FABIANA DI LÚCIA DA SILVA PEIXOTO

DOS CRIMES PRATICADOS POR MEIO DO COMPUTADOR

(Uma abordagem dos critérios de fixação de competência para julgamento de tais práticas)

Brasília – DF

2013

FABIANA DI LÚCIA DA SILVA PEIXOTO

DOS CRIMES PRATICADOS POR MEIO DO COMPUTADOR

(Uma abordagem dos critérios de fixação de competência para julgamento de tais práticas)

Monografia apresentada como requisito parcial à obtenção de título de especialista em Direito Constitucional, no Curso de Pós Graduação *Latu Sensu* do Instituto Brasiliense de Direito Público - IDP.

Orientador (a):

Brasília – DF

2013

FABIANA DI LÚCIA DA SILVA PEIXOTO

DOS CRIMES PRATICADOS POR MEIO DO COMPUTADOR

(Uma abordagem dos critérios de fixação de competência para julgamento de tais práticas)

Monografia apresentada como requisito parcial à obtenção de título de especialista em Direito Constitucional, no Curso de Pós Graduação *Latu Sensu* do Instituto Brasiliense de Direito Público - IDP.

Orientador (a):

Aprovado pelos membros da banca examinadora em __/__/__, com menção____(_____).

Banca Examinadora:

_____

Presidente: Prof.

_____

Integrante: Prof.

_____

Integrante: Prof.

RESUMO

Juntamente ao avanço da tecnologia informática e sua influência em quase todas as áreas da vida social, surgem novos meios para o cometimento de quase todos os crimes. O sistema informático é um meio para alcançar o fim almejado quando se trata de ações lesivas a informações referentes ao patrimônio, à honra, à um arquivo literário refletindo um direito autoral etc. Importante se faz, num primeiro momento, analisar e determinar que tipo de bem é a informação contida em um sistema informático, que na verdade é um bem intangível especial que deve ser tratado de forma autônoma, haja vista que se trata de um bem tão valioso quanto um bem corpóreo. Atualmente, convivemos com condutas envolvendo meios eletrônicos, que necessitam de enquadramento em tipos penais, bem como a fixação da competência para julgamento de tais delitos, ante a divergência doutrinária, para que assim possa se efetivar a prevenção e repressão no tocante a tais condutas.

Palavra-chave: computador, delitos, competência.

ABSTRACT

Along with the advancement of computer technology and its influence on almost all areas of social life, there are new ways to commit almost any crime. The computer system is a means to achieve the desired end when it comes to actions detrimental to information concerning the property, honor, a file literary reflecting a copyright etc.. Becomes important, at first, to analyze and determine what kind of good is the information contained in a computer system, which is actually an intangible special that should be treated independently, given that it is such a valuable asset as tangible.Currently we live with pipelines involving electronic media, needing framework for criminal offenses, as well as establishing the jurisdiction for trial of such offenses, compared doctrinal divergence, so that it can be effective prevention and repression in relation to such conduct.

Key words: computer, crimes, competence.

“Alguns qualificam o espaço cibernético como um novo mundo, um mundo virtual, mas não podemos nos equivocar. Não há dois mundos diferentes, um real e outro virtual, mas apenas um, no qual se deve aplicar e respeitar os mesmos valores de liberdade e dignidade da pessoa".

(Jacques Chirac)

SUMÁRIO

INTRODUÇÃO

Até a década de 1980, o uso da internet não era acessível a todas as pessoas, se restringindo às universidades e agências governamentais. No entanto, o avanço tecnológico e a democratização no acesso à internet têm permitido a comunicação de diversas formas, que tanto pode ser por escrito quanto por transmissão virtual em tempo real. Graças ao surgimento e a popularização do mundo virtual, diversas barreiras, sejam físicas ou linguísticas, vêm se rompendo. Neste sentido, podemos dizer que a internet é um foro de troca de idéias e de conhecimento.

A democratização do acesso à internet, assim como a produção em série de diversos tipos de computador, com os mais variados preços, cada vez mais acessível à população, vem permitindo a propagação da prática de condutas ilícitas no âmbito da informática. Neste sentido é que surge a necessidade da adequação de tais condutas com o nosso ordenamento jurídico penal, a fim de resguardar a inviolabilidade de bens jurídicos tradicionalmente protegidos.

Assim, é comum que com o uso da internet haja também, o abuso. Neste sentido, diversos indivíduos a utilizam como um meio para a prática de delitos das mais variadas espécies, atingindo diversos bens jurídicos tutelados pelo direito penal, tais como a vida, a propriedade, a honra etc.

O direito penal, assim como os demais ramos do direito, tem seu fundamento nas relações humanas. Estas relações sofrem constantes mudanças e assim, são objetos de constantes adaptações que devem ser feitas no âmbito do direito penal no sentido de adequá-las aos nossos ordenamentos jurídicos vigentes. Neste sentido, as mudanças e os avanços no mundo tecnológico trazem a problemática relativa à criação ou readaptação do ordenamento penal para a proteção desses bens jurídicos que possam ser atingidos criminosamente através do uso da internet.

Na adequação de tais práticas é necessário o respeito a alguns princípios constitucionais, e em especial, ao da Legalidade, onde estabelece que “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”. A descrição do tipo penal há de ser especifica é individualizada do comportamento criminoso, sob pena de

não atingir uma garantia real e efetiva. Deve ser estabelecido anteriormente ao fato todas os elementos norteadores do tipo penal.

E por ser a internet hoje um dos principais meios de cometimentos de delitos e por possuir um potencial lesivo ilimitado onde o agente não precisa deslocar-se para o local do crime para que sua pretensão seja atingida é importante analisar como será julgado alguém que cometer um delito que produzir resultados em diversas esferas jurisdicionais, principalmente quando este não se encontrar em território nacional? Há grande divergência doutrinária e jurisprudencial no tocante ao assunto, visto que para alguns o melhor critério é o da teoria da atividade, fixando ao juízo do local da ação a responsabilidade de julgar o infrator, para outros o melhor critério é a fixação através da teoria do resultado, principalmente no que tange à litispendência processual.

A idéia do presente trabalho é a de abordar alguns aspectos acerca dos crimes praticados por meio da internet. Primeiramente trataremos da evolução histórica da informática, em seguida da relação do direito penal com a informática, abrangendo a análise do bem jurídico tutelado pelo direito penal no âmbito das condutas praticadas através da internet e, dos princípios que devem ser obedecidos no momento da aplicação da lei penal. No terceiro momento, trataremos do conceito, classificação e espécies delitivas no que se refere a tais condutas. E por fim, explicar os critérios de fixação da competência no âmbito do Código de Processo Penal para o julgamento de tais práticas.

Usaremos neste trabalho a expressão “crimes praticados por meio do computador”, porém, devemos considerar a ampla tecnologia hoje existente como *tablets* e celulares, que podem ser meios de acesso à internet, bem como espaço de cometimentos de delitos.

1. EVOLUÇÃO HISTÓRICA DA INFORMÁTICA

Tendo em vista que o objeto do presente estudo é observar a questão criminal e os aspectos envolvidos nas interações virtuais em redes sociais e a sua relação com a prática em diversos delitos a fim de fixar a sua competência para julgamento.

Porém, antes de examinar o crime, a questão probatória, a competência e outros aspetos relacionados aos delitos em questão, necessário se faz relatar sucintamente a definição de computadores, internet e redes sociais, bem como as principais terminologias utilizadas.

1.1 Origem dos computadores

Durante a segunda Guerra Mundial houve a necessidade de se controlar os estoques de materiais bélicos, ou seja, era necessário calcular a tabela de artilharia para cada lote de munição que fosse fabricado. Em face disso, em lugares do mundo, tais como os EUA, Alemanha e Inglaterra, via-se a busca pelo desenvolvimento tecnológico com o intuito de colocar esse novo tipo de arma à disposição do arsenal moderno. Neste momento então, surgiu o primeiro computador eletromecânico, o AutomaticSequenceControlledCalculator que recebeu o nome de Mark I.

O primeiro computador de grande porte foi desenvolvido em laboratórios universitários no EUA e, depois, na Inglaterra. Foi criado por John PresperEckert e John W. Mauchly, na Universidade da Pensilvânia para resolver problemas balísticos, entre 1934 e 1946 e chamava-se Electronic, Numeric, IntegratorandCalculator (ENIAC). Mas a verdade é que, em outubro de 1973, a justiça norte-americana reconheceu como o verdadeiro inventor do computador John Atasanoff, da Universidade Iowa. Ele construiu

um calculador binário chamado ABC, que se diferencia basicamente do ENIAC por ser não-automático e não-programável[1].

Aldemário Araújo cita que[2]:

> Outra classificação muito frequente dos computadores é aquela que identifica as seguintes gerações (refletindo a evolução dos componentes básicos da máquina):
> a) primeira (1940-1952): quando os computadores eram constituídos de válvulas e quilômetros de fios, gerando equipamentos lentos, enormes e com produção de bastante calor;
> b) segunda (1952-1964): quando as válvulas foram substituídas por transistores;
> c) terceira (1964 - 1971): quando os computadores passaram a ser construídos com circuitos integrados (conjunto de milhares ou milhões de transistores, resistores e capacitores construídos sobre um *chip* a base de silício);
> d) quarta (a partir de 1971): quando surge o microprocessador (um processador de computador em um *microchip*).

O computador possui dois elementos principais: o *hardware* e o *software*. O primeiro consiste na parte física. Já o segundo, são os programas que viabilizam a realização de determinadas tarefas. Ele realiza quatro operações fundamentais: entrada, processamento, armazenagem e saída de informações. Atualmente a internet é o componente principal de utilização de um computador.

1.2 Conceito e origem da Internet

A internet é uma rede de computadores e outras redes menores interligados ou conectados entre si em escala mundial através de um protocolo comum chamado TCP/IP (*TransmissionControlProtocol/Internet Protocol*). Com isso temos a referência direta e resumida da internet como sendo a **rede mundial de computadores.** Podemos definir Internet como uma gigantesca rede mundial de computadores, interligados por

[1]SILVA, Rita de Cássia Lopes. **Direito Penal E Sistema Informático** – Ed. Revista dos Tribunais, páginas 17 e 18.
[2] CASTRO, Adelmario Araújo – **Livro Eletrônico** – Noções de Informática, capítulo III, disponível em: http//:www.aldemario.adv.br

linhas comuns de telefone, linhas de comunicação privadas, cabos submarinos, canais de satélite e diversos outros meios de telecomunicação[3].

A internet teve sua origem nos anos 60,durante a Guerra Fria entre duas importantes potências mundiais, os EUA e a União Soviética. As inovações na manipulação de dados eletrônicos provinham principalmente de iniciativas militares. No Departamento de Defesa Americano, estudava-se como melhor proteger os importantes dados militares. Mesmo no caso de um ataque inimigo, os dados não deveriam ser destruídos. A única solução viável era uma rede eletrônica de dados. Os mesmos dados deveriam estar armazenados em diversos computadores, distantes uns dos outros. Quando houvesse modificações, os dados deveriam ser atualizados em todos os computadores no menor espaço de tempo possível. Cada computador deveria ter várias opções de vias de comunicação com todos os outros. Desta forma, a rede continuaria funcionando mesmo que um computador ou uma via de comunicação fossem destruídos.

No entanto, a decolagem da Internet ocorreu no ano de 1973, quando VindonCerf, do Departamento de Pesquisa avançada da Universidade da Califórnia e responsável pelo projeto, registrou o (protocolo TCP/IP) Protocolo de Controle da Transmissão/Protocolo Internet; trata-se de um código que consente aos diversos networks incompatíveis por programas e sistemas comunicarem-se entre si.

A internet é hoje a ferramenta mais utilizada no mundo para disseminação da informação, e isto modificou a forma como as pessoas se comunicam de tal forma que nenhuma outra invenção teve o condão de alterar. Além do grande poder de construção intelectual a partir da intensa comunicação entre os indivíduos é vista como um meio de comunicação que interliga dezenas de milhões de computadores do mundo inteiro e permite o acesso a uma quantidade de informações praticamente inesgotáveis, anulando toda distância de lugar e tempo.

1.3 Redes Sociais

[3] CASTRO, Adelmario Araújo – **Livro Eletrônico** – Noções de Informática, capítulo V, disponível em: http//:www.aldemario.adv.br acesso em 15 de março de 2013.

As redes sociais é uma estrutura social composta por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns. Uma das características fundamentais na definição das redes é a sua abertura e porosidade, possibilitando relacionamentos horizontais e não hierárquicos entre os participantes.

As redes sociais constituem um modelo basilar de organização de todo e qualquer sistema vivente. Neste sentido, o físico e teórico de sistemas Capra em tópico abordou a ampliação da hipótese sistêmica, mencionou a importância para a compreensão da lógica da vida, considerando sua aplicação na esfera social, *in verbis*:

> O padrão de rede (network pattern), especificamente, é um dos padrões de organização mais básicos de todos os sistemas vivos. Em todos os níveis de vida desde as redes metabólicas das células até as teias alimentares dos ecossistemas, os componentes e os processos dos sistemas vivos se interligam em forma de rede.
> A aplicação da compreensão sistêmica da vida ao domínio social, portanto, identifica-se à aplicação de nossos conhecimentos dos padrões e princípios básicos de organização da vida e, em específico, da nossa compreensão das redes vivas à realidade social[4].

As redes sociais têm adquirido importância crescente na sociedade moderna. São caracterizadas primariamente pela autogeração de seu desenho, pela sua horizontalidade e sua descentralização.

Um ponto em comum dentre os diversos tipos de rede social é o compartilhamento de informações, conhecimentos, interesses e esforços em busca de objetivos comuns. A intensificação da formação das redes sociais, nesse sentido, reflete um processo de fortalecimento da Sociedade Civil, em um contexto de maior participação democrática e mobilização social.

1.4 Terminologias utilizadas na Informática

[4] CAPRA, Fritjof. As conexões ocultas: ciência para uma vida sustentável. 2. ed. São Paulo: Cultrix, 2002, p. 93.

Para o estudo da presente obra é necessário o entendimento de determinadas terminologias citadas posteriormente no presente trabalho, dentre elas:

a) Informática: É a ciência que estuda as formas *automáticas* de coleta, processamento, conservação, recuperação e disseminação da informação. Atualmente, o tratamento automático da informação faz-se preponderantemente por meio de técnicas eletrônicas (uso do computador eletrônico).

b) Programa: É uma sequência de instruções em uma linguagem, que faz o computador realizar determinada ou determinadas tarefas.

c) Hacker: Em inglês, o verbo *hack* significa cavar, fuçar. O sentido exato de hacker é esse: um sujeito curioso, que entende de informática e eletrônica, que vira e revira um computador e programas para saber como eles funcionam.

d) Web: Termo alternativo para designar a Internet.

e) Redes: São sistemas compostos por computadores interligados. Na rede clássica, os vários computadores interligados utilizam recursos de um computador especial conhecido como servidor. Por intermédio de cada computador em rede é possível compartilhar e trocar informações e recursos, inclusive periféricos. A otimização do trabalho coletivo e a redução de custos são fortes atrativos para a instalação de redes.

f) Hardware: Consiste na parte física do computador, podendo ser o teclado, o mouse, o monitor etc.

g) Software: É um conjunto de programas, procedimentos e de documentação relativa à operação de um sistema de processamento de dados.

h) Telemática: É a ciência que trata da manipulação e utilização da informação por meio do uso combinado de computadores (eletrônicos) e meios de telecomunicação.

i) Protocolos: Existem aos montes e são usados na comunicação entre computadores. Determina como será o “dialogo” entre as máquinas, como os dados e arquivos serão passados de um lado para o outro, como será a verificação de erros etc.

2. DA RELAÇÃO DO DIREITO PENAL COM A INFORMÁTICA

Diante das gigantescas mutações introduzidas pela globalização, que escapam do tradicional controle político e jurídico, em razão das evoluções dos meios de cometimentos de práticas delitivas a sociedade atingiu um novo estágio de desenvolvimento, a Era da Informática. Essa revolução modificou principalmente a forma de comunicação entre as pessoas, mas não se restringe somente a isso. Como será abordado adiante, todas as relações interpessoais foram modificadas, inclusive aquelas nocivas à sociedade.

2.1. Bem jurídico tutelado pelo direito penal no âmbito das condutas praticadas por meio do computador

A partir da noção tridimensionalista formulado por Miguel Reale[5], verificamos que o fenômeno jurídico é formado por um tríplice aspecto, qual seja fato, valor e norma, integrados em uma unidade funcional e de processo. Já a ciência do Direito é uma ciência histórico-cultural que tem por objeto a experiência social, enquanto esta normatividade se desenvolve em função de fatos e valores para a realização da convivência humana. Devido à modificação constante na valoração dos bens jurídicos podemos dizer que o Direito é, portanto, uma ciência dinâmica e não estática, configurando em um sistema aberto e não fechado. Desta feita, surge certa dificuldade no tocante à conceituação do bem jurídico, sempre levando em conta que da mesma forma que o direito, o conceito de bem jurídico não é estático, mas dinâmico e aberto às

[5]**Teoria Tridimensional do Direito**, 5ª ed., São Paulo: Saraiva, 2003, p. 123.

mudanças sociais e ao avanço cientifico. Por isso o seu conceito é mutável de acordo com a evolução do homem, da sociedade e do Estado.[6]

Entretanto, podemos considerar que na concepção jurídica, a expressão *bem jurídico,* designa tudo aquilo com que possa se satisfazer uma necessidade humana e que possa ter valor reconhecido para o Direito. Um bem jurídico, para ser protegido, deve ser definido e delineado de modo a que se autorize sua tutela pelo direito penal, valendo ressaltar que não é qualquer lesão que acarretará a atuação do Direito Penal, mas apenas aquelas lesões ou ameaças de lesões consideradas relevantes e justificadoras da sanção penal. Sendo que também é dever do Direito Penal a proteção de bens jurídicos tradicionalmente reconhecidos e lesionados com o uso da informática, bem como a proteção de outros valores jurídicos recentes havidos com o advento e proliferação dos computadores.

Desta feita, para delimitar em que sentido será feita a proteção penal no âmbito do direito informático, necessário se faz demonstrar qual o bem jurídico que será penalmente tutelado nesta área, verificando sempre, se há amparo no ordenamento jurídico pátrio e que esse amparo feito pelo direito somente deve ser concretizado na preservação dos bens mais relevantes e imprescindíveis nas relações sociais, sempre dentro dos limites da intervenção mínima.

No tocante aos bens que podem ser atingidos com os delitos informáticos, consideramos que há dois grandes grupos merecedores de amparo específico pelo Direito Penal. Sendo o primeiro relacionado às condutas utilizando meios computadorizados para atacar bens jurídicos já tradicionalmente protegidos, isto é, referente a infrações penais comuns, onde os atentados perpetrados são contra a honra, o patrimônio, a Administração Pública e fé pública, a segurança nacional e a diversos outros direitos individuais. Já o segundo grupo refere-se a uma criminalidade informática onde as condutas recaem sobre objetos informáticos propriamente ditos, tais como hardwares, programas, dados, documentos eletrônicos etc.

Saliente-se que deve ser levado em consideração pelo Direito Penal que os dados eletrônicos, matéria prima para as operações computacionais são bens materiais

---

[6]SMANIO, GianpaoloPoggio, **O Bem Jurídico e a Constituição Federal**, disponível em: http://jus2.uol.com.br, acesso em 21 de abril de 2013.

intangíveis, que não podem ser facilmente transportados de um lado para o outro pelas formas tradicionalmente reconhecidas, trazendo assim, uma evidente vulnerabilidade a esses. Por tudo isso, por seu caráter imaterial, deve ser criado e mantido algum sistema de proteção penal, com a finalidade de desenvolver cuidados jurídicos específicos ao material informático.

Notadamente, o que separa os crimes praticados por computador dos crimes comuns é o instrumento utilizado para alcançar e manipular um sistema em proveito próprio ou para lesionar outrem. De outro lado, não podemos negar que mesmo os crimes comuns, no mais das vezes, também se utilizam de um meio ou instrumento que possibilite ou facilite a execução, como por exemplo, a utilização de chave falsa, da arma de fogo etc.

No tocante aos crimes comuns, a nossa legislação penal, possui ajustes relativos ao aumento de pena pela maior gravidade da conduta e ainda, pelos meios empregados pelo o infrator.

Porém, no que se refere aos fatos delituosos cometidos por meio computadorizado, surge a dificuldade na averiguação e na obtenção de prova substancial de tais delitos, destacando ainda a dificuldade de questões de cunho processuais, como a definição de competência para a apuração de delitos transnacionais e efetivação de perícias e outras.

2.2 Princípio da Legalidade

Considerando que a lei é a fonte imediata de conhecimento do Direito Penal, temos que a lei penal é o pressuposto das infrações e das sanções. Sendo assim, o Estado não pode castigar um comportamento que não esteja descrito em suas leis, nem punir o cidadão quando inexistir sanção jurídica cominada ao delito. De acordo com o art. 5º, inciso II, da Constituição Federal é dito que ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei. Ou seja, somente através de espécies normativas devidamente elaboradas é que se pode criar obrigações para o indivíduo. Tal

princípio visa evitar e combater o poder arbitrário do Estado. Trata-se de uma base direta da própria noção de Estado de Direito, implantada com o advento do Constitucionalismo, expressando então, a vontade geral.

Conforme salientam Celso Bastos e Ives Gandra Martins, no fundo, portanto, o princípio da legalidade mais se aproxima de uma garantia constitucional do que de um direito individual, já que ele não tutela, especificamente, um bem da vida, mas assegura ao particular a prerrogativa de repelir as injunções que lhe sejam impostas por uma outra via que não seja a da lei, pois como já afirmava Aristóteles, "a paixão perverte os Magistrados e os melhores homens: a inteligência sem paixão – eis a lei".[7]

2.2.1 Distinção entre o Princípio da Legalidade e o da Reserva Legal

Segundo Jose Afonso da Silva, o princípio da legalidade significa a submissão e o respeito à lei, ou a atuação dentro da esfera estabelecida pelo legislador. Já o princípio da reserva legal consiste em estatuir que a regulamentação de determinadas matérias haja de fazer-se necessariamente por lei formal. Desta feita afirma ainda, que o princípio da legalidade poderá ser satisfeito não somente com a expedição de lei formal, mas também, pela "atuação dentro da esfera estabelecida pelo legislador", o que dá margem à expedição de atos infralegais, nos limites fixados pelo legislador, que estabeleçam obrigações de fazer ou não-fazer.

Afirma Alexandre de Moraes, que o princípio da legalidade é de abrangência mais ampla do que o princípio da reserva legal. Por ele fica certo que qualquer comando jurídico impondo comportamentos forçados há de provir de uma das espécies normativas devidamente elaboradas conforme as regras e processo legislativo constitucional. Já o princípio da reserva legal opera de maneira mais restrita e diversa, não sendo este genérico e abstrato, mas concreto. Ele incide tão-somente sobre os campos materiais especificados pela Constituição. Se todos os comportamentos humanos estão sujeitos ao princípio da legalidade, somente alguns estão submetidos ao da reserva da lei. Este é, portanto, de

[7] Moraes, Alexandre de. **Direito Constitucional** 17ª ed., p. 36.

menor abrangência, mas de maior densidade ou conteúdo, visto exigir o tratamento de matéria exclusivamente pelo legislativo, sem participação normativa do Executivo. [8]

Sendo assim, tais princípios têm significado político, no sentido de ser uma garantia constitucional dos direitos do homem. Constitui a garantia fundamental da liberdade civil, que não consiste em fazer tudo o que se quer, mas somente aquilo que a lei permite. À lei e somente ela compete fixar as limitações que destacam a atividade criminosa da atividade legítima. Esta é a condição de segurança e liberdade individual assegurados em nosso ordenamento constitucional, a fim de evitar abusos por parte do Estado.

2.2.2 O Princípio da Legalidade e a Anterioridade da Lei

2.3 Do uso da Analogia no Direito Penal

Como visto no tópico anterior o princípio legalidade é o princípio primordial que rege o Direito Penal pátrio. Segundo este preceito apenas serão puníveis as condutas reprováveis que estiverem em clara e expressamente previstas em lei, sendo proibido o estendimento do tipo penal para abranger situações originalmente não previstas. Sendo assim, a lei penal se interpreta de forma restrita, não podendo a definição dos crimes e contravenções ser vaga, incerta, duvidosa ou determinada.

Decorrência direta do princípio da legalidade e do princípio da reserva legal é a vedação do uso da analogia *in malam partem,* isto é, interpretação que de qualquer forma prejudique o agente do delito. Sendo assim, a partir de uma determinada hipótese criminosa não se pode, em situações semelhantes, invocar a aplicação da referida lei e imputar como crime.

A criação de novos tipos penais não se faz possível através do uso da analogia, tampouco para conceber penas que não estejam expressamente previstas em lei. E os

[8] Op. cit. P. 37.

delitos praticados por meio do computador que não tiver expressa e anterior previsão em lei, não poderão ser invocados para serem aplicados num caso concreto.

3 CRIMES PRATICADOS POR MEIO DO COMPUTADOR

A Internet é hoje um dos principais meios de cometimento de práticas delitivas e que possui um potencial lesivo ilimitado, posto que o agente não precisa deslocar-se para o local do crime para que sua pretensão seja atingida.

3.1 Conceito

O avanço tecnológico cada vez mais vem permitindo que, por meio da informática sejam desenvolvidas diversas atividades individuais e coletivas, e, no tocante ao direito penal, vem colocando novos instrumentos nas mãos dos criminosos, cujo alcance não foi corretamente avaliado, haja vista que a cada dia surgem novas modalidades lesivas a diversos bens e interesses que o Estado deve tutelar, propiciando a formação de uma criminalidade específica de informática, onde cada vez mais tem sido alargada.

Num primeiro momento, necessário se faz a correta utilização de uma denominação aos crimes praticados por meio do computador, e aqui não será usada nenhuma das nomenclaturas por especifica, haja vista de não haver uma legislação vigente que preceitua o termo a ser utilizado corretamente para tais condutas, mas em diversas obras são chamados de *crimes eletrônicos*, *crimes de computador*, *crimes de informática*, *crimes cibernéticos*, *crimes telemáticos etc.*

Marco Aurélio Costa define como sendo crime de computador[9], *in verbis:*

[9] DA COSTA, Marco AurélioRodrigues. "**Crimes de Informática**". Revista Eletrônica Jus Navigandi (online). Disponível na internet via: http://www.jus.com.br/doutrina/crinfo.html.

> a conduta que atenta contra o estado natural dos dados e dos recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar. Isto posto, depreende-se que o crime de informática é todo aquele procedimento que atenta contra os dados, que o faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão. Assim, o crime de informática pressupõe dois elementos indissolúveis: contra os dados que estejam reparados às operações do computador e, também, através do computador, utilizando-se um software e hardware, para perpetrá-los. Conclui-se que aquele que ateia fogo em sala que estiverem computadores com dados, com o objetivo de destruí-los, não comete crime de informática, do mesmo modo, aquele que, utilizando-se de computador, emana ordem a outros equipamentos e cause, por exemplo, a morte de alguém. Estará cometendo homicídio e não crime de informática.

O mesmo autor denomina de "criminalidade informática" todas as formas de comportamento ilegal, que venham a, de qualquer forma, provocar danos sociais, por intermédio de um computador.

Podendo ainda ser definido como:

> [...] aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador. Inclui-se neste conceito os delitos praticados através da internet, pois o pressuposto para acessar a rede é a utilização de um computador.[10]

Segundo Patrícia Peck[11], os crimes digitais podem ser conceituados como sendo às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros.

---

[10] CASTRO. Carla Rodrigues Araújo De. **Crimes de Informática e Seus Aspectos Processuais**. Pág. 9. 2ª Edição. Ed.Lumem Juris.

[11] PINHEIRO, Patrícia Peck. Direito Digital. 4. Ed. São Paulo: Saraiva, 2010.p.46.

3.2 Classificação

Aldemario Araújo Castro que define tais condutas como crimes de informática, cita três modalidades no tocante ao objetivo material como critério[12], in verbis:

> **Crime de informática puro:** onde o agente visa o sistema de informática, em todas as suas formas ou manifestações. Exemplo: acesso indevido aos dados e sistemas contidos no computador;
>
> **Crime de informática misto:** onde o agente não visa o sistema de informática, mas a informática é instrumento indispensável para consumação da ação criminosa. Exemplo: transferência de fundos de uma consta bancaria para outra (pressupondo que os registros bancários existem somente na forma de dados de sistemas informatizados);
>
> **Crime de informática comum:** onde o agente não visa o sistema de informática, mas usa a informática como instrumento (não essencial, poderia ser outro o meio) de realização da ação. Exemplo: acionamento de uma bomba por sistemas de computadores.

Ressalta ainda, que a classificação apresentada demonstra claramente que os problemas mais significativos dos crimes de informática residem basicamente nos chamados crimes de informática puros.

Damásio de Jesus e Gianpaolo Smanio classificam tais crimes como[13]:

> *puros* (ou próprios) e *impuros* (ou impróprios), sendo que os primeiros seriam os delitos praticados por computador que se realizes ou se consumem em meio eletrônico. As ações delituosas se manifestam por atentados à integridade física do sistema ou pelo acesso não autorizado ao computador e aos dados nele contidos. O agente visa especificamente danos ao sistema de informática em todas as suas formas (*hardwares*, *softwares*, *dados e sistemas).* Já os impróprios

---

[12]Aldemario Araújo Castro, Livro Eletrônico, Capítulo 18, **Crimes de Informática**, disponível em: http://www.aldemario.adv.br, acesso em 16 de março de 2013.

[13] JESUS, Damásio E. eSmanio, GianpaoloPoggio. In: Internet: **cenas de sexo explícito envolvendo menores e adolescentes – aspectos civis e penais**. Revista do Conselho Nacional de Política Criminal e Penitenciária. Brasília: vol. 1, n. 9, p. 27-29. Janeiro/junho 1997 (apud) LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**, Ed. Millenium, Campinas/SP, 2006.

> seriam aqueles 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, diversos da informática, sendo o bem penal juridicamente protegido é diverso da informática, porém o sistema de informática é ferramenta essencial para a consumação.

Porém, talvez a melhor sistematização é a apresentada por Vicente Greco Filho[14], neste sentido, *in verbis:*

> focalizando-se a internet, há dois pontos de vista a considerar, crimes ou ações que merecem incriminação praticados por meio da internet e crimes ou ações que merecem incriminação praticados contra a internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre esses crimes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, como por exemplo, o homicídio. O crime, no caso, é provocar o resultado morte, qualquer que tenha sido ou meio ou a ação que o causou.

Complementa Fragoso, que denominação dos delitos deve ser feita de acordo com o bem jurídico protegido[15]:

> A Classificação dos crimes na parte especial do código é questão ativa, e é feita com base no bem jurídico tutelado pela lei penal, ou seja, a objetividade jurídica dos vários delitos ou das diversas classes de intenções.

Portanto, ao analisar um crime como sendo de informática, é necessário uma analise inicial, primeiramente para verificar se o esmo é um cibercrime ou não, e depois aplicar o tipo penal correspondente, tendo em vista o bem jurídico tutelado, para assim adequar às espécies delitivas e normativas.

---

[14] Greco Filho, Vicente. "**Algumas observações sobre o direito penal e a internet**". Boletim IBCCRIM, edição especial. Ano 8, n. 95, outubro de 2000.

[15]FRAGOSO, Heleno Cláudio. Lições de direito penal: parte especial: arts. 121 a 212 do CP. Rio de Janeiro: Forense, 1983.p.5.

3.3 Das Espécies Delitivas

Sabemos que, modernamente, diversas são as possibilidades de se verificar as várias ações criminosas no ambiente informático. No tocante a seara cível pode ser pleiteada a reparação de danos, por via responsabilidade civil, advinda do direito obrigacional. Porém, o maior problema é visto no campo do direito penal, uma vez que, não há no Brasil uma legislação que abarque todas as condutas ilícitas praticadas no mundo virtual face à modernização de tais condutas e o fato de o Código Penal de 1940 não ter acompanhado tais avanços tecnológicos. Tais delitos, conforme já conceituados e classificados e, considerando o bem jurídico penalmente tutelado, importante é identificar e mencioná-los quanto à possibilidade de tipificação.

Com o advento da Lei 12.737/12, popularmente conhecida como Lei Carolina Dieckman, apenas algumas condutas foram previstas no Código Penal. Sendo assim, os crimes praticados por meio do computador encontram no Código Penal Brasileiro e em outros ordenamentos Jurídicos, tais como o Estatuto da Criança e Adolescente, várias possibilidades de repressão penal, variando o seu enquadramento de acordo com o objeto material, ou seja, o bem jurídico penalmente tutelado que o agente pretenda atingir.

3.3.1 Os crimes praticados por computador e o Código Penal

Existem diversos crimes previstos no Código Penal que, em tese, podem ser praticados por intermédio do computador, entre os quais se encontram:

a) **Do estelionato e outras fraudes previstos no Capítulo VI do Código Penal:** o estelionato previsto no art. 171, CP: "obter para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento", neste caso poderá incidir pena de reclusão que varia de uma a cinco anos, e multa.

Essa ampla conceituação legal do estelionato permite que ele se configure com qualquer obtenção de vantagem ilícita em prejuízo alheio, praticada com o emprego

de artifício, ardil ou qualquer outro meio fraudulento, o que facilita a sua aplicação às variadas hipóteses, que deverão ter sempre o elemento dolo no sentido de induzir ou manter alguém em erro.

Para caracterização desse tipo penal é necessário, ainda, que o agente tenha atingido pessoa determinada e que o resultado final visado pelo agente deve ser a obtenção de vantagem ilícita em prejuízo alheio.

É um crime material que somente se consuma no instante em que o agente efetivamente consegue obter a vantagem ilícita por ele visada. A não ocorrência do resultado caracteriza a tentativa, que se configura em casos, por exemplo, em que o agente, engana a vítima, mas não consegue obter a vantagem ilícita visada, ou emprega a fraude e não consegue enganar a vítima.

O sujeito ativo tanto pode ser aquele que emprega a fraude, quanto àquele que recebe a vantagem ilícita, desde que este, tenha de alguma maneira, estimulado a pratica do crime. O sujeito passivo pode ser tanto quem sofre o prejuízo quanto quem é enganado pela fraude (normalmente é a mesma pessoa).

Acertada é a posição de Cezar Roberto Bittencourt onde diz que "embora nossa CP ainda não tenha previsão específica sobre o tema, como ocorre com as modernas legislações (CP português, art. 221.1; CP espanhol, art. 248.2; CP francês, arts. 323-1 a 323-3), é perfeitamente possível a prática de estelionato por meio da informática, desde que seus requisitos legais estejam presentes. As penas uma legislação especial poderia ampliar suas modalidades, como fizeram as legislações referidas."[16]

Sendo assim, para incidir o crime de estelionato por meio da internet é necessário que o agente induza ou mantenha alguém em erro, ou seja, uma pessoa, um ser humano, de modo que a atuação da vítima, seja ela comissiva ou omissiva, é fundamental para a configuração do crime. Caso contrário, estará desconfigurada a conduta prevista no art. 171, caput, do CP.

b) Das Fraudes: Com a difusão acelerada da rede mundial de computadores, a Internet, e o acesso a ela cada vez mais facilitado, temos visto crescer na mesma

[16] BITENCOURT. Cezar Roberto. **Código Penal Comentado**, p. 750, Ed. Saraiva, 2002.

proporção as fraudes digitais. Os chamados "Hackers", especialistas em informática e rede de computadores, estão usando cada vez mais a Internet para invadir sites pessoais ou de empresas, praticando todo tipo de golpe, sendo que o que mais acontece é de caráter financeiro. Para isso são usados os mais variados meios, como criar sites on-line de compras, usando logomarcas de instituições como Banco do Brasil e Caixa Econômica. Assim, o fraudatório consegue colher dados pessoais da pessoa lesada, acessando sua conta e retirando o dinheiro que tiver.

Outro golpe praticado é a criação de sites de leilões ou de venda de produtos com preço muito "atrativo", onde geralmente o cliente recebe um produto que não condiz com o solicitado, ou, como acontece na maioria das vezes, acaba não recebendo nada e poderá ter seus dados pessoais e financeiros furtados, caso a transação tenha envolvido, por exemplo, o número do seu cartão de crédito. É comum também acontecer fraudes através do envio de e-mails, onde a pessoa é induzida a acessar uma página fraudulenta. Neste caso também geralmente é solicitado os dados pessoais. Existem também, tentativas de atacar o servidor de instituições financeiras e comerciais, mas estas cada vez mais dificultam as ações dos hackers, e por isso os ataques mais comuns e frequentes tem sido a usuários, isoladamente.[17]

c) **Crimes contra a honra**: nas condutas contra a honra, seja ela objetiva ou subjetiva (calúnia, difamação ou injúria, previstos nos arts.138, 139 e 140 do CP), dependendo do tipo penal, pode se dar por vários meios, haja vista que se trata de delitos de forma livre, inclusive por meio informático, o que permite a conclusão da necessidade das previsões contidas no Projeto de Lei 76/2000, no art. 1º,§3º, que descreve como conduta criminosa o uso indevido da informática contra a honra pela difusão material injurioso por meio de mecanismos virtuais. Vale ressaltar, que o referido projeto de lei não descreve o que é o uso indevido da informática, ferindo assim o princípio da taxatividade, uma vez que não se tem a limitação do que se deva reconhecer por uso devido. O simples termo uso indevido tornaria a descrição de difícil aplicação, haja vista ser demasiadamente amplo.

d) **Ameaça:** preceitua o art. 147 do Código Penal que "ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e

[17]**Crimes Virtuais**, disponível em http://br.geocities.com/lrbs1003, acesso em 18 de marco de 2008.

grave. Pena – detenção de 1(um) a 6(seis) meses, ou multa)". Neste sentido, entende-se perfeitamente possível a configuração de ameaça por meio do computador. Hoje, tem sido muito praticada por meio de envio mensagens através de sites de telefonia celular, onde basta o agente digitar e enviar a mensagem. Neste caso, não é necessário nem a identificação do usuário para tal prática, sendo um instrumento acessível a qualquer pessoa.

3.3.2 Os Crimes praticados por Computador e o Estatuto da Criança e do Adolescente

De acordo com o *art. 241* do Estatuto da criança e do adolescente é considerado crime a produção, venda, fornecimento, divulgação e publicação, por qualquer meio de comunicação, inclusive a rede mundial de computadores (internet), fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo crianças ou adolescentes.

Apesar do crescimento constante da pedofilia na internet, hoje em dia, no Brasil, ainda não há uma lei específica para esse tipo de prática. Para efeito de punição é utilizada a *Lei n° 8.069*, de 13 de julho de 1990, que dispõe sobre o Estatuto da Criança e do Adolescente, e que sofreu alteração em sua redação, trazida pela *Lei n°10.764*. Antes dessa alteração o art. 241 sofria críticas por não haver aplicação penal na rede mundial de computadores, mas essas críticas não foram acolhidas pelo Supremo Tribunal Federal – STF, que produziu ampla jurisprudência dando validade ao antigo art. 241do ECA (Estatuto da Criança e do Adolescente).

Sobre essa conduta segue um dos primeiros julgados do Supremo Tribunal Federal (HC nº 76689/PB):

> Crime de Computador: publicação de cena de sexo infantil (Estatuto da Criança e do Adolescente, art. 241) mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte.
> 1.O tipo cogitado – na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" – ao contrário do que sucede, por exemplo, aos da Lei de Imprensa, no tocante ao

> processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da aça punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador.
> 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta incriminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explicito que nela se compreendia a morte dada a outrem mediante arma de fogo.
> 3.Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum impõe-se a realização de prova pericial.

O Processo de investigação e prisão de pessoas envolvidas em exploração sexual de menores na internet é bastante lento, primeiramente porque depende do desenvolvimento das tecnologias, como por exemplo, para identificar o IP (*Internet Protocol*) de provedores caseiros.

O IP é o número de identificação da máquina e permite descobrir qual é o país de origem da publicação do site. Outra dificuldade, depois de ter descoberto o provedor e o país de origem do site, é a investigação para se chegar ao criminoso, porque isso depende de quebras de sigilos, atuação do Ministério Público e outras burocracias.

A melhor forma de combater a pornografia infantil no internet, talvez seja o reconhecimento dos códigos de ética da sociedade. O uso de forma responsável dos computadores deve ser ensinado desde cedo nas escolas. A internet pode ser um espaço democrático sem ser criminoso, usando de práticas inaceitáveis contra a criança e o adolescente.

Devido a sua universalidade, interação e crescimento, a internet não pode correr o risco de ser acusada, em um futuro próximo, de incentivadora de uma cultura que aceita a satisfação sexual de adultos por crianças e adolescente.

Com o intuito de aumentar o rigor contra os crimes praticados por meio do computador, foi editada a Lei 12.737/2012 dispondo sobre a tipificação criminal de delitos informáticos.

3.3.3 Lei 12.737/12 – Que dispõe sobre a tipificação de delitos informáticos –Lei "Carolina Dieckmann"

O dia 03 de dezembro de 2012 foi marcado por um grande avanço legislativo no que concerne à criminalidade informática. As Leis 12.735/12 e 12.737/12 foram sancionadas pela presidente Dilma Rouseff, com o fito de diminuir as lacunas concernentes ao âmbito dos delitos praticados pela internet.

O caso da atriz Carolina Dieckmann, foi que deu velocidade à tramitação do processo legislativo que deu ensejo à mudança. Embora não tenha sido o primeiro caso de extorsão e divulgação de conteúdo sigiloso na internet, foi o que deu maior repercussão midiática, que, sem dúvidas, é o fundamento da maior parte das últimas criações legislativas do âmbito penal.

Vejamos o inteiro teor da lei[18]:

> Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.
>
> **A PRESIDENTA DA REPÚBLICA** Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:
> Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
> Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
> **Invasão de dispositivo informático**
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações

[18] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
I - Presidente da República, governadores e prefeitos;
II - Presidente do Supremo Tribunal Federal;
III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
Ação penal
Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."
Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:
"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública
Art. 266. .....
§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública." (NR)
"Falsificação de documento particular
Art. 298. .....
Falsificação de cartão
Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito." (NR)
Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.
Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.
DILMA ROUSSEFF
José Eduardo Cardozo
Este texto não substitui o publicado no DOU de 3.12.2012

Indispensável ressaltar que a alteração da sociedade na era da informação, nos moldes do que fora exposto até o momento é reconhecida por diversos doutrinadores, de

acordo com o que corrobora Liliana Minardi Paesani, ao coordenar a obra "O Direito na Sociedade da Informação", que ao abordar o tema leciona[19]:

> [...] vivemos em uma época em que a produção normativa é insuficiente tanto para fazer frente às mudanças sociais, causadas pelo rápido avanço tecnológico, como para obter sua legitimação diante de grupos sociais cada vez mais fracionados, que não compartilham seus valores com os demais e encontram um dos poucos pontos de contato justamente no próprio avanço tecnológico, notadamente na internet [...].

Sendo assim, conclui-se que a entrada em vigor da Lei nº 12.737/12 além de demonstrar uma evolução de nossa legislação pátria por tratar de assunto contemporâneo a nossa sociedade se demonstra apta a complementar os institutos jurídicos existentes, tornando ainda mais eficaz nosso ordenamento jurídico do ponto de vista de apresentar resguardo no âmbito civil e agora criminal no tocante a infrações cometidas em ambiente virtual.

3.3.4 Crimes presentes em ordenamentos jurídicos com expressa menção a elementos de informática[20]:

Diversos crimes praticados com utilização de dispositivos eletrônicos estão previstos em legislações esparsas no nosso ordenamento jurídico passível de reprimenda estatal, vejamos:

a) art. 35 e 37 da Lei 7.646 de 18 de dezembro de 1987: violação de direitos autorais de programa de computador. Os referidos dispositivos foram revogados com a edição da Lei 9.609, de 19 de fevereiro de 1998, que veiculou tipos praticamente idênticos no art. 12: "Violar direitos de autor de programa de computador: Detenção de seis meses a dois anos ou multa.

---

[19] PAESANI, Liliana Minardi. O Direito na Sociedade da Informação. Ed. Atlas. São Paulo. pág. 76.
[20] CASTRO, Aldemario Araújo. **Livro Eletrônico**, capítulo 18, disponível: www.aldemario.adv.br, acesso em: 13 de maio de 13.

§1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena - Reclusão de um a quatro anos e multa.

§2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral".

b) art. 2o, inciso V da Lei n. 8.137, de 27 de dezembro de 1990: possuir informação contábil diversa daquela fornecida à Fazenda Pública:

Lei n. 8.137, de 27 de dezembro de 1990 (art. 2o): "V - utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública. Pena - detenção, de 6 (seis) meses a 2 (dois) anos, e multa.

c) art. 67, incisos VII e VIII da Lei n. 9.100, de 29 de setembro de 1995: crimes eleitorais:

Lei n. 9.100, de 29 de setembro de 1995 (art. 67): "VII - obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizados pelo serviço eleitoral, a fim de alterar apuração ou contagem de votos: (...)

VIII - tentar desenvolver ou introduzir comando, instrução ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados utilizados pelo sistema eleitoral.

d) art. 10 da Lei n. 9.296, de 24 de julho de 1996: interceptação de comunicações de informática ou telemática:

Lei n. 9.296, de 24 de julho de 1996: "Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei."

e) art. 313-A do Código Penal (inserido pela Lei n. 9.983, de 14 de julho de 2000): inserção de dados falsos em sistemas de informações:

Lei n. 9.983, de 14 de julho de 2000: "Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados a Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano".

f) art. 313-B do Código Penal (inserido pela Lei n. 9.983, de 14 de julho de 2000): modificação ou alteração não autorizada de sistema de informações:

"Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente."

g) art. 241 do Estatuto da Criança e do Adolescente (com redação dada pela Lei n. 10.764, de 12 de novembro de 2003): divulgação, por qualquer meio de comunicação, inclusive pela internet, de imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:

Art. 4º O art. 241 da Lei nº 8.069, de 1990, passa a vigorar com a seguinte redação:

> Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:
> Pena - reclusão de 2 (dois) a 6 (seis) anos, e multa.
> § 1º Incorre na mesma pena quem:
> I - agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo;
> II - assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do **caput** deste artigo;
> III - assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do **caput** deste artigo.

Conclui-se, então, que é possível reconhecer o sistema informático como um instrumento eficaz na prática de várias modalidades criminosas sem que com isso se verifique a necessidade de adequação legislativa do meio utilizado pelo agente para que se possa verificar a tipicidade da conduta. Desta feita, os delitos praticados de forma livre, assim incluindo o sistema informático, faz-se pela simples indagação da eficácia ou não do meio para a obtenção do resultado lesivo ao bem jurídico protegido pelo tipo.

Os criminosos atuam das mais diversas formas. Eles utilizam sites para proliferarem ideais racistas, invadem contas bancárias, praticam pedofilia e interceptam comunicações eletrônicas, piratarias que ferem o direito autoral, por exemplo, sem que para isso precisem utilizar qualquer ferramenta palpável, como armas, mas apenas sofisticados programas tecnológicos que possibilitam que o agente esteja até mesmo em outro território, a quilômetros de distância da vítima alvo da sua empreitada criminosa.

4 DA COMPETÊNCIA

As dificuldades acerca de jurisdição e competência estão cada vez mais presentes no cotidiano dos operadores do Direito que se defrontam com questões relativas à internet. Destarte, fundando-se na pretensão punitiva e nas regras que irão distribuir a competência no âmbito do processo penal, notadamente em relação às redes sociais na internet passa-se para a análise da competência no Processo Penal.

4.1 Conceito de Jurisdição e Competência no Processo Penal

Tendo em vista que o objetivo do presente trabalho é abordar também aspectos acerca da competência atualmente determinada para julgamento dos crimes praticados por meio do computador, necessário se faz conhecer o que é a competência, os critérios determinantes desta, e o que preceitua o Código de Processo Penal no tocante ao julgamento das condutas tipificadas em nosso Código Penal e demais legislações. Ao tratarmos do estudo da competência no Processo Penal é necessário que seja feita uma abordagem acerca do conceito de jurisdição, seus princípios e limites e, logo depois os critérios determinantes da competência fixados pelo Código de Processo Penal.

4.1.1 Jurisdição

É o poder atribuído, constitucionalmente, ao Estado para aplicar a lei ao caso concreto, compondo litígios e resolvendo conflitos. Em regra, a atividade jurisdicional é exclusiva dos integrantes do Poder Judiciário, permitindo a própria Constituição no art. 52, I e II, como exceção, que o Senado Federal processe e julgue determinadas autoridades, Desta feita, todo juiz, investido na sua função, possui jurisdição.

No tocante a jurisdição alguns princípios devem ser observados, dentre eles:

a) Princípio da indeclinabilidade: o juiz não pode abster-se de julgar os casos em que lhe forem apresentados;
b) Princípio do Juiz natural: ninguém pode ser processado ou julgado senão pelo juiz competente, de acordo com normas preestabelecidas;
c) Princípio da inércia (ou iniciativa das partes): o juiz não pode dar início à ação penal;
d) Princípio da indelegabilidade: O poder jurisdicional não pode ser delegado a quem não o possui;
e) Princípio da improrrogabilidade: as partes, mesmo que entrem em acordo, não pode retirar do juiz natural conhecimento de determinada causa, na esfera criminal;
f) Princípio da inevitabilidade (ou irrecusabilidade): as partes não podem recusar o juiz, salvo nos casos de suspeição, impedimento ou incompetência;
g) Princípio da unidade: a jurisdição é única, pertencente ao Poder Judiciário, diferenciando-se apenas no tocante à sua aplicação e grau de especialização, podendo ser civil, penal, trabalhista, militar ou eleitoral.

4.1.2 Competência

A lei estabelece limites ao exercício da jurisdição pelos magistrados, estes limites são fixados através da competência atribuída legalmente a cada julgador. Trata-se da delimitação da jurisdição, ou seja, o espaço dentro do qual a autoridade judiciária poderá exercer as suas atribuições, aplicando o direito aos litígios que lhe forem apresentados, compondo-os. Destarte, mesmo que o magistrado seja dotado do poder jurisdicional, ele deverá respeitar os limites de sua competência, fixados por lei.

4.1.3 Competência absoluta e Competência relativa

A competência de determinado juiz pode ser estabelecida de forma absoluta ou relativa. Temos que, competência absoluta é aquela não admite prorrogação, isto é, as normas estabelecidas através da Constituição ou do Processo Penal no tocante ao remetimento de determinado processo ao juiz natural competente, devem ser obedecidas, sob pena de nulidade do feito.

As competências *ratione materiae(*ex.: federal ou estadual; cível ou criminal) *e ratione personae*, bem como a funcional, são casos de competência absoluta. Em contrapartida, a competência relativa é aquela que admite a prorrogação, ou seja, se não foi arguida a incompetência do foro, via exceção, no momento oportuno, reputa-se competente o juízo que conduz o feito, não podendo ser feita posteriormente tal arguição de nulidade. A competência *ratione loci*, ou seja, em razão da lugar ou ainda, competência territorial, encaixa-se nesse perfil.

É importante remeter este assunto ao que diz Maria Lucia Karam[21], no tocante às regras sobre competência territorial, *in verbis*:

> No caso do processo penal, em que as regras de competência territorial estabelecem como foro comum o lugar da consumação do delito, o que se leva em conta não é o interesse de qualquer das partes, mas sim, o interesse público, manifestado quer em função da repercussão do fato na localidade onde se deu seu cometimento, quer em função do bom funcionamento da máquina judiciária, já que ali haverá, em tese, maior facilidade de obtenção de provas, a favorecer a maior exatidão possível na reconstituição dos fatos, maior exatidão esta especialmente necessária no processo penal. Tem-se aqui, portanto, não obstante se tratar de competência territorial, hipótese de improrrogabilidade da competência, manifestando-se na inadequada atuação do órgão jurisdicional no processo, em decorrência da inobservância das regras que estabelecem aquele foro comum, hipótese de incompetência absoluta.

Segundo a mesma autora, temos que:

---

[21] KARAM, Maria Lucia. **Competência no Processo Penal**, p. 79 e 80, 4ª Ed., Revista dos Tribunais, 2005.

> o que irá indicar se a incompetência é absoluta ou relativa é o caráter imperativo ou não da regra que atribui a competência, vinculado à prevalência ou não do interesse público, a desautorizar, no caso desta prevalência, sua modificação por vontade das partes, pouco importando se os elementos determinantes desta atribuição de competência se relacionam com a matéria, lugar ou qualquer outro fator.[22]

Destaca Arnaldo Siqueira Lima[23] que:

> o que se observa é que muitos desses que reconhecem a incompetência territorial, no processo penal, como relativa, julgam a arguição em preliminar, não sendo aí coerentes como ponto de vista esposado, pois a via adequada é a exceção. Preliminar, como sabemos, é matéria reservada à incompetência absoluta.

A doutrina majoritária posiciona-se no sentido de que o juízo penal tanto a competência absoluta quanto a relativa podem ser reconhecidas de ofício pelo órgão julgador.

4.1.4 Critérios de fixação de competência

Ao longo do tempo, a doutrina buscou sistematizar os critérios adotados na lei para a distribuição de competências entre os órgãos jurisdicionais. As teorias mais aceitas dão conta de que a fixação da competência constitui um procedimento lógico de concretização, ou seja, requer um raciocínio que parte desses critérios mais genéricos para critérios mais específicos. Nesse sentido, a doutrina identifica como critérios mais abstratos de fixação de competência dois elementos: as características da lide (da relação jurídica material que constitui o objeto do processo) e os atos processuais. O primeiro elemento diz respeito à chamada competência material, enquanto o segundo se relaciona à competência funcional.[24]

---

[22] Op. cit. p. 80.
[23] Lima, Arnaldo Siqueira. **A competência relativa no Processo Penal**, disponível em: http://www.neofito.com.br/artigos/art01/ppenal38.htm, acesso em 18 de maio de 2013.
[24] MOUGENOT, Edílson. **Curso de Processo Penal,** p. 196, Editora Saraiva, 2006.

4.1.4.1 Competência Material

Segundo Mougenot, a competência material divide-se em três aspectos: i) o direito material que rege a relação jurídica levada à apreciação do poder judiciário; ii) a qualificação das pessoas envolvidas no litígio e iii) o território.[25]

4.1.4.1.1 Competência "ratione materiae": é a competência determinada em razão do tipo de matéria em que se irá julgar.

4.1.4.1.2 Competência "ratione personae": é a competência determinada para o julgamento de certas pessoas de acordo com uma qualidade que estas circunstancialmente possuem, pode-se concluir que refere-se às que desempenham determinadas funções ou ocupam determinados cargos. Nestes casos, tais pessoas são julgadas por órgãos diferentes dos que ordinariamente julgariam outros infratores que não possuem tais características.

4.1.4.1.3 Competência "ratione loci": é a competência determinada de acordo com o lugar em que foi cometida a infração ou pelo domicílio/residência do réu.

4.1.4.2 Competência Funcional

Tendo em vista que o processo é formado por um conjunto de atos encadeados, temos que, em princípio, um mesmo juízo que pratica originalmente certos atos num determinado processo é competente para prática de todos os atos no âmbito de um mesmo processo. Entretanto, é comum que os atos processuais, ainda que no âmbito de um mesmo processo, sejam praticados por diversos juízes. Mongenot cita que a doutrina identifica três situações em que isso ocorre[26]:

a) Distribuição conforme a fase do processo: determinados processos, de acordo com a fase em que se encontram, pode ser que a competência para a condução do processo seja mudada. É o que

[25] Op. cit. P. 197
[26] Op. cit. p. 198

ocorre, por exemplo, no Tribunal do Júri, onde a instrução do processo é conduzida por um órgão e o julgamento por outro.

b) Distribuição quanto ao objeto do juízo: Fala-se em objeto do juízo quando os órgãos julgadores apenas podem atuar no processo em relação a uma parcela específica de seu objeto. Outra vez, é o exemplo do Tribunal do Júri, em que a competência dos jurados se restringe a responder aos quesitos relativos às questões controversas, enquanto ao juiz caberá decidir as questões de direito, lavrando a sentença e fixando a pena aplicável.
c) Distribuição vertical: Podem atuar no processo órgãos julgadores alocados em diferentes instâncias. Interposto determinado recurso de apelação, por exemplo, deixará de ser competente para conduzir o processo o juízo do primeiro grau, passando a ser competente o tribunal ao qual se dirige o recurso.

4.1.4.3 Competência Jurisdicional

De acordo com o art. 69 do Código de Processo Penal são estabelecidos os critérios determinativos da competência jurisdicional, sendo:

I. o lugar da infração;
II. o domicílio ou residência do réu;
III. a natureza da infração;
IV. a distribuição;
V. a conexão ou continência
VI. a prevenção;
VII. a prerrogativa de função.

4.1.4.3.1 Competência pelo lugar da infração

De acordo com o art. 70 do CPP, como regra geral, temos que a competência para julgar a ação penal será do foro do local em que for consumada a infração. Entende-se como local da infração, o local em que houver ocorrido o *resultado* da prática criminosa. Já o Código Penal no art. 6º estabelece que o local do crime é tanto o local "em que ocorreu a ação ou omissão, no todo ou em parte", quanto o local "onde se produziu o resultado ou deveria produzir-se o resultado". Temos então, que o código de processo penal adotou a teoria do resultado, enquanto o código penal adotou a teoria da ubiquidade.

4.1.4.3.2 Competência pelo domicílio ou residência do réu

De acordo com o art. 70 do Código Civil, domicilio é o local em que a pessoa mora com ânimo definitivo, e residência o local em que a pessoa mora com ânimo transitório.

Nos termos do art. 72, caput, do Código de Processo Penal, não sendo conhecido o lugar da infração, a competência será determinada pelo domicilio ou residência do réu. Trata-se como foro subsidiário ou supletivo para as hipóteses em que houver impossibilidade de determinar o lugar de consumação do crime.

Se o réu tiver mais de uma residência, a competência será firmada entre uma delas por prevenção (art. 72,§1º do CPP). Entretanto, vale observar que, se o réu não tiver residência ou for ignorado o local em que o mesmo mora a competência será do juiz que primeiro tomar conhecimento (formal) do fato (art. 72,§2º do CPP). No caso de pluralidade de réus, domicílios ou residências diferentes, a competência será aplicada pela regra da prevenção.

O art. 73 do Código de Processo Penal prevê uma exceção quanto a esta regra, permitindo que nos casos de ação privada, mesmo sendo conhecido o lugar da infração, a vítima pode optar por dar início ao processo no foro do domicilio ou residência do réu.

4.1.4.3.3 Competência pela natureza da infração

Uma vez firmada a justiça competente, e determinada a competência pelo lugar da infração ou, pelo domicílio ou residência do réu, é preciso fixá-la em razão da matéria. Conforme a natureza do delito, a ação será julgada por uma determinada justiça competente, podendo o julgamento ficar a cargo da Justiça Especial ou da Justiça Comum, dependendo da natureza da infração cometida. Sendo a Justiça Especial dividida em: Eleitoral, para os crimes eleitorais (art. 121, CF) e Militar, para os crimes militares (art.

124, CF). Já a Justiça Comum divide-se em Federal e Estadual (a Justiça Estadual também é conhecida como residual; para ela resta o que não for da competência das Justiças Eleitoral, Militar e Federal).

A competência da Justiça Federal está prevista no artigo 109 da CF, competindo-lhe, na esfera penal, processar e julgar:

a) os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções penais (inc. IV);

b) os crimes previstos em tratado ou convenção internacional, desde que a distância (inc. V);

c) os crimes contra a Organização do trabalho e, nos casos determinados por lei, contra o sistema financeiro e a ordem econômica e financeira (inc. VI);

d) os crimes cometidos a bordo de navios ou aeronaves (inc. IX);

e) ingresso de permanência de estrangeiro permanente no Brasil (art. 125, Lei 6815/80).

A competência da Justiça Comum estadual é fixada, de um modo geral, por exclusão, ou seja, tudo quanto não cabe na competência das justiças especiais e da Justiça Federal é da competência dela (art. 125, § 1°, CF).

4.1.4.3.4 Competência por distribuição

Quando houver na mesma circunscrição judiciária vários juízes igualmente competentes para a apreciação e julgamento de determinado caso, a fixação da competência proceder-se-á segundo o critério da distribuição (sorteio). Podendo dizer ainda que, a distribuição é um ato de repartição dos feitos entre os juízes que possuem idêntica competência. A existência desse critério tem por finalidade evitar o ajuizamento direcionado de determinadas causas, de acordo com o posicionamento de cada julgador acerca de determinado assunto.

4.1.4.3.5 Competência por conexão ou continência

Apesar de a conexão e a continência estarem previstas como critério de determinação da competência, a doutrina as considera como critérios de *modificação/prorrogação* da competência. Com efeito, quando existe algum vínculo (conexão ou continência) entre duas ou mais infrações, independentes entre si, a lei estabelece que deverá existir um só processo.

A conexão é configurada quando há um vínculo que liga duas ou mais infrações, já a continência configura-se quando uma demanda, em face de seus elementos (partes, causa de pedir e pedido) esteja contida em outra.

4.1.4.3.6 Competência por prevenção

A prevenção é um critério residual de determinação de competência, incidindo quando há pluralidade de juízes igualmente competentes para a apreciação e julgamento de uma determinada ação. Neste caso, torna-se prevento aquele que tiver antecedido aos demais na pratica de algum ato do processo ou de medida a este relativa, ainda que anterior ao oferecimento da denúncia ou queixa (decisão acerca da concessão de fiança ou prisão preventiva no curso de inquérito policial, por exemplo).[27]

4.1.4.3.7 Competência pela prerrogativa de função

É o critério utilizado para determinar a competência nos casos em que determinadas pessoas em face de ocuparem certas funções ou cargos, no exercício destas,

[27]Mougenot, op. cit. p. 228.

passarão a ser julgadas originalmente perante órgãos diferentes (órgãos superiores) daquelas que não exercem tais funções.

Em suma, cada um desses critérios de fixação de competência, estabelecidos pelo art. 70 do CPP, tem finalidade diversa. Neste entendimento, a competência pelo lugar da infração e pelo domicilio ou residência do réu têm por finalidade fixar a comarca competente. Uma vez fixada a comarca, o critério da natureza da infração serve para que se encontre a Justiça competente (Federal, Militar, Eleitoral etc). Por fim, fixada a comarca e a Justiça, é possível que vários juízes sejam igualmente competentes para o julgamento da ação.

Se algum deles praticou algum ato válido primeiramente, estará ele prevento. Se, todavia, não há nenhum juiz prevento, deverá ser utilizado o critério da distribuição (sorteio). A conexão e a continência, em verdade, são formas de prorrogação da competência. E a competência por prerrogativa de função é verificada quando o legislador, levando em consideração a relevância do cargo ou função ocupados pelo autor da infração, estabelece órgãos específicos e preestabelecidos do Poder Judiciário para o julgamento do caso em questão.

Temos a competência *ratione loci* no critério pelo lugar da infração e pelo domicilio/residência do réu; a competência *ratione materiae* no critério natureza da infração; e a competência *ratione personae* no critério por prerrogativa de função.

Discute-se ainda a fixação da competência no tocante aos crimes praticados por meio do computador.

4.2 Da competência nos crimes praticados por meio do computador

A questão da fixação da competência no tocante aos crimes praticados por meio de computador tem sido muito discutida, haja vista que nem sempre há previsão legal no tocante tais práticas.

É dito por Celso Valin[28] que

> o grande problema ao se trabalhar com o conceito de jurisdição e territorialidade na Internet, reside no caráter internacional da rede. Na Internet não existem fronteiras e, portanto, algo que nela esteja publicado estará em todo o mundo. Como, então, determinar o juízo competente para analisar um caso referente a um crime ocorrido na rede? Em tese, conforme VALIN, um crime cometido na Internet ou por meio dela consuma-se em todos os locais onde a rede seja acessível. Ver, por exemplo, o crime de calúnia. Se o agente atribui a outrem um fato tido como criminoso e lança essa declaração na Internet, a ofensa à honra poderá ser lida e conhecida em qualquer parte do mundo. Qual será então o foro da culpa? O local de onde partiu a ofensa? O local onde está o provedor por meio do qual se levou a calúnia à Internet? O local de residência da vítima ou do réu? Ou o local onde a vítima tomar ciência da calúnia?

Ivette Senise Ferreira entende que já se deu a internacionalização da criminalidade informática, devido à mobilidade dos dados nas redes de computadores, facilitando os crimes cometidos à distância. Diante desse quadro, é indispensável que os países do globo harmonizem suas normas penais, para prevenção e repressão eficientes[29].

Maria Lucia Kram[30] define a competência territorial da seguinte forma: A competência de foro, disciplinada pela legislação processual penal, tem como regra básica, que constitui o chamado foro comum, a de que a competência se estabelece pelo lugar em que se teria consumado a infração penal alegada ou, no caso de tentativa, pelo lugar em que teria sido praticado o último ato de execução, conforme o disposto no caput do artigo 70 do Código de Processo Penal, regulando as regras contidas nos §§ 1o e 2o daquele artigo os casos em que a consumação ou o último ato de execução da alegada infração penal tenham ocorrido fora do território nacional.

A competência comum estadual é residual, ou seja, a mesma só será aplicada quando se tratar de casos que não competem à Justiça Federal, que por sua vez é taxativa e está prevista no artigo 109 da Constituição Federal.

---

[28]ARAS, Vladimir apud Valin, Celso. Crimes de Informática: Uma nova criminalidade. Disponível em: www.jus2.com.br , acesso em 13 de maio de 2008.
[29] ARAS, Vladimir apud Valin, Celso. Crimes de Informática: Uma nova criminalidade. Disponível em: www.jus2.com.br , acesso em 13 de maio de 2008.
[30]KARAM, Maria Lúcia. Competência no Processo Penal. 3. ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 2002. p.39

Ocorre que tal dispositivo não menciona os crimes de informática, e por esta razão é de grande importância a análise das teorias do lugar do crime, para assim fixar a competência.

Pela teoria da atividade, lugar do crime seria o da ação ou da omissão, ainda que outro fosse o da ocorrência do resultado. Já a teoria do resultado despreza o lugar da conduta e defende a tese de que lugar do crime será, tão somente, aquele em que ocorrer o resultado. Já teoria da ubiquidade ou mista adota as duas posições anteriores e argumenta que lugar do crime será o da ação ou omissão, bem como onde se produziu ou deveria produzir-se o resultado. Dessa forma, se o delito simplesmente 'tocar' o território nacional, em qualquer fase do *'iter criminis'*, na ação ou omissão, ou no resultado, será tal fato alcançado pela legislação penal brasileira.

Porém, de acordo com a teoria da ubiquidade, o entendimento legal é que a lei penal brasileira é aplicável não só na origem do crime ou resultado. É possível a aplicação sempre que alguma parte do delito tenha se dado em território nacional, já que parte do resultado não deixa de ser resultado, conforme estabelece o 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".

E um dos principais enfoques a ser dado no tocante às condutas praticadas por meio do computador é o referente a fixação do foro competente para a apreciação e julgamento de ações oriundas de práticas ilícitas cometidas por meio da internet. Tendo em vista que os crimes praticados por meio do computador podem ser cometidos em diversos lugares e que pode haver a prática de mais de uma conduta lesiva, deve-se analisar as seguintes situações:

a) Se houve a prática de um único crime praticado pela mesma pessoa:

Segue a regra prevista pelo art. 70 do Código de Processo Penal, onde prevê que:

> Art. 70 - A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.

b) Se houve a prática de vários crimes praticados por uma mesma pessoa ou grupo, ou ainda no caso de um só crime praticados por várias pessoas.

Conforme dito anteriormente, fala-se em conexão quando existe algum elemento entre as infrações ou entre os autores que torne mais racional a apreciação do processo por um só juízo. A conexão desloca a competência para o que se denomina foro prevalente, ou seja, aquele que atrairá todos os feitos relacionados pela conexão a fim de que todos sejam apreciados pelo mesmo juízo.

O CPP trata longamente da conexão, da denominada continência (que veremos a seguir) e das regras aplicáveis para a determinação do foro prevalente.

Existe **conexão** nas seguintes hipóteses, todas descritas no art. 76 do CPP:

a) Quando ocorrem duas ou mais infrações;

a.1) praticadas ao mesmo tempo por várias pessoas reunidas;

a.2) praticadas em tempo e lugares diversos, por várias pessoas em concurso (p. ex., crimes praticados por uma quadrilha em locais e tempos diversos);

a.3) praticadas por várias pessoas, uma contra as outras (conexão por reciprocidade).

b) Quando uma infração for praticada para facilitar ou ocultar a prática de outra. É a denominada conexão material e o exemplo comum é a ocultação ou destruição de cadáver ou o espancamento da única testemunha de um crime para intimidá-la a não depor.

c) Quando a prova de uma infração ou de qualquer de suas circunstâncias elementares influir na prova de outra infração. É a denominada conexão instrumental. É evidente que, nestes casos deve haver unidade de processos, até mesmo para se evitarem decisões divergentes ou que se suspenda um processo para aguardar a decisão de outro em que está sendo apreciada a prova decisiva à caracterização do delito acessório.

A continência é, também, uma forma de deslocamento da competência no processo penal. O fundamento dessa alteração da competência é o mesmo que foi expendido ao tratarmos da conexão, ou seja, é conveniente a unidade de processos a fim de possibilitar-se uma adequada apreciação das provas e uniformidade de decisões.

Ocorre a **continência** nas seguintes hipóteses, previstas no art. 77 do CPP:

a) Quando duas ou mais pessoas forem acusadas pela mesma infração;

b) Na hipótese de *aberratio ictus* (o agente, por erro, além de atingir a pessoa que pretendia atingir lesa outra que não desejava ferir);

c) No caso de *aberratio criminis* (o agente, fora do caso acima descrito, além do resultado pretendido, causa outro que não desejava causar).

No Caso de haver a necessidade de estabelecer o foro prevalecente nos casos de conexão e continência será observada as regras do art. 78 do CPP:

Vimos que tanto a conexão como a continência deslocam a competência unificando os processos em um determinado foro, denominado foro prevalente (*forumattractionis*). Para estabelecermos o foro que prevalecerá, devemos seguir as regras plasmadas nos arts. 78 a 82 do CPP, abaixo transcritos:

> Art. 78. Na determinação da competência por conexão ou continência, serão observadas as seguintes regras: (Redação dada pela Lei nº 263, de 23.2.1948)
> I - no concurso entre a competência do júri e a de outro órgão da jurisdição comum, prevalecerá a competência do júri; (Redação dada pela Lei nº 263, de 23.2.1948)
> Il - no concurso de jurisdições da mesma categoria: (Redação dada pela Lei nº 263, de 23.2.1948)

a) preponderará a do lugar da infração, à qual for cominada a pena mais grave;

b) prevalecerá a do lugar em que houver ocorrido o maior número de infrações, se as respectivas penas forem de igual gravidade;

c) firmar-se-á a competência pela prevenção, nos outros casos;

> III - no concurso de jurisdições de diversas categorias, predominará a de maior graduação; (Redação dada pela Lei nº 263, de 23.2.1948)
> IV - no concurso entre a jurisdição comum e a especial, prevalecerá esta. (Redação dada pela Lei nº 263, de 23.2.1948).

Acerca da competência, e também sobre a matéria afeta as redes sociais na internet, a jurisprudência pátria tem se manifestado conforme se verifica nos seguintes julgados:

Supremo Tribunal Federal:

> Ementa: HABEAS CORPUS. PENAL. PROCESSUAL PENAL. CRIMES DE PEDOFILIA E PORNOGRAFIA INFANTIL, PRATICADOS VIA INTERNET, E DE ESTUPRO DE VULNERÁVEL. CONEXÃO INSTRUMENTAL. COMPETÊNCIA DA JUSTIÇA FEDERAL. I – Crimes de pedofilia e pornografia infantil praticados no mesmo contexto daquele de estupro e atentado violento ao pudor, contra as mesmas vítimas. Reunião dos processos, em virtude da existência de vínculo objetivo entre os diversos fatos delituosos e de estarem imbricadas as provas coligidas para os autos, nos quais foram apuradas as práticas das condutas incriminadas. II – Há conexidade instrumental: a prova relacionada à apuração de um crime influirá na do outro, razão pela qual é competente para conhecer da controvérsia a Justiça Federal. III – Ordem de habeas corpus indeferida, ficando mantida, em consequência, a decisão proferida pelo Superior Tribunal de Justiça no Conflito de Competência 111.309/SP[31].

Superior Tribunal de Justiça:

> CONFLITO NEGATIVO DE COMPETÊNCIA. DIVULGAÇÃO DE IMAGENSPORNOGRÁFICAS DE MENORES POR MEIO DA INTERNET. CONDUTA QUE SE AJUSTAÀS HIPÓTESES PREVISTAS NO ROL TAXATIVO DO ART. 109 DA CF.COMPETÊNCIA DA JUSTIÇA FEDERAL.
> 1. A competência da Justiça Federal para processar e julgar os delitos praticados por meio da rede mundial de computadores é fixada quando o cometimento do delito por meio eletrônico se refere a infrações previstas em tratados ou convenções internacionais, constatada a internacionalidade do fato praticado (art. 109, V, da CF), ou quando a prática de crime via internet venha a atingir bem, interesse ou serviço da União ou de suas entidades autárquicas ou empresas públicas (art. 109, IV, da CF).
> 2. No presente caso, há hipótese de atração da competência da Justiça Federal, uma vez que o fato de haver um usuário do Orkut, supostamente praticado delitos de divulgação de imagens pornográficas de crianças e adolescentes, configura uma das situações previstas no art. 109 da Constituição Federal.
> 3. Além do mais, o Brasil comprometeu-se perante a comunidade internacional a combater os delitos relacionados à exploração de crianças e adolescentes em espetáculos ou materiais pornográficos, ao incorporar no direito pátrio, por meio do decreto legislativo nº28 de 14/09/1990, e do Decreto nº 99.710 de 21/12/1990, a Convenção sobre direitos da Criança adotada pela Assembleia Geral das Nações Unidas.
> 4. Ressalte-se, ainda, que a divulgação de imagens pornográficas, envolvendo crianças e adolescentes por meio do Orkut, não se restringe a uma comunicação eletrônica entre pessoas residentes no Brasil, uma vez que qualquer pessoa, em qualquer lugar do mundo, desde que

[31] BRASIL. Supremo Tribunal Federal. Habeas Corpus. HC 114.689 SP, Rel. Min. Ricardo Lewandowski. Julgado em 13/08/2013. Disponível em WWW.stf.jus.br acesso em 20/08/2013.

> conectada à internet e integrante do dito sítio de relacionamento, poderá acessar a página publicada com tais conteúdos pedófilos-pornográficos, verificando-se, portanto, cumprido o requisito da transnacionalidade exigido para atrair a competência da Justiça Federal.
> 5. Conflito conhecido para declarar competente o Juízo Federal da16ª Vara de Juazeiro do Norte - SJ/CE, ora suscitado[32].

Tribunal Regional Federal da 2ª Região:

> CRIMINAL. HABEAS CORPUS. PRISÃO PREVENTIVA. PRESSUPOSTOS. FUNDAMENTOS. 1. A prisão preventiva, regulamentada no art. 312 do Código de Processo Penal, configura-se como medida de natureza cautelar, e, portanto, sujeita à existência do f*umus boni iuris e* do *periculum in mora.* 2. A materialidade delitiva e os indícios suficientes de autoria – *fumus comissi delicti* – encontram-se delineados, na presente hipótese, através das provas acostadas aos autos da ação penal, que indicam que o paciente, divulgava fotos de meninas menores em poses eróticas em comunidade do orkut, supostamente criada por ele, bem como por meio de distribuição de CDs/DVDs.
> 3. Resta configurada a necessidade da prisão preventiva – periculum libertatis – como medida garantidora da ordem pública, de forma a impedir a continuidade da prática delitiva, eis que os crimes imputados são de fácil reiteração e o paciente não destruiu as fotos pornográficas das menores, que detinha há quatro anos, conforme seu interrogatório, havendo, portanto, indícios de intenção de uso.
> 4. Os bons antecedentes, a conduta social e a residência fixa do paciente não bastam, por si só, para a revogação da manutenção
> da prisão determinada pelo Juízo impetrado, eis que plenamente legal e necessária.
> 5. O decreto segregacional cautelar encontra-se devidamente fundamentado, uma vez que analisou, à luz dos dados fáticos e jurídicos presentes nos autos, os pressupostos necessários para a segregação preventiva.
> 6. Ordem denegada[33].

As regras acima descritas demonstram uma adequação frente aos crimes praticados por meio do computador haja vista que, conforme dito anteriormente, uma

---

[32] BRASIL. Superior Tribunal de Justiça. Conflito de Competência. CC 120.999-CE, Rel. Min. Alderita Ramos de Oliveira. Julgado em 24/10/2012. Julgado em 13/082013. Disponível em www.stf.jus.br acesso em 20/08/2013.

[33] BRASIL. Tribunal Regional Federal 2ª Região. Habeas Corpus. 2006.02.01.000016-0. Primeira Turma Especializada. Relator: Des. Liliane Roriz. DJ 22/03/2006, p. 273. Disponível em: <http://www2.trf2.gov.br/NXT/gateway.dll?f=templates&fn=default.htm&vid=base_jur:v_juris>. Acesso em: 20 ago. 2013

mesma pessoa pode realizar várias condutas delitivas, e essas condutas podem atingir seu objeto final face à vários locais.

Desta forma, os critérios da continência, conexão e prevenção, além dos outros critérios materiais e jurisdicionais já citados, mostram que mesmo com poucas legislações específica no tocante aos crimes praticados por meio do computador, é possível que seja feito o enquadramento de tais condutas em diversas legislações penais já existentes sem ferir os preceitos do princípio da legalidade, anterioridade etc. E desta forma, tais condutas, sujeitarão os sujeitos praticantes de tais condutas às previsões de nosso ordenamento jurídico existente: o Código Penal e demais legislações aplicáveis.

CONCLUSÃO

Com o advento das novas tecnologias foi potencializado dos meios de comunicação em massa, principalmente por causa do desenvolvimento na área da informática. E estas inovações vêm, cada vez mais, refletindo no mundo das relações humanas e, por conseguinte, no Direito. Desta forma, cabe ao Direito regular tais relações que, assim como ele, se mostram cada vez mais dinâmicas, pois a cada dia sofrem mudanças.

A origem do computador e, por conseguinte, da Internet propiciaram diversas mudanças na vida do ser humano, especialmente no que se refere às formas de comunicação, onde a cada dia passam a ser possíveis de formas cada vez mais inovadoras (transmissão em tempo real, por exemplo).

Ocorre, que com a facilidade na prática de diversas ações, assim como a manifestação do pensamento, a comunicação sob todas as formas, várias pessoas têm utilizado a internet para a prática de ações lesivas a bens juridicamente tutelados pelo direito, e em especial, pelo Direito Penal. Esses bens, tais como a vida, o patrimônio, a honra etc., são os principais objetos visados pelos agentes de tais práticas.

A aplicação de repressão no tocante a tais condutas não pode ferir princípios constitucionais, sob pena de os ditames constitucionais acerca das liberdades individuais. Esses crimes praticados por meio do computador em alguns casos podem ser enquadrados em condutas ilícitas já previstas no código penal, tais como: o estelionato, fraudes, injúria, calúnia e difamação. E além das previsões no Código Penal, também estão presentes em outras legislações, como o Estatuto da Criança e do Adolescente, por exemplo. Outras condutas ilícitas presentes no Código Penal já mostram previsão às praticadas por meio do uso de elementos informáticos.

O Código de Processo Penal estabelece diversos critérios para a determinação da competência no tocante ao julgamento das condutas lesivas praticadas. Critérios como em razão da matéria, em razão da pessoa ou ainda em razão do lugar. E mesmo às praticados por meio do computador, devem seguir tais determinações.

A legislação penal existente no combate aos crimes virtuais ainda é ineficiente para reprimir todas as condutas criminosas cometidas por meio do computador ou contra seus dados e sistemas.

Assim, seja no território brasileiro ou em outros lugares do mundo, ponderando quanto aos aspectos econômicos e financeiro de tais crimes ou, ainda, tendo em vista todos aqueles que utilizam essa tecnologia de informação (como instituições financeiras ou o próprio Governo Federal em seus diversos órgãos), intensificam-se os investimentos em desenvolver medidas legislativas de proteção aos dados computadorizados. É ainda preciso dizer que com a difusão da Internet no mundo surgiram novas atividades comerciais pela rede mundial de computadores (*e-commerce)* que cada vez mais consubstanciam o ataque dessa nova criminalidade.

Ocorre que às práticas não estão voltadas apenas às pretensões econômicas ou financeiras, mas também a outros bens importantíssimos como os referentes à vida, à honra, ao patrimônio e em especial, às crianças, onde são divulgadas cenas de pornografia com crianças presentes.

Não se olvidando da capacitação jurídica, demasiadamente importante, os operadores do direito devem se adequar à nova realidade mundial, que busca diminuir fronteiras e a celeridade. O conhecimento acerca do ordenamento legal tem que ser associado ao conhecimento sobre as ferramentas virtuais, possibilitando o surgimento de profissionais capazes de solucionar conflitos atuais, que em sua maioria envolvem questões tecnológicas.

Além disso, o uso dessas tecnologias, associado à competência profissional, pode gerar a prestação de um serviço muito mais eficiente, além de tornar menos morosa a prestação jurisdicional. Para aumentar a segurança dos meios virtuais, as grandes empresas de navegação deveriam unir-se para desenvolver técnicas eficazes que possibilitassem a identificar o usuário agente criminoso.

O ordenamento jurídico penal brasileiro é deficiente em oferecer resposta aceitável para a perfeita solução quanto às condutas lesivas ou potencialmente lesivas que possam ser praticadas pela Internet e que não encontram adequação típica no estreito rol de delitos novos existentes no Código Penal e nas diversas leis especiais brasileiras que tratam da matéria.

Além do enquadramento perfeito e eficaz de tais condutas em face de legislações penais, é preciso que haja neste enquadramento as previsões no que se refere ao foro competente para julgar tais ações, visto que vários juízes podem ser igualmente competentes para julgar um mesmo ato.

Considerando que um mesmo indivíduo pode praticar por meio de um só computador diversas condutas lesivas e com resultado em diversos locais, é necessário que seja feita uma perfeita adequação ao estabelecer o foro competente para julgamento de tais condutas. Os critérios jurisdicionais, como a conexão, continência e prevenção, presentes no Código de Processo Penal mostram-se suficientes para pôr fim às questões em caso de dúvidas no tocante ao foro prevalecente no julgamento de tais condutas.

Por fim, para que se possa prevenir e combater a prática dos crimes de informática, é necessário que as autoridades legais disponham de todo tipo de recurso físico e virtual, para investigar e julgar tais crimes, mas observado o fato de que devem estar sempre à frente dos infratores em termos de equipamentos e informações. Sendo assim, legislações específicas acerca deste assunto se fazem imprescindíveis.

REFERÊNCIAS

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus aspectos processuais**. Rio de Janeiro: Lúmen Júris, 2003.

SILVA, Rita de Cássia Lopes. **Direito Penal e Sistema Informática** – São Paulo: Revista dos Tribunais, 2003.

PAESANI, Liliana Minardi. **Direito e Internet**, São Paulo: Atlas, 2006.

SCHOUERI, Luís Eduardo. **Internet – O direito na era virtual –** Rio de Janeiro: Forense, 2001.

MORAES, Alexandre de. **Direito Constitucional** 17ª Edição . Editora Atlas.

JESUS, Damásio E. de. **Direito Penal**, 1º Volume – Parte Geral. 25ª Edição, Editora Saraiva.

Vicente Paulo e Marcelo Alexandrino, **Direito Constitucional Descomplicado**, 2ª Edição, Editora Impetus.

JESUS, Damásio E. e Smanio, GianpaoloPoggio. In: Internet: **cenas de sexo explícito envolvendo menores e adolescentes – aspectos civis e penais**. Revista do Conselho Nacional de Política Criminal e Penitenciária. Brasília: vol. 1, n. 9, p. 27-29. janeiro/junho 1997

GRECO FILHO, Vicente. "**Algumas observações sobre o direito penal e a internet"**. Boletim IBCCRIM, edição especial. Ano 8, n. 95, outubro de 2000.

KARAM, Maria Lúcia. **Competência no Processo Penal**, 4ª edição, Editora Revista dos Tribunais, 2005.

NUCCI, Guilherme de Souza. **Manual de Processo Penal**, 3ª edição, Editora Revista dos Tribunais, 2007.

REIS, Alexandre Cebrian Araújo. e GONÇALVES, Victor Eduardo Rios. **Processo Penal**, Sinopses Jurídicas, 7ª Edição, Ed. Saraiva: 2003.

Mougenot, Edílson. **Curso de Processo Penal**. Ed. Saraiva, 2006.

CASTRO, Adelmario Araújo – **Livro Eletrônico – Noções de Informática**, disponível em: <http//:www.aldemario.adv.br> Acesso em 03/02/2013

ARAS, Vladimir. Crimes de Informática: **Uma nova criminalidade**. Disponível em: <http://www.jus2.com.br> Acesso em 12/05/2013.

SMANIO, Gianpaolo Poggio, **O bem jurídico e a Constituição Federal**. Disponível em <http://www.jus2.com.br> Acesso em 12/05/2013.

BRASIL. **Supremo Tribunal Federal**. Disponível em <www.stf.jus.br> Acesso em 20/08/2013.

BRASIL. **Superior Tribunal de Justiça**. Disponível em < www.stj.jus.br > Acesso em 20/08/2013.

BRASIL. **Tribunal Regional Federal da 2ª Região**. Disponível em < www.trf2.jus.br > Acesso em 20/08/2013.