão sendo procuradas, como a criação de leis específicas e uma melhor capacitação dos agentes responsáveis pela persecução penal, a fim de acompanhar o crescente desenvolvimento da tecnologia e o consequente surgimento de novas ameaças virtuais.

6.4 FALTA DE CAPACITAÇÃO TÉCNICA

A tecnologia de informações,detém uma grande complexidade e dinamismo sem igual, o que faz com que os órgãos investigativos e judiciários não estejam adequadamente preparados para lidar com esta nova criminalidade e a cada uma de suas repentinas mudanças.

Não muito dificilmente serão encontrados agentes públicos sem qualquer conhecimento sobre as tecnologias e das informações necessárias para uma melhor prestação da proteção estatal aos cidadãos nos órgãos responsáveis pela persecução penal.

Todavia, não é somente a capacitação técnicas dos agentes estatais que preocupa, vez que mesmo quando o agente possui o conhecimento técnico necessário, muitas vezes o trabalho investigativo esbarra na falta de equipamento necessário para um melhor desempenho nas investigações dos crimes cibernéticos, caracterizando uma falha do Estado, em seu sentido amplo, em propiciar uma melhor capacitação dos seus agentes com as armas necessárias ao combate ao crime virtual.

Sendo assim, é de extrema necessidade que haja uma melhor preparação dos agentes responsáveis pela persecução penal, bem como o desenvolvimento de uma melhor estrutura organizacional da polícia investigativa, a fim de que o Estado possa prestar a devida proteção aos cidadãos ao combater os cibercriminosos.

6.5 COMPUTAÇÃO NAS NUVENS (CLOUD COMPUTING)

Outra questão encontrada na investigação dos crimes virtuais é a chamada cloud computing, conhecida também como computação nas nuvens, este serviço permite o acesso e a consequente execução de arquivos e programas diretamente

pela internet, permitindo o acesso de todas as funcionalidades de um computador pessoal.

Consequência disso, os dados almejados não precisam estar, necessariamente, no computador do usuário, permitindo que este execute as mais diversas atividades, como acessar um arquivo de mídia ou executar um programa, sem que o tenha em seu computador, por meio de qualquer dispositivo de informática que possua acesso com a rede mundial de computadores, a internet.

Desta forma, os arquivos e programas acessados não estarão no computador do usuário, mas sim em servidores que hospedam esse tipo de serviço, ou seja, em computadores que possuem acesso permanente à rede com a finalidade específica de possibilitar o acesso de seu conteúdo pelos usuários que se utilizam de tal serviço.

A nuvem, ou seja, estes computadores acessados remotamente, podem, inclusive, estar localizados em outros países, ou seja, o usuário pode estar utilizando do serviço disponibilizado por esses servidores no Brasil, enquanto o computador responsável por prestar o acesso pode estar localizado em outro país.

Por fim, apesar de útil, esta tecnologia dificulta e muito a investigação, uma vez que dificilmente será possível apreender um computador que esteja em outro país, podendo vir a impossibilitar que se obtenha a prova da materialidade do delito cometido.

6.5 COOPERAÇÃO INTERNACIONAL MEDIANTE CONVENÇÕES E TRATADOS INTERNACIONAIS

O que antigamente levava-se meses para chegar ao conhecimento de um indivíduo, hoje pode ser acompanhado em tempo real. A rede é internacional, os seus usuários estão localizados em diferentes partes do mundo, permitindo a comunicação entre pessoas de diferentes nações que estejam em diferentes localidades.

Por isso, as práticas dos crimes também aderiram a tal característica de internacionalidade, passando as ameaças a serem globalizadas, permitindo o concurso de agentes que estejam localizados em diferentes países, que podem nem mesmo se conhecer, utilizando-se de recursos tecnológicos para a preparação e execuções de seus crimes.

Assim, devido à natureza transnacional da internet é necessário que haja uma melhor cooperação internacional entre os órgãos judiciários e investigativos de diferentes países que, hodiernamente, infelizmente é extremamente burocrática, posto que a internet é uma rede sem limites ou fronteiras, sendo que tais crimes

podem ser praticados em uma parte do planeta e o seu resultado ocorrer em outra.

A cooperação internacional entre os órgãos responsáveis pela persecução penal de diferentes países é hoje extremamente necessário, pois não há outra forma para se enfrentar uma modalidade criminosa que não conhece fronteiras, mas que, ainda assim, é praticada em um mundo que é politicamente dividido, com estruturas e culturas distintas. Caso contrário, não haverá como acompanhar a evolução dos crimes tecnológicos, tendo como consequência a impossibilidade de combater tal atividade delituosa (CAVALCANTE, 2013).

Assim, é necessário que o Brasil seja signatário de tratados que envolvam o combate aos crimes cibernéticos, em especial a Convenção sobre o Cibercrime, de 23 de novembro de 2001, também conhecida como Convenção de Budapeste, que é hoje o principal tratado internacional de direito penal e processual penal envolvendo os crimes cibernéticos e que tem por finalidade definir de forma harmônicas entre os países quais os crimes praticados mediante o uso da internet e qual as medidas a serem tomadas para a sua persecução.

7 **CONCLUSÃO**

Em que pese haver diversas outras medidas para a apuração dos crimes cometidos no ciberespaço, o presente trabalho objetivou trazer informações básicas acerca dos procedimentos investigativos adotados pelos agentes encarregados da persecução penal quando os crimes são praticados pelo meio virtual, sendo elas medidas necessárias a todo e qualquer processo investigativo que envolvam crimes dessa natureza.

Foram trazidas a essa análise algumas noções acerca de como foi criada e qual a função da internet, bem como informações acerca do conceito e classificação dos crimes cibernéticos, além de outros tipos de ameaças, com o intuito de oferecer ao leitor elementos necessários para uma melhor compreensão sobre a dificuldade em identificar a autoria do crime informático.

A internet é de fato uma das grandes obras modernas criadas pelo homem, simbolizando a capacidade de desenvolvimento do ser humano, sendo capaz de reduzir o tempo e espaço entre as pessoas em um momento em que a sociedade exige que tudo se movimente cada vez mais rápido e em maior quantidade, transformando-se em um instrumento do cotidiano da comunidade global, que cada vez mais necessita da versatilidade e agilidade que a internet oferece, sendo, hoje, impensável um mundo na qual a mesma não exista ou seja necessária.

Contudo, a internet, também é cercada de ameaças e de usuários mal intencionados que utilizam-se dela para a prática de suas condutas criminosas. Assim, se faz necessário que sejam tomadas medidas que garantam que a internet seja constituída em um ambiente saudável e livre de ameaças aos seus usuários.

A legislação nacional demonstrou alguns avanços nos últimos anos no que concerne à criação de leis que regulem o ambiente virtual, tal como o Marco Civil da Internet. Todavia, ainda é uma legislação tímida, carente de uma melhor regulamentação e maior precisão técnica, a fim de criar tipos penais específicos aos crimes virtuais para evitar que haja a impunidade dos agentes que se utilizam da internet para a prática de condutas ilícitas.

O Direito e a legislação devem tentar ser, se não mais rápidos, paralelamente evolutivos com a informatização, do contrário, as consequências por não conseguir acompanhar essa constante evolução poderá acarretar em situações irreversíveis. O que se percebe na tentativa legislativa para essa matéria é a inexperiência do legislador.

O Marco Civil da Internet não exige que a guarda de logs seja realizada por todos os provedores de acesso, inviabilizando que o investigador obtenha as informações necessárias para uma eficaz apuração dos crimes cibernéticos, por não

haver registrados de dados armazenados pelas provedores não obrigados por lei.

Ainda, é necessário que a regulamentação do ambiente virtual também abranja os locais com redes Wi-Fi abertas e sem controle, bem como o uso do serviço de internet nas denominadas lan houses e cyber cafés, exigindo-se que se tenha um registro dos usuários que se utilizam de tais serviços, possibilitando assim que haja a identificação da autoria do crime cometido com o uso da internet, com origem em tais locais.

Do mesmo modo, fica evidente a necessidade de que o Brasil seja signatário de tratados e convenções internacionais que versem sobre crimes de informática, como por exemplo a Convenção de Budapeste, uma vez que a própria internet tem por característica intrínseca a natureza transnacional, dependendo, muitas vezes, para que haja a efetiva prestação estatal ao combate dos crimes cibernéticos, do auxílio dos órgãos responsável pela persecução penal de outros países para prestarem as informações necessárias para que o Estado exerça o seu *jus puniendi*, vez que o ambiente virtual é atemporal e não se limita perante as fronteiras políticas criadas pelos homens.

Há a necessidade de que os órgãos responsáveis pela persecução penal, como as Polícias Civil e Federal, bem como o Poder Judiciário e o Ministério Público, instruam seus agentes acerca das infinitas possibilitadas trazidas pelo uso da internet e, consequentemente, das ameaças que nela estão presentes. É necessário que haja uma capacitação técnica específica, para que estejam preparados para lidar com as inúmeras adversidades e situações envolvendo os crimes virtuais, a fim de que possam, de forma eficaz, combater os criminosos virtuais, que sem dúvida alguma estão sempre atualizados acerca dos mecanismos disponíveis na rede para a prática de seus crimes.

Deve-se proporcionar instrumentos de trabalhos compatíveis com a nova realidade criminosa, vez que é evidente que, em diversas repartições públicas os equipamentos não possuem o mínimo de condições para acompanhar a evolução tecnológica.

Por fim, e não menos importante, é necessário que o Governo adote políticas públicas no sentido de conscientizar a comunidade em geral acerca do correto e ético uso dos serviços disponíveis na internet, bem como acerca das ameaças que nela espreitam e as formas de combatê-las.

Uma vez consciente acerca dos riscos apresentados pelo uso inconsequente da rede, bem como das maneiras pelas quais os criminosos se utilizam para concretizar o crime, os usuários estão mais capazes de se defender de ataques virtuais, diminuindo assim a probabilidade de sucesso das investidas dos criminosos no ambiente virtual, pois a prevenção é, sem dúvidas, uma das medidas mais eficientes ao combate dos crimes cibernéticos.

REFERÊNCIAS

. In: GRINOVER, Ada Pellegrini apud INELAS. **Gabriel Cesar Zaccarias de.**: Crimes na Internet. 2. ed. 2009, p. 138.

. In: PARIZATTO, João Roberto apud Idem. . **Ibidem**, p. 138.

ANDREUCCI, Ricardo Antônio. **Legislação Penal e Especial**. 7. ed. São Paulo: Saraiva, 2010.

ARAS, Vladimir. **Crimes de informática:**: Uma nova criminalidade. **JUS**. 2001. Disponível em: http://jus.com.br/artigos/2250. Acesso em: 6 Nov. 2019.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**. 3. ed. São Paulo: Saraiva, 2003.

BRASIL. Constituição. República Federativa do Brasil de 1988. Constituição: Federal. Brasília, DF: Senado Federal: Saraiva, 1988.

BRASIL. Presidência da República. Decreto-lei n. 2.848, de 07 de dezembro de 1940. Diário Oficial da União.

BRASIL. Presidência da República. Lei n. 10.406, de 10 de janeiro de 2002. Diário Oficial da União.

BRASIL. Presidência da República. Lei n. 12.737, de 30 de novembro de 2012. Diário Oficial da União. Brasília, 30 de novembro de 2012.

BRASIL. Presidência da República. Lei n. 12.965, de 23 de abril de 2014. Diário Oficial da União.

BRASIL. Senado. LEI n. 8.069, de 13 de julho de 1990. Diário Oficial da União. Brasília.

BROWN, Dan. **Fortaleza Digital**. 1. ed. Sextante, 2005. 336 p.

CABETTE, Eduardo. **Novos artigos no Código Penal**. Disponível em: http://atualidadesdodireito.com.br. Acesso em: 8 Nov. 2019.

CAVALCANTE, Waldek Fachinelli . **Crimes cibernéticos**: noções básicas de investigação e ameaças na internet. **JUS**. 2013. Disponível em: https://jus.com.br/artigos/25743/crimes-ciberneticos. Acesso em: 6 Nov. 2019.

COSTA, Marco Aurélio Rodrigues da. **Crimes de informática**. **JUS**. 1997. Disponível em: https://jus.com.br/artigos/1826/crimes-de-informatica . Acesso em: 6 Nov. 2019.

DORIGON, ALESSANDRO. **Crimes cibernéticos:**: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. **JUS**. São Paulo, 2018. Disponível em: https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade/4. Acesso em: 6 Nov. 2019.

ECOIT. **Crimes cibernéticos**: saiba onde denunciar caso você seja vítima. **Ecoit**. São Paulo. Disponível em: https://ecoit.com.br/crimes-ciberneticos/#targetText=Os%20crimes%20cibern%C3%A9ticos%20comuns%2C%20por,j%C3%A1%20tipificado%20pela%20lei%20penal%E2%80%9C.. Acesso em: 21 Out. 2019.

FERREIRA, Ivete Senise . **Direito & Internet:** : Aspectos Jurídicos Relevantes. 2. ed. São Paulo: Quartier Latin, 2005.

MARCOS ROQUE, SERGIO. **Criminalidade informática**: Os criminosos do computador. São Paulo: ADPESP Cultural, 2007.

MENDES, Carolina de Aguiar Teixeira. **Como surgiu a internet?**. **Brasil Escola**. São Paulo. Disponível em: https://brasilescola.uol.com.br/curiosidades/como-surgiu-a-internet.htm . Acesso em: 7 Out. 2019.

MINISTÉRIO PÚBLICO FEDERAL. **CRIMES CIBERNÉTICOS**: MANUAL PRÁTICO DE INVESTIGAÇÃO. **MPPA**. São Paulo, 2006. 100 p. Disponível em: https://www2.mppa.mp.br/sistemas/gcsubsites/upload/60/ManuaL%20Pr%C3%83%C2%A1tico%20de%20Investiga%C3%83%C2%A7%C3%83%C2%A3o%20sobre%20Crimes%20de%20Inform%C3%83%C2%A1tica.PDF. Acesso em: 6 Nov. 2019.

NETO, Mario Furlaneto . **Crimes na internet e inquérito policial eletrônico**: Mario Furlaneto Neto, José Eduardo Lourenço dos Santos, Eron Veríssimo Gimenes. 1. ed. São Paulo: Edipro, 2012.

NUCCI, Guilherme de Souza. **Código Penal Comentado**. 4. ed. São Paulo: Revista dos Tribunais, 2005.

PENTEADO, Jaques de Camargo (Coord.). **Justiça Penal**: Críticas e sugestões. 1. ed. São Paulo: Revista dos Tribunais, 1994. 95 p.

PINHEIRO, Reginaldo César. **Os cybercrimes na esfera jurídica brasileira**. **JUS**. 2000. Disponível em: https://jus.com.br/artigos/1830/os-cybercrimes-na-esfera-juridica-brasileira. Acesso em: 8 Nov. 2019.

ROSA, Fabrízio. **CRIMES DE INFORMÁTICA**. 2. ed. Campinas: Bookseller, f. 140, 2005. 142 p.

RUTHERFORD SANTOS DO NASCIMENTO, Esp. Mikhail. **Crimes na internet: falta de normatização, dificuldades na regulamentação e entendimentos sobre o assunto**. **JusBrasil**. São Paulo, 2015. Disponível em: https://mikhail.jusbrasil.com.br/artigos/234313175/crimes-na-internet-falta-de-normatizacao-dificuldades-na-regulamentacao-e-entendimentos-sobre-o-assunto. Acesso em: 5 Nov. 2019.

SCHMIDT, Guilherme. **Crimes Cibernéticos**. **JusBrasil**. 2014. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. Acesso em: 20 Out. 2019.

SILVA, Leonardo Werner . **Internet foi criada em 1969 com o nome de "Arpanet" nos EUA**. **Folha de São Paulo**. São Paulo, 2001. Disponível em:

https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml . Acesso em: 7 Out. 2019.

VIEIRA, Jair Lot. **Crimes na internet interpretados por tribunais**: Repertório de jurisprudência e legislação. 1. ed. Bauru, SP: Edipro, 2009. 342 p.

WENDT; JORGE, EMERSON; IGOR VINICIUS NOGUEIRA. **Crimes cibernéticos:** : Ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: BRASPORT, 2013.