Patrícia Santos da Silva

Direito e Crime Cibernético

Análise da competência em razão do lugar no julgamento de ações penais

Editora Vestnik

S586d

Patrícia Santos da Silva.

Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais [recurso eletrônico] / Patrícia Santos da Silva, Matheus Passos Silva (coord.). Brasília: Vestnik, 2015.

Recurso digital.

Inclui bibliografia.

Formato: ePub

Requisitos do sistema: multiplataforma

ISBN: 978-85-67636-13-9

Modo de acesso: World Wide Web

1. Direito. 2. Crime. 3. Internet. 4. Crime cibernético. 5. Ações penais. I. Título.

Editado por Matheus Passos Silva.

Editora Vestnik

CNB 13 Lote 9/10 Apto. 304 – Taguatinga

72115-135 – Brasília – DF

Tel.: (61) 8127-6437

Email: editoravestnik@gmail.com

Sobre a autora

Patrícia Santos da Silva é bacharel em Direito pela Faculdade Projeção (Brasília/DF).

Sobre o coordenador desta edição

Matheus Passos Silva atualmente (2015) cursa o doutorado em Direito, com especialização em Ciências Jurídico-Políticas, na Universidade de Lisboa (Portugal). Possui mestrado em Ciência Política pela Universidade de Brasília (2005) e graduação também em Ciência Política pela Universidade de Brasília (2002). Cursa também pós-graduação em Direito Eleitoral e em Direito Constitucional pelo Instituto Brasiliense de Direito Público (Brasília/DF, Brasil). É Conselheiro Científico e Editor da Revista Jus Scriptum, do Núcleo de Estudos Luso-Brasileiro da Faculdade de Direito da Universidade de Lisboa, desde 2014. Leciona disciplinas no curso de Direito, tais como Ciência Política e Teoria Geral do Estado, Filosofia Geral e Jurídica, Direito Constitucional, Direito Eleitoral, Orientação de Trabalho de Conclusão de Curso, História do Direito, Sociologia e Metodologia de Pesquisa. Tem larga experiência como coordenador de núcleo de pesquisa na área jurídica, bem como na coordenação de trabalhos de conclusão de curso. Dedicou-se ao Núcleo Docente Estruturante e ao Colegiado do curso de Direito em várias IES nas quais trabalhou. Áreas de interesse: Ciência Política, Democracia, Direito Constitucional, Direito Eleitoral, Direitos Políticos, Representatividade, Justiça, Nações e Nacionalismo no Leste Europeu. Mais informações sobre o autor podem ser encontradas nos links abaixo:

- Canal no Youtube: www.youtube.com/profmatheuspassos
- Página no Facebook: www.facebook.com/profmatheus
- Site do Prof. Matheus Passos: http://profmatheus.com
- Currículo Lattes: http://lattes.cnpq.br/4314733713823595

Sobre o Projeto “Jovens Juristas”

Venho trabalhando como orientador de trabalhos de conclusão de curso (TCC) do curso de Direito desde 2008. Neste período um dos meus principais objetivos foi incutir em meus alunos a ideia de que um TCC não pode (nem deve) ser visto apenas como “mais um trabalho acadêmico”: o trabalho faz parte de um processo de aprendizado e, como tal, deve ser visto como o ápice de uma graduação em nível superior. Desta maneira, a proposta foi a de transformar os TCCs, cada vez mais, em verdadeiros projetos de pesquisa acadêmica, ainda que com âmbito limitado devido à sua própria natureza – muitas vezes um TCC é o primeiro trabalho acadêmico-científico realizado pelo aluno.

É neste contexto que se insere o Projeto “Jovens Juristas”. O objetivo do projeto não é outro senão o de identificar, dentre os inúmeros trabalhos de conclusão de curso que são apresentados semestralmente pelos alunos, aqueles que mais se destacam, seja do ponto de vista da robustez doutrinária, seja do ponto de vista da inovação e/ou originalidade trazida pelo aluno ou ainda sob o ponto de vista da análise prática da realidade por meio de uma pesquisa de campo, de maneira que tais trabalhos possam ser publicados como livro em formato digital - o conhecido eBook. Todos os trabalhos publicados passaram pelo crivo de uma Banca Examinadora composta pelo professor-orientador e por pelo menos mais dois professores-examinadores. O projeto se iniciou em janeiro de 2014 e os livros já publicados podem ser obtidos por meio do site http://profmatheus.com/livros.

Este livro, intitulado *Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais*, tem por objetivo explicar como é determinada a competência para o processamento e julgamento dos crimes cibernéticos. A internet e o avanço das tecnologias informatizadas são fatores que influenciaram de forma direta no aparecimento desses crimes, precisando que o Estado começasse a ter olhos mais precisos com relação a estes ilícitos a fim de puni-los, fato este que só veio a ocorrer com maior exatidão com a aprovação da lei 12.737/12, posto que antes da citada norma, os crimes envolvendo o mundo virtual para sua prática eram punidos de forma análoga aos crimes tradicionais do Código Penal.

O objetivo do livro, logicamente, não é o de esgotar o assunto; ao contrário, tem-se como objetivo estimular a realização de mais pesquisas deste tipo no âmbito jurídico de maneira que se possa sair da *rotina* de trabalhos de conclusão de curso que são geralmente vistos pelos alunos como um mero "pré-requisito" para sua aprovação em uma disciplina. Espera-se que o Projeto "Jovens Juristas" incentive novos pesquisadores na área do Direito, além de fazer com que os autores participantes

possam, já no início de sua vida acadêmica, ter em seu currículo uma publicação que eventualmente poderá ser continuada no âmbito de uma pós-graduação ou de um mestrado.

O texto apresentado a seguir é o original conforme defendido pela aluna Patrícia Santos da Silva perante Banca Examinadora no ano de 2014, já com as devidas correções sugeridas pela Banca. A autora é detentora de todos os direitos autorais desta obra, sendo a mesmo a único responsável pelo conteúdo apresentado no livro.

Espero que a leitura seja agradável e que o texto possa enriquecer seus conhecimentos a respeito de tema.

Matheus Passos Silva

Projeto "Jovens Juristas"

Março de 2015

A autora por ela mesma

Meu nome é Patrícia Santos da Silva. Nasci dia 23/09/1987, na cidade de Floriano-PI, mas fui criada desde os 2 dias de nascida na cidade de São João dos Patos-MA, terra onde mora até hoje parte de minha família e de onde provém minhas raízes. Tenho 27 anos e sou Bacharelada em Direito pela Faculdade Projeção. No presente momento, dedico-me aos estudos em casa mesmo, com o objetivo de alçar uma vaga no serviço público na área jurídica e também de conquistar a tão difícil Carteira de Ordem dos Advogados do Brasil, pois apesar de não ter tamanho interesse em exercer a profissão de advogada penso em tê-la, por questão de honra e também porque ter esta, é normalmente requisito para alguns concursos que almejo. Além disso, é como uma forma de reconhecimento dos anos estudados na academia de Direito e de toda minha dedicação no decorrer dos 5 anos de curso.

Atualmente (2015), além de estudar para concurso conforme já mencionado, estou trabalhando como especialista na área dos direitos da mulher, em uma empresa de Call Center e me sinto muito feliz por poder ajudar a fazer com que as leis que primam pela justiça sejam espalhadas ao mundo.

Desde ainda criança tinha sonhos de seguir profissão na área jornalística ou jurídica. Recordo que sonhava em ser uma juíza respeitada, de grande renome e que fosse lembrada por ser justa. Sempre fui muito estudiosa, mas minha família não possuía condições de arcar com os custos de uma faculdade para mim, ainda mais para um curso tão caro quanto é o Direito, foi assim que tive que traçar metas e decidir os caminhos a serem seguidos, levando comigo sempre a confiança e a fé em Deus de que tudo iria dar certo. Desta forma, em 2008 resolvi ir embora de minha cidade São João dos Patos para tentar fazer um cursinho pré-vestibular na cidade de Teresina-PI. Posso dizer, que não foi nada fácil, mas com esforço e empenho de meus familiares consegui fazer o cursinho e ter o suficiente para manter-me longe de casa. Meu objetivo, era passar no vestibular da Universidade Estadual ou da Universidade Federal do Piauí. Confesso que nesta época estava um pouco descrente de fazer o curso de Direito, porque o via muito aquém da minha realidade, e então ao me inscrever para o Vestibular da Universidade Estadual do Piauí-UESPI, coloquei como opções o Direito e também Turismo. Ao realizar a prova sonhava em passar, mas com uma quantidade alta de candidatos, tudo poderia acontecer..., mas passei sim, porém não para o meu curso em primeira opção, (Direito), mas sim para o curso de Turismo que era minha segunda opção e ainda que não dentro do número de vagas, fiquei imensamente feliz de ter concorrido com um grande número de candidatos e ter ficado ao menos para na lista de 2 ª chamada; isso para mim era um grande sinal de

Deus de que logo eu estaria alcançando o que eu tanto desejava, que era me tornar universitária e uma profissional de sucesso, e ser assim motivo de orgulho para minha família. No ano seguinte, 2009, no mês de fevereiro vim para Brasília e desta vez não mais a passeio, mas para morar com minha irmã, que sempre me deu todo o apoio mesmo de longe para que eu nunca desistisse dos meus sonhos. Chegando aqui tentei de tudo: cheque educação, prova na UDF para ganhar bolsa de estudos e ganhei de fato 75%, mas foi através da minha nota do Enem de 2008 que eu consegui uma bolsa de 100% para o Curso do Serviço Social, e graças a Deus e às pessoas que cruzei pelo caminho mudei o curso para Direito, e no segundo semestre de 2009 estava eu iniciando uma jornada de 5 anos no curso dos meus sonhos - meu tão amado Direito na Faculdade Projeção, lugar onde fui muito bem recepcionada e onde conheci muitas pessoas especiais, professores inesquecíveis e onde aprendi de tal forma que nunca mais serei só uma moça que queria estudar, mas sim alguém que lutou, insistiu e venceu. Deus me abençoou e eu conseguir conquistar a minha tão sonhada vaga no mundo dos acadêmicos. Nesta mesma época também fui aprovada em 7º lugar para cursar na Escola Técnica de Brasília o curso de telecomunicações. Agradeci muito a Deus por tamanhas bênçãos e fiz ao mesmo tempo os dois cursos. Penso que Deus sempre ver nossa vida e tudo o que precisamos e se nele confiamos nossos desejos, ele realizará sempre e ainda pode nos surpreender com coisas além daquelas que esperávamos, porém tudo isso só ocorre no tempo dele, que é e sempre será o melhor momento, eu acredito nisso. No decorrer desses anos de curso de Direito tive a oportunidade de realizar estágios na área jurídica que me fizeram ser muito feliz e onde absorvi muitos ensinamentos acerca da justiça, das boas relações com as outras pessoas. Estagiar na Receita Federal do Brasil foi sem dúvida um grande presente para inicio de morada em Brasília, até mesmo porque nesse lugar conheci pessoas incríveis, aprendi muitas coisas que não ficaram apenas no ambiente de trabalho, mas que carrego comigo para minha vida. E da mesma forma ao estagiar no Tribunal de Justiça do Distrito Federal e Territórios, com muitos colegas dotados de grande saber jurídico, de grande personalidade, e ainda conviver com os advogados diariamente atendendo-os e vendo suas formas de atuação e com juízes e sua maneira de dizer o Direito, foi sem dúvida presentes de Deus que muito me acrescentaram na vida e que ficarão para sempre guardados em minha memória.

Considero-me uma pessoa guerreira e otimista, que acredita nos sonhos com muita fé em Deus e que sempre teve força de vontade para lutar por eles. Tenham certeza que ainda vão ouvir falar muito bem de mim, pois acredito que alçarei voos mais altos na vida e me tornarei alguém importante para a justiça de nosso País, talvez uma delegada e porque não uma importante juíza; serei alguém que lutará para que a justiça e o respeito às leis sejam feitos por todos, e ainda que todas as pessoas se sintam felizes por fazer parte deste nosso Brasil querido, e que possam um dia ser tratadas com igualdade conforme prevê a nossa Constituição Federal, sem distinção

de qualquer tipo.

Escrever além de ser uma arte é também um dom de Deus. As palavras tem o poder de adentrar em nossa mente e de ficar para sempre nela se tiverem sido escritas por alguém que se baseia no conhecimento e que escreve com amor uma história. Aquele que escreve tem a grande missão de bem dizer aquilo de que tem conhecimento, que absorveu ao longo do tempo, a partir de muitas leituras, dedicação em um determinado assunto e foco na realização da obra.

Dedicatória

Dedico este trabalho a Deus em primeiro lugar, por me permitir viver com saúde para conseguir realizar meus sonhos.

À minha família, especialmente à minha amada mãe, razão do meu viver, que sempre me apoiou em tudo o que busquei na vida e a quem dou o orgulho de mais uma graduação entre os irmãos.

À minha irmã Júlia que sempre me deu força e me fez ser cada dia uma pessoa mais confiante, alguém que sempre me ajudou como pôde, e nunca deixou de sonhar junto comigo e vibrar por minhas conquistas.

À minha irmã Silvana que nunca mediu esforços para me ajudar no que fosse preciso, sempre me incentivando a buscar o melhor que a vida pudesse me oferecer.

Ao meu amado e eterno irmão Carlos Alberto Santos da Silva (*in memorian*), o qual sei que muito se alegraria neste momento de êxito e conclusão de mais uma das jornadas de estudo, pelas quais já passei.

Agradecimentos

Agradeço a Deus por nunca ter deixado que eu desacreditasse que os sonhos poderiam ser realizados, e por estar comigo em todos os momentos, me mostrando que eu era capaz de vencer os meus próprios limites. A ti, meu senhor, é consagrada essa vitória, e que muitas outras venham, sob a tua supervisão e vontade.

À minha orientadora profa. Vyvyany Viana Nascimento de Azevedo Gulart, que me acompanhou durante o período de confecção desta monografia, acreditando sempre no meu sucesso.

Aos demais professores que me acompanharam no decorrer da caminhada do curso, os quais muito me ajudaram com seu apoio, livros emprestados, opiniões acerca do meu tema.

Por fim, agradeço aos amigos que direta ou indiretamente estiveram ao meu lado durante toda essa jornada de estudo, acreditando sempre em meu potencial, especialmente minha amiga querida Thatiana Mendes.

Resumo

O presente trabalho de conclusão do curso de Direito, da Faculdade Projeção, Taguatinga, 2014, tem por objetivo explicar como é determinada a competência para o processamento e julgamento dos crimes cibernéticos. Para o alcance de tal objetivo utilizou-se o método dedutivo, tendo em vista a pesquisa se desenvolver partindo de dados gerais acerca da competência territorial sedimentada para os crimes tradicionais, com o fim de aplica-la aos crimes cibernéticos. A internet e o avanço das tecnologias informatizadas são fatores que influenciaram de forma direta no aparecimento desses crimes, precisando que o Estado começasse a ter olhos mais precisos com relação a estes ilícitos, afim de puni-los, fato este que só veio a ocorrer com maior exatidão com a aprovação da lei 12.737/12, posto que antes da citada norma, os crimes envolvendo o mundo virtual para sua prática eram punidos de forma análoga aos crimes tradicionais do Código Penal. Os critérios para fixação da competência de modo geral são disciplinados no Código de Processo Penal, no artigo 69, todavia a doutrina e a jurisprudência tem feito tal determinação, usando as regras de competência como base no lugar de consumação do crime, em que se aplica a teoria do resultado (art. 70, CPP), ou ainda onde se localiza o provedor que permite o acesso, ou onde se encontra a máquina. É notável, que o uso do meio informático associado ao uso da rede de transmissão de dados (*internet*) do qual se utilizam os criminosos para cometer ilícitos penais envolvendo crimes cibernéticos, permitem que a conduta criminosa alcance distâncias muito além do território nacional, situação em que poderá ser aplicada a regra prevista no artigo 72 *caput*, que diz respeito ao lugar do domicílio do réu, e pelos parágrafos 1º e 2º, quando o réu possui mais de um domicílio ou residência, ou ainda quando não possui o réu lugar certo onde resida ou não se sabe onde ele se encontre, a competência se dará por meio do instituto da prevenção. Para tal estudo não serão observados todos os crimes cometidos pelo meio virtual, posto que a ideia não é esgotar o tema, mas entende-lo. Assim, serão vistos crimes como o racismo, contra a honra, pornografia infantil, para análise da competência de julgá-los.

Palavras-Chave: Internet; Crime; Cibernético; Território; Competência.

Introdução

Surgiram com a internet e os dispositivos informáticos, a exemplo do computador, celulares, tablets, dentre outras tecnologias digitais, uma grande quantidade de crimes efetuados não só por meio destas novas ferramentas, mas também contra estas, seus sistemas operacionais, arquivos particulares, dentre outros. Com isso, havia a necessidade de se ter uma lei que punisse os crimes cometidos contra os dispositivos informáticos e seus componentes no ordenamento jurídico brasileiro.

O Ordenamento Jurídico Brasileiro, ganhou uma lei específica que pune os crimes cibernéticos no país – a Lei 12.737/12. O legislador brasileiro elaborou referida lei que foi aprovada em novembro de 2012 e chamada de “Lei dos crimes cibernéticos” ou “Lei Carolina Dieckmann”. Com esta lei passa-se a punir a conduta de invasão de dispositivo informático sem a devida autorização do dono, onde o dispositivo esteja protegido por mecanismo de segurança, de modo que o criminoso precisa driblar tal mecanismo para então executar o crime.

Importante destacar, que há também os crimes que são cometidos tanto pelo uso da informática como sem o auxílio desta, podendo citar como exemplos: a injúria, a calunia, difamação, racismo, pedofilia e outros. Para os criminosos que atuam neste meio, a informática funciona nesses casos apenas como mais uma ferramenta por onde podem cometer tais crimes. Desta forma, nesses casos não se está lesando bem jurídico novo (advindo da própria informática), como a lei nova prevê, mas atinge-se bens jurídicos tradicionais do Código Penal.

É notório, que desenvolver uma pesquisa sobre os crimes cibernéticos no País, os modos de proteção que cada indivíduo pode utilizar e as proporções que uma conduta criminosa nesta seara podem alcançar, são de grande relevância para a sociedade, tendo em vista ser a internet um meio de comunicação bastante usado pela maior parte da população brasileira, e que por muitas vezes sem ter conhecimento específico acerca do uso e formas de proteção se deixam lesionar pelos infratores.

As controvérsias que circundam os crimes cibernéticos próprios e impróprios no país sobre a competência de julgamento desses crimes, ocorrem devido ao fato de que um crime cometido por meio de dispositivo informático, com ou sem o auxílio da rede de tráfego de transmissão de dados (internet), não surtem efeitos apenas locais ou estaduais, mas também podem ter abrangência nacional, o que faz em tese ser da justiça federal a competência nestes casos para julgar ações penais cibernéticas, e mais faz surgir a dúvida na hora de determinar a competência do juízo, se será o do lugar onde a prática delituosa teve início ou onde se consumou.

Além disso, por conta da lacuna legislativa no que concerne a matéria de competência para o processo e julgamento dos crimes cibernéticos, os quais causam efeitos tanto no território nacional brasileiro quanto fora dele, faz-se necessário a realização de um estudo aprofundado acerca do assunto sob a ótica da doutrina e jurisprudência, de modo a não restarem dúvidas acerca da forma como é determinada a competência para julgar tais crimes, observando para tanto a regra geral prevista no processo penal (teoria do resultado do crime).

A pesquisa se fundará no estudo doutrinário acerca do tema: "Direito e crime cibernético: análise da competência em razão do lugar para julgar ações penais", visando demonstrar ao final como é feita a determinação da competência para julgar os crimes cibernéticos sob a ótica doutrinária e jurisprudencial, e para tanto se utilizará da modalidade monografia, uma vez que esta se fundamenta na visão de vários doutrinadores acerca de determinado assunto.

É importante para esta monografia, ser feito um estudo de institutos referentes não só ao mundo da tecnologia informatizada, mas sobretudo referentes ao Direito Penal de forma geral, verificando sua extensão ao mundo virtual.

O estudo sobre os crimes cibernéticos, e a influência da informática para o aumento da criminalidade neste meio é de suma importância para sociedade, pois é uma área que se expande a cada dia, precisando desta forma de um olhar mais atento do judiciário, da polícia e da própria sociedade.

O objetivo geral da pesquisa monográfica será o de verificar se pode ser aplicada a regra da competência em razão do lugar, conforme previsto no artigo 70, do Código de Processo Penal para o processo e julgamento dos crimes cibernéticos. Para isso far-se-á a divisão da pesquisa monográfica em 4 capítulos, onde serão demonstrados institutos necessários ao estudo do tema e solução do problema de pesquisa.

No primeiro capítulo pretende-se discorrer acerca da internet, da tecnologia informatizada, a evolução histórica, bem como demonstrar qual a influência do uso destas tecnologias e da rede de transmissão de dados exercem na vida das pessoas que vivem em sociedade.

Já no segundo capítulo será feito um estudo acerca dos crimes cibernéticos dentro da sociedade brasileira, explicando o conceito de crime de forma geral e do crime cibernético, qual o bem jurídico afetado, como são classificados, quais são os criminosos que atuam na área informática e quem são as vítimas.

O terceiro capítulo tratará da competência de forma geral no âmbito do Direito Penal,

explicando cada critério de determinação de competência dada pela lei processual penal, sob a ótica da doutrina. Aqui também serão explicados o conceito de competência, o instituto da jurisdição e os princípios que se fazem necessários quando da aplicação da lei processual penal no espaço.

E no quarto capítulo será tratado do instituto da competência para julgar ações penais no âmbito da informática, o lugar do crime cibernético, a jurisdição, o espaço virtual onde são realizados esses crimes, sob a ótica doutrinária e jurisprudencial. Ao final deste capítulo será respondido ao seguinte questionamento: aplica-se a regra da competência em razão do lugar, conforme o previsto no artigo 70 do Código de Processo Penal para o processo e julgamento de crimes cibernéticos?

A internet

A internet é um meio de comunicação bastante utilizado pelas pessoas diariamente, sendo considerada pela maioria delas atualmente uma ferramenta de uso indispensável, pois com o seu uso é possível que uma pessoa consiga resolver várias coisas do seu dia-a-dia, sem precisar sair de casa, além de facilitar muito as relações sociais.

Nas palavras de Corrêa (2002, p. 42): “a internet é um paraíso de informações, e, pelo fato de estas serem riqueza, inevitavelmente atraem o crime. Onde há riqueza há crime”.

Das brilhantes palavras de Gustavo Corrêa acima citadas, pode-se compreender, que a internet possui um vasto banco de informações, e que estas por sua vez são consideradas riquezas aos olhos dos criminosos, que as observam com o intuito de cometer ilícitos e prejudicar a vida de outras pessoas.

Origem da internet

A internet originou-se nos Estados Unidos nos anos 60, quando foi desenvolvida uma rede de computadores de uso exclusivo de militares, como uma importante arma da guerra fria (CORRÊA, 2002, p. 7).

Afirma Crespo (2011, p. 30) ter a internet surgido exatamente no ano de 1966, no momento em que houve a união de algumas universidades para desenvolver o projeto da Arpanet, consoante o texto abaixo:

> Podemos dizer que ela surgiu na década de 60, mais precisamente no ano de 1966, quando algumas universidades, se uniram para desenvolver a ARPANET (*Advanced Research Projects Administration* – Administração de Projetos e Pesquisas Avançados). Naquela oportunidade, seu uso era exclusivo das Forças Armadas norte-americanas.

No entanto, afirma Paesani (2000, p. 25), que o projeto da *Arpanet* da agência de projetos avançados (arpa) do Departamento de Defesa norte-americana confiou, no ano de 1969 à *Rand Corporation* a confecção de um sistema onde fosse garantida que um ataque nuclear partindo da Rússia não interrompesse a corrente de comando dos Estados Unidos.

O propósito do projeto ARPANET era o de providenciar um continuado

funcionamento daquela rede, ainda que em casos de uma catástrofe como um ataque nuclear. Assim, era muito importante não existir um comando central, o qual pudesse ser um alvo (CRESPO, 2011, p. 30).

A solução foi se criar pequenas redes locais chamadas de LAN, postas em lugares planejados do País e coligadas por redes de comunicação à distância chamadas de WAN. Desta forma, se por acaso uma cidade fosse arruinada por um ataque nuclear, essa rede de comunicação conexa chamada de *Internet* ou *Inter Networing* (coligação de redes locais distantes), garantiria que a comunicação continuasse entre as cidades coligadas que sobrassem (PEDEMONTE apud PAESANI, 2000, p. 25).

No entanto para Paesani (2000, p. 25) a internet só se desenvolveu para valer, no ano de 1973, quando Vinton Cerf, membro 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*. Esse protocolo é um código que permite aos diversos *networks* incompatíveis por programas e sistemas de realizarem uma comunicação entre eles.

Segundo Silva (apud COSTA, 2011, p. 23):

> A *internet* de fato passou a existir com a ligação dos *backbones* NSF com a ARPANET. Define-se *backbone* como a espinha dorsal de cabos de telecomunicação de dados entre computadores de grande porte e roteadores que controlam o tráfego na *internet*, possibilitando a visualização e a transferência de dados através de quilômetros de distância.

O tempo passou, mas o princípio basilar da internet continuou vivo. Até hoje ela tem como base a ideia de não se produzir comandos centrais, tornando todos os pontos correspondentes (CRESPO, 2011, p. 31). Além disso, o mesmo autor ainda diz que, “toda essa evolução fez com que as relações comerciais, as administrações públicas e a sociedade em geral passassem a depender muito da eficiência e segurança da chamada tecnologia da informação” (CRESPO, 2011, p. 31).

No início da década de 1980, a ARPANET foi repartida em duas outras redes, a ARPANET e Milnet, esta última era uma rede militar. Esta interconexão das duas redes chamou-se DARPA Internet (LAQUEY; RYER apud CASTRO, 2003, p. 2-3).

Entende Paesani (2000, p. 26) que o elemento mais importante que fez com que a internet se tornasse um meio de comunicação em grande escala, foi a WWW, também conhecida como World Wide Web ou Web, vinculado a rede mundial.

Conceitualmente a World Wide Web é consoante Corrêa (2002, p. 11):

> um conjunto de padrões e tecnologias que possibilitam a utilização da Internet por meio dos programas navegadores, que por sua vez tiram todas as vantagens desse conjunto de padrões e tecnologias pela utilização do hipertexto e suas relações com a multimídia, como som e imagem, proporcionando ao usuário maior facilidade na sua utilização, e também a obtenção de melhores resultados.

Foi em março de 1989 que o World Wide Web nasceu, e também neste mês Tim Bernes-Lee, integrante do laboratório de Física de Genebra, sugeriu a criação de um sistema de hipertexto, onde fosse possível a comunicação de forma eficaz, entre grupo de pesquisadores que estivessem em diferentes lugares, os quais fizessem parte da *High Energy Physics Community* (CORRÊA, 2002, p. 11).

Contudo, o projeto foi apresentado e começou a ser desenvolvido somente em 1990. Neste ano o primeiro browser (WWW) começou a ser desenvolvido, ficando quase pronto do final deste mesmo ano. O princípio desse projeto já tinha sido mostrado, que era o hipertexto e a leitura de diferentes tipos de documentos (CORRÊA, 2002, p. 12). Acrescente-se ainda que foi em 1993, que iniciou-se um período de constante desenvolvimento da rede. No início deste ano foram criados os navegadores CERN Macintosh browser e o Mosaic (CORRÊA, 2000, p. 12).

Neste diapasão, tem-se que a internet foi desenvolvida em uma época de grande revolução mundial (Guerra Fria), momento em que existia certo medo de que ataques advindos da Rússia contra os Estados Unidos pudessem destruir o comando central deste. Porém a internet de fato ganhou lugar significativo no mundo, com a criação da World Wide Web, consoante apresentado pelos autores supra.

Conceito

A internet chegou ao convívio diário das pessoas, e sem ela praticamente não se faz mais nada. Mas o que seria então essa tecnologia que faz com que todos se encantem e resolvam por meio dela, encurtar as distâncias, ou mesmo, resolver problemas que antes precisavam de deslocamento de um lugar para outro e hoje não se faz mais necessário.

Nos dizeres de Fabrízio Rosa, a expressão internet somente foi assim denominada no ano de 1980, com a seguinte definição:

> (...) um conjunto de redes de computadores interligados pelo mundo inteiro, que têm em comum um conjunto de protocolos e serviços, possuindo a

> peculiaridade de funcionar pelo sistema de trocas de pacotes e cada pacote pode seguir uma rotina distinta para chegar ao mesmo ponto. (ROSA apud FERNANDES, 2013, p. 142).

A Internet (*Internconnected Networks*) é uma rede de computadores e outras redes menores que estão interligados ou conectados, a nível mundial por meio de um protocolo normal entre eles chamado de TCP/IP (*Transmission Control Protocol/Internet Protocol*). Disso decorre ter a internet referência direta e resumida como a chamada rede mundial de computadores. (ALMEIDA FILHO; CASTRO, 2005, p. 24, grifo do autor).

Para Crespo (2011, p. 30), “a internet é uma vastíssima rede capaz de interligar computadores de todo o mundo, possibilitando, assim, a comunicação entre eles”. Desta forma, entende o autor supra então, que a internet é uma grandiosa rede que tem a capacidade de realizar a comunicação entre vários computadores do mundo inteiro.

A internet de maneira técnica compõe-se de uma interligação entre milhares de computadores no mundo todo, por meio de protocolos (chamados de IP ou Internet Protocol). Isso quer dizer que essa interligação se faz possível, porque usa um mesmo padrão para transmitir os dados. (PECK, 2002, p. 14).

Esta tecnologia informática, consoante entendimento de Marcos Salt é definida como a segunda Revolução Industrial, diz também, que é mais modificadora do que a revolução industrial ocorrida no século XIX, tendo em vista o desenvolvimento de sua tecnologia e a influente ligação diária na vida da população (SALT apud COSTA, 2011, p. 20).

Entende Corrêa (2002, p. 8), que a internet é um sistema mundial de rede de computadores que permite a comunicação e a transferência de arquivos de uma máquina para qualquer outra que esteja interligada na rede, tornando possível, que haja uma troca de informações sem antecedente na história, de forma rápida, confiável, e onde não há fronteiras, gerando novos meios de relacionamento. Saliente-se ainda, que a internet não é o World Wide Web (WWW), posto que a aquela tem por significado o meio por meio do qual o correio eletrônico, os servidores FTP, a WWW, o *Usenet* e outros serviços transitam, e isso se deve a sua amplitude e extensão.

Por ser bastante abrangente, a internet atrai não só usuários domésticos, como também uma totalidade grandiosa de organizações do comércio que conhecem as estimativas referentes a sua popularização e capacidade de rendimento de lucros. (CORRÊA, 2002, p. 9). Assim, pode-se perceber que conforme o autor supra, a internet abre caminhos, que fascinam e permitem a navegação não só a uma pessoa que use da

máquina informatizada apenas para seu uso pessoal em casa, como também às pessoas que trabalham em setores do comércio.

Diante do exposto pelos autores citados acima, entende-se que a internet nada mais é do que uma forma de interligar duas ou mais pessoas independentemente do lugar onde elas estejam, por meio de uma conexão de redes capaz de fazer existir uma comunicação entre elas de forma rápida, eficiente, sem limites de alcance e em tempo real.

Funcionamento

Para que a internet funcione, faz-se necessário que alguns componentes trabalhem juntos, de modo a conectar um computador a outro, independentemente da parte do mundo em que estejam e quem deles se utiliza. Desta forma, será demonstrado nos parágrafos que seguem como se dá o funcionamento da internet.

Nas palavras de Érica Lourenço de Lima Ferreira, a internet: “é uma autêntica teia de aranha que permite múltiplas direções (navegações/websurfing) de um lado a outro do planeta”. (FERREIRA apud CAVALCANTE, 2011, p. 43).

A ligação de um computador a outro é feita por meio de linhas telefônicas, fibra ótica, satélite ou rádio. A conexão do computador com a rede pode ser de forma direta por intermédio de outro computador, que se conhece como servidor, e este último pode ser da própria pessoa ou de terceiros (provedores de acesso). (PECK, 2002, p. 14).

Consoante Almeida Filho; Castro (2005, p. 25), é necessário que um computador de uso doméstico esteja ligado a uma linha telefônica, por intermédio de um modem, que por sua vez liga para o computador de seu provedor de acesso à internet. Assim, enquanto houver conexão, também haverá comunicação entre o computador de uso doméstico (uso simples), e o computador do provedor.

Na comunicação via internet entre computadores, é gerado um protocolo de identificação da máquina, chamado de TCP/IP. É este protocolo que divide a mensagem que se deseja transmitir em pequenos blocos contendo informações, chamados pacotes de dados, e depois disso é que se verifica para onde se destina a mensagem e como fazer para refazer a mensagem original (ALMEIDA FILHO; CASTRO, 2005, p. 25). Ademais, o computador do provedor conduz os diversos pacotes da mensagem para um ponto de acesso que esteja mais próximo do computador destinatário da mensagem, e tudo isso é feito por máquinas chamadas roteadores (ALMEIDA FILHO; CASTRO, 2005, p. 26).

Neste tipo de conexão onde um computador se comunica com outro por meio de uma linha telefônica, transmissão de dados por discagem é atribuído um novo número ao computador do usuário, toda vez que ele navegar na rede. Desta forma, sempre que for finalizado o acesso, o número IP que identificava esta máquina, é liberado para ser usado como identificação do computador de outra pessoa. Entretanto, para alguns tipos de acesso via banda larga, o número de IP é único, ou seja, não muda vez que não há sessão de conexão. (ALMEIDA; FILHO, 2005, p. 27).

O IP é usado na internet com o intuito de atribuir a cada máquina um endereço individualizado, e é através desse número que se faz possível identificar de onde vem a mensagem e para onde vai. O endereço IP assume a forma de números, numa sequência de 4 *bytes* ou 32 *bits*, que são agrupados em quatro números de 8 *bits*, todos separados por um ponto (ALMEIDA FILHO; CASTRO, 2005, p. 27). Esse endereço IP, em forma de números é traduzido para os seus correspondentes em palavras por meio do protocolo chamado DNS (*Domain Name System*). (PECK, 2002, p. 14).

O usuário navega na internet por meio da utilização de um browser, ambiente operacional com interface gráfica que faz uso de aplicativos que permitem a visualização de ícones e a facilidade da navegação. São exemplos de browser o MS Internet Explorer de propriedade da Microsoft, o Netscape Navigator da Netscape, e outros. (PECK, 2002, p. 15).

As pessoas navegam na internet por diferentes modos atualmente, bastando para isso que se tenha um equipamento eletrônico com acesso à internet para que a comunicação se expanda por uma imensidão de lugares, a depender da escolha que o próprio navegante faça na hora em que decide realizar uma pesquisa utilizando-se desta rede.

A internet no Brasil

No ano de 1965, foi elaborado o Serviço Social de Processamento de Dados e ainda o Brasil se juntou ao consórcio internacional de telecomunicações por meio de satélite, conhecida por INTELSAT. Também foi criada a Empresa Brasileira de Telecomunicações, que é ligada ao Ministério das Comunicações, que havia sido criado a pouco tempo. Em 1972, surge o primeiro computador no País, cujo nome de patinho feio foi dado pela Universidade Federal de São Paulo (WENDT; JORGE, 2013, p. 8).

A consolidação da Internet ocorreu, segundo reportagem da Super Interessante Citada

por Wendt, em 1988 com a conexão à Bitnet da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), do Laboratório Nacional de Computação Científica (LNCC) e da Universidade Federal do Rio de Janeiro (UFRJ) (SUPER INTERSSANTE apud WENDT; JORGE, 2013, p. 8).

Segundo Rita de Cássia Lopes da Silva somente em 1992 é que foi implantada a primeira ligação de rede conectada à internet nas principais universidades, centros de pesquisa do Brasil e, em algumas ONGS – Organizações não Governamentais (SILVA apud COSTA, 2011, p. 24).

A regulamentação da Internet no Brasil adveio com a criação de um Comitê Gestor de internet no Brasil, no ano de 1995, em decisão conjunta do Ministério das Comunicações e o Ministério da Ciência e Tecnologia, que tinham como objetivo efetivar a participação da sociedade nas decisões sobre a implantação, administração e o uso da Internet (ALMEIDA FILHO; CASTRO, 2005, p. 30).

O Comitê foi criado pela Portaria Interministerial nº 147, datada de 31 de maio de 1995. Para compor esse comitê foram sorteadas representantes do Poder Público, das entidades operadoras e gestoras das linhas de conexão e alta velocidade, de provedores de serviço, de usuários, das empresas e das comunidades acadêmicas (ALMEIDA FILHO; CASTRO, 2005, p. 31).

Nas palavras de Corrêa (2002, p. 17-18):

> O Comitê Gestor Internet do Brasil é o maior exemplo da tendência mundial a tornar a Grande Rede algo desvinculado do Poder Público, incentivando a participação da sociedade civil na formulação de diretrizes básicas para o desenvolvimento organizado.

As principais funções do Comitê, que foram definidas ainda na época de sua criação são: fomentar o desenvolvimento de serviços Internet no Brasil; fazer recomendações de padrões e procedimentos técnicos e operacionais para a Internet no Brasil; coordenar a atribuição de endereços Internet, o registro de nomes de domínios e a interconexão de espinhas dorsais (*Backbones* ou linhas de conexão de alta velocidade de uma rede que se conectam às linhas de baixa velocidade) e coletar, organizar e espalhar informações sobre os serviços da Internet (ALMEIDA FILHO; CASTRO, 2005, p. 31).

Importante destacar, que o Comitê Gestor de Internet deu a FAPESP – Fundação de Amparo à Pesquisa do Estado de São Paulo, a função para realizar o registro de nomes de domínio denominado de “Registro.br” (RESOLUÇÃO Nº 2/98 apud

CASTRO, 2003, p. 4-5).

Assim, conforme o exposto pelos autores acima citados verifica-se que apesar do surgimento da internet no Brasil datar do ano de 1988, foi somente no ano de 1995, com a criação do Comitê Gestor Internet Brasil que ela foi de fato regulamentada no país passando assim, a ganhar força e expansão.

O computador

Importante, falar um pouco sobre o computador no presente trabalho, posto que este faz parte da evolução histórica da área tecnológica que lida com as informações transmitidas com tamanha rapidez e eficiência com o auxílio da internet, para um número bastante considerável de pessoas ao mesmo tempo.

A expressão computador vem do latim *computadore*, que significa aquele que faz cálculos. A primeira máquina que fez cálculos foi o ábaco, que já existem há 2000 a.C, sendo ainda hoje usada por países do Oriente. (PEREIRA apud COSTA, 2011, p. 14).

Computador é segundo consta no Mini Dicionário Aurélio Século XXI: “aparelho ou dispositivo capaz de realizar operações lógicas e matemáticas segundo programas previamente preparados.” (FERREIRA, 2000, p. 170).

Consoante escreve Castro (2003, p. 1):

> Computador é conceituado como sendo um processador de dados que pode efetuar cálculos importantes, incluindo numerosas operações aritméticas e lógicas, sem a intervenção do operador humano durante a execução. É a máquina ou sistema que armazena e transforma informações, sob o controle de instruções predeterminadas. Normalmente consiste em equipamento de entrada e saída, equipamento de armazenamento ou memória, unidade aritmética e lógica e unidade de controle. Em um último sentido, pode ser considerado como uma máquina que manipula informações sob diversas formas, podendo receber, comunicar, arquivar e recuperar dados digitais ou analógicos, bem como efetuar operações sobre lei.

Interessante notar, que a busca em desenvolver novos equipamentos que pudessem melhorar a vida do homem, não é recente. É neste sentido que ensina Crespo (2011, p. 27), dizendo que, “desde os primórdios até os dias atuais, o homem sempre buscou desenvolver máquinas e ferramentas que lhe fossem úteis nas atividades diárias”.

No século XVII, o francês Blaise Pascal criou a primeira calculadora, e esta serviu de base para o matemático alemão Gottfried Wilhelm von Leibniz concluir com esmero a ideia e criar uma máquina de multiplicar e dividir; pois a inventada por Pascal era capaz apenas de somar e diminuir. (CIVITA apud CASTRO, 2003, p. 1).

Na década de 40, John Von Neuman desenvolveu o EDVAC, que significa *Electronic Discrete Variable Automatic Computer*, que trazia com ele a funcionalidade da memória única, base da informática moderna. (CRESPO, 2011, p. 29). Porém, a criação do primeiro computador digital, automático e em grande Escala é de merecimento do Professor Howard Aiken, que fez o Mark I. (CRESPO, 2011, p. 29).

Importante destacar, todavia, que o primeiro computador eletrônico surgiu no ano de 1946, o qual foi criado por conta das necessidades dos militares, que foi denominado de ENIAC – *Eletronic Numeric Integrator and Calculator*, tendo sido usado para montar tabelas de cálculo das trajetórias dos projéteis. (CASTRO, 2003, p. 2). Esse computador foi desenvolvido pela Universidade de Morre, da Pensilvânia, pesava cerca de 30 toneladas e media uma área de 140 metros quadrados, além de ter o funcionamento com número próximo de 18.000 válvulas. (GOUVÊA apud CRESPO, 2011, p. 29-30).

É preciso destacar, que os computadores não eram acessíveis a todas as pessoas, e apenas com a criação dos transistores é que os computadores começaram a ser colocados no comércio. Atualmente esses transistores nem são mais usados, pois foram sendo substituídos pelos microprocessadores, os quais estão cada vez mais desenvolvidos, e serão lentamente trocados por *biochips* – circuitos orgânicos com DNA. (CRESPO, 2011, p. 30).

No ano de 1951 surgiram os primeiros computadores em série e, com a acelerada e a dominante evolução tecnológica hoje já se tem os PC computadores de uso pessoal e os notebooks. (CASTRO, 2003, p. 2).

Consoante Lima (2011, p. 2-3), tem o computador o ofício fundamental de fazer a concentração e a operação de informações, o que traz perigosa semelhança a nossa maneira de viver. Uma consequência de quem utiliza o computador, é que gera uma monitorização de nossas manias, o que não deve passar despercebido pelos legisladores de todos as especialidades do Direito.

Nas palavras de Kaminiski (2002): “o computador e seus efeitos, nos poucos anos que vêm trazendo modificações para as mais diversas práticas, tem suscitado novos problemas e ressaltado outros. Deixou de ser apenas uma máquina de escrever moderna”.

Como se pode observar das afirmações dos autores supracitados, o computador foi evoluindo com o passar dos anos, e com ele caminha a internet que como visto em tópico anterior, teve sua criação atrelada justamente ao uso do computador, capaz de transmitir informações no período da Guerra Fria, ocasião em que essas máquinas computadorizadas eram uma grande arma de defesa.

Cibernética

Nos termos do Minidicionário Aurélio Cibernética significa, “ciência que estuda as comunicações e o sistema de controle nos organismos vivos e também nas máquinas” (FERREIRA, 2000, p. 152). Compreende-se então que consoante o minidicionário, seria a cibernética aquela ciência, que pesquisa e busca entender as comunicações e os sistemas que controlam não só as pessoas como também as máquinas (estes últimos seres sem vida), mas que precisam da ação humana para funcionar.

Cientificamente a palavra cibernética tem surgimento no ano de1948, momento no qual Norbert Wiener (matemático), escreveu a obra: “Cibernética: ou controle e comunicação no animal e na máquina”. Importante esclarecer, todavia que o termo não foi empregado por Wiener pela primeira vez (CRESPO, 2011, p. 44).

Consoante Antônio Chaves, a etimologia do termo cibernética advém de uma palavra grega *kybernetes* – expressão esta que indica a arte do timoneiro, sendo a ciência geral dos sistemas informantes e em particular, dos sistemas de informação (CHAVES apud CRESPO, 2011, p. 45).

Wiener, usando um modelo matemático-reducionista, quis conceder às leis gerais da matemática de tornar possível prever, realizar o controle e compreender a capacidade retroalimentadora que existia entre homens, natureza e máquinas. (COLLI, 2010, p. 21).

A definição de cibernética consoante Roque Antônio Carrazza é:

> Cibernética é definida como sendo a ciência que trata das matérias, do cérebro, do sistema nervoso do homem, buscando descobrir seu funcionamento, analisando, de forma crítica e profunda, o modo de realização das coisas (CARRAZZA apud CRESPO, 2011, p. 45).

Segundo Colli (2010, p. 21), “a cibernética possui como um de seus fundamentos a interatividade entre sistemas de controle e processamento de informações entre maquina, seres vivos e sociedade”.

Ressalta Costa (2011, p. 17), que “enquanto o computador é um processador de dados, a cibernética é a ciência dos sistemas de informática. Não se pode com precisão definir seu campo de estudo, já que se encontra em constante transformação”.

Ademais, “o sistema informático, sob o ponto de vista cibernético, analisa a informação, a comunicação e o controle da vida humana, quer no seu mundo interior, quer no exterior”. (SILVA apud COSTA, 2011, p. 18).

Diante do que os autores aqui dizem a respeito da cibernética, entende-se que esta cuida de entender as comunicações, a transmissão de informações e como é que se dá o funcionamento desta comunicação, observando os seres humanos e as máquinas, que possuem sistemas capazes de fazer circular as informações.

Relação entre o Direito e a Informática

O mundo evoluiu bastante com o passar dos anos, e com a informática essa evolução tem sido constante dia-a-dia, pois as pessoas estão cada vez mais *online* e buscando resolver sua vida ao passo de um clique, e por tal processo evolutivo se faz necessário que o Direito olhe para a tecnologia informática com olhos precisos, de modo a identificar a sua participação enquanto objeto de uso do crime, ou de ser esta mesmo a afetada.

Na qualidade em que é o Direito um fenômeno cultural, deve estar seguindo, de alguma forma, a realidade temporal e geografica onde se desenvolve, tendo em vista que com as evoluções do mundo social, político e econômico exercem influência nos aspectos jurídicos. Ademais, se deve levar em conta que a informática, transformou-se em um importante instrumento de informação, e esta, por sua vez, se tornou bem econômico de grande valor. (CRESPO, 2011, p. 38).

Historicamente, todos os meios de comunicação componente da sociedade convergente passaram a ter importância jurídica no instante em que se tornaram ferramenta de comunicação em grande escala, uma vez que esta massificação do comportamento exige que a conduta seja olhada pelo Direito, pois se assim não for, poderá se criar uma insegurança no ordenamento jurídico e também na sociedade. (PECK, 2002, p. 26).

Aponta ainda Castro (2003, p. 5), que o avanço da tecnologia na área da informática causa uma imensa revolução nas relações sociais. As facilidades conquistadas por meio uso do computador e de forma essencial da internet, modificaram a vida moderna, e isso é que se chama de era da Informática.

Importante destacar que com a chamada “era da informática” surgem questionamentos acerca de um ramo do Direito, por onde são processadas as informações jurídicas em complemento ao trabalho executado pelo jurista. Este ramo é denominado de Informática Jurídica e de acordo com Kaminiski (2002), é quase unânime o uso desta nomenclatura entre os estudiosos da área, definindo-a da seguinte forma:

> A Informática Jurídica é o processamento e armazenamento eletrônico das informações jurídicas, com caráter complementar ao trabalho do operador do Direito; é o estudo da aplicação da informática como instrumento, e o conseqüente impacto na produtividade dos profissionais da área. E também a utilização do computador como ferramenta na Internet.

Acrescente-se também a existência do Direito da Informática, que em consonância com Kaminiski (2002), pode ser chamado de Direito Eletrônico, Ciberdireito, Direito Online, e outros, e que cuida dos valores éticos e as relações que surgem através da informática em sentido amplo, e ainda que estuda os efeitos jurídicos que surgem com a tecnologia.

Defende a ideia de um Direito Digital, a especialista nesta área, Patrícia Peck que sobre este escreve dizendo:

> O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal e Direito Internacional etc). (PECK, 2002, p. 25).

Pode-se afirmar ainda, consoante entendimento de Peck (2002, p. 26), que não há que se falar em um novo direito da internet, assim como não há também um direito televisivo ou direito radiofônico. Existem peculiaridades do veículo e que devem ser observados pelas várias especialidades do Direito, mas não necessita de se criar um novo ramo específico do Direito.

De fato, o direito da informática não aparenta ser, até o momento, um ramo específico do Direito, mas é visto como uma nova leitura, uma nova visão de interpretação das normas jurídicas aos olhos da sociedade da informação, do que um novo ramo. (CRESPO, 2011, p. 39).

Assevera Kaminski (2002) que, “o aporte da informática, como ferramenta para o tratamento da informação jurídica, transformou a atividade própria dos profissionais da área. Porém, a relação entre informática e Direito não se esgota na recepção da primeira pelo segundo: também existe um fenômeno inverso”.

A informática tem relação com muitos ramos do direito, e com o advento da internet tem exercido grande influência nas relações entre as pessoas, e gerado um aumento da criminalidade, que aos olhos dos criminosos, é mais uma nova ferramenta para cometerem ilícitos. Todavia, apesar de serem muitos os ramos do direito que se relacionam com a informática/internet, o presente trabalho não visa esgotar o tema falando de todos eles em demasia, pois a abordagem problemática do trabalho está ligada a ciência penal e processual penal.

Escreve Castro (2003, p. 6), que as inovações trazidas pela internet atingem o Direito em todas as suas formas. Encontramos na rede diversos tipos de objetos para se comprar, trocar e vender. Leilões são realizados. O comércio eletrônico, também chamado de e-commerce, cresce diariamente, as transações de bens, feitas por meio da internet multiplicam-se e trazem como consequência, um número bastante grande de pessoas consumindo. Pode ainda acrescer toda a publicidade utilizada com o objetivo de conseguir mais negócios.

No âmbito do Direito Constitucional, consoante ensina Lima (2011, p. 40), a relação deste com a informática é patente, uma vez que a Constituição Federal é a base do nosso ordenamento. Exemplificando, tem-se a liberdade de se comunicar, de modo especial pelo uso da internet, meio pelo qual é manifestado um das expressões fundamentais, que é a liberdade de pensar.

No que tange a área fiscal, diversos tributos recaem sobre as operações da internet, tendo em vista que os fatos geradores não mudam dos moldes tradicionais. Inclusive, é discutida a possível tributação do serviço de acesso à internet por meio do imposto de ICMS ou ISSQN. (Castro, 2003, p. 7).

Com a internet tudo ficou mais fácil, até mesmo para se estudar com a internet, tornou-se algo mais prático, rápido e independente de fronteiras de tempo e lugar específicos para isso. Nota-se também a influência forte da internet nas coisas mais simples, como pagar contas, ver extratos bancários, comunicação face a face com outra pessoa, por meio do monitor, e outros.

Em relação ao Direito Penal diz Crespo (2011, p. 44), que a relação deste com a informática também se mostra presente ao passo em que são postas em debates questões concernentes ao acesso não autorizado a sistemas, *spam*, engenharia social e

estelionato, vírus, legítima defesa referente a ataques nos sistemas de computador, local onde acontece o crime, Direito de Intervenção e de Velocidades, harmonização internacional, e outros.

Destaque-se que ao Direito Penal da Informática cabe o cuidado de uma nova realidade, de bens jurídicos específicos do âmbito da tecnologia de computadores e o que pode ser afetado com seu uso negativo. Nas palavras de Aras (2001):

> A toda nova realidade, uma nova disciplina. Daí cuidar-se do Direito Penal da Informática, ramo do direito público, voltado para a proteção de bens jurídicos computacionais inseridos em bancos de dados, em redes de computadores, ou em máquinas isoladas, incluindo a tutela penal do software, da liberdade individual, da ordem econômica, do patrimônio, do direito de autor, da propriedade industrial, etc. Vale dizer: tanto merecem proteção do Direito Penal da Informática o computador em si, com seus periféricos, dados, registros, programas e informações, quanto outros bens jurídicos, já protegidos noutros termos, mas que possam (também) ser atingidos, ameaçados ou lesados por meio do computador.

Pode-se ainda acrescer aqui as palavras de Castro (2003, p. 7), que entende ser devido a tantas coisas novas na área tecnológica, o aparecimento de novos tipos de delitos ou novas formas de se praticar os tipos penais que já se conhecem.

Diante das acepções aqui expostas pelos autores, é importante então que o Direito acompanhe a evolução tecnológica para adaptar-se às novas modalidades de fraudes, que por meio da informática/internet tem sido cada vez mais constantes, tendo em vista que a criminalidade no meio virtual atinge diversos bens jurídicos e influenciam ramos do Direito público, privado e até mesmo internacional.

Redes sociais e a privacidade

As redes sociais são nos dias atuais, uma febre nas relações de comunicação das pessoas, tendo em vista a facilidade de interação, o ultrapassar de fronteiras de tempo e distância que estas proporcionam aos seus usuários. São estas redes de relacionamento interpessoal que conectadas à Internet, proporcionam um modo de socialização ampla da sociedade, porém, trazem consigo uma crescente criminalidade na rede.

Segundo entendimento de Paulo Lima, a rede social por meio da internet é definida:

> Como um *site*, um lugar na telemática, onde pode o usuário publicar o perfil

> que julgar conveniente de si mesmo, anexando fotos, ideias, qualificações e outros dados pessoais. Tais informações serão disponibilizadas aos amigos digitais, de acordo com alguns critérios de privacidade definidos pelo site de relacionamento e por alguns do próprio usuário. (LIMA, 2011, p. 45).

As redes sociais na internet fazem a harmonização das relações entre milhões de pessoas e as empresas brasileiras e mundiais, sendo avaliado que cerca de 80% de brasileiros possuem um perfil em algum site de relacionamento. (LIMA, 2011, p. 45). Pode ser observado com base nesta porcentagem trazida pelo autor supra, que as redes fazem parte da vida de uma considerável parte da população do país.

São as redes, um novo meio de um fenômeno chamado hipercomunicabilidade, que faz com que no mesmo instante em que se esteja em contato com o mundo real, os outros eus, (que nas palavras de Stefano Rodolta, são chamados de personalidades digitais ou corpos digitais) mantenham a interação com outras pessoas em seus "avatares digitais", usando seus celulares (*smartphones*), *netbooks*, *ireaders* e vários outros instrumentos ao mesmo tempo. (LIMA, 2011, p. 45).

O facebook e o twiter, são algumas das redes da atualidade por meio das quais se faz um perfil de si mesmo, imperando uma comunicação constante entre as pessoas. No entanto com a publicização exacerbada de que as pessoas fazem de si mesmas, acabam atraindo a atenção dos criminosos e gerando crimes.

O facebook é uma rede americana, cuja sede fica em Palo Alto, na Califórnia, que foi lançada no mercado em 2004. Tem por fundador Mark Zuckerberg, ex-estudante de Harvad, que desenvolveu essa ideia com afinco num pedido feito pelos gêmeos Winklevoss, para que criasse um site de uso exclusivo de Havard. No início somente os estudantes de Havard poderiam aderir ao facebook, mas depois foi expandida epidemicamente ao Instituto de Tecnologia de Massachusetts, à Universidade de Boston, ao Boston College e a todas as escolas Ivy League. (LIMA, 2011, p. 48).

Esse *website* possui atualmente mais de 600 milhões de usuários ativos, sendo um dos primeiros no *ranking* de tráfego de visitantes do Alexa e um dos maiores sites de fotografias dos Estados Unidos e do mundo, com mais de 60 milhões de fotos novas publicadas semanalmente. (LIMA, 2011, p. 48).

Quanto ao Twiter é uma rede social, que tem como característica servir como criador e servidor de *microblogging*. De forma básica, permite aos usuários enviar e receber atualizações pessoais de outros contatos em tempo real, bem como as enviadas a outros usuários. Há limite de caracteres de texto, limitados a 140 caracteres, chamados de tweets; possui acesso e postagem gratuitos, podendo ser feitos pelo

website, por SMS ou ainda por programas específicos. (LIMA, 2011, p. 49).

Considerando que as pessoas utilizam esses sites para suprir a solidão em que vivem, para encontrar em amigos virtuais, uma amizade diferente que entende o eu alheio, pode se mencionar o que Paulo Lima traz acerca dessas solidões quando cita Robert Weiss:

> Para o sociólogo americano Robert Weiss, existem dois tipos de solidão: a emocional e a social. Segundo Weis, "a solidão emocional é o sentimento de vazio e inquietação causado pela falta de relacionamentos profundos. A solidão social é o sentimento de tédio e marginalidade causado pela falta de amizades ou de um sentimento de pertencer a uma comunidade. (LIMA, 2011, p. 47).

Importante destacar que conforme escreve Gisele Truzzi de Lima, nas redes sociais, a informação é um bem de muita preciosidade no mundo virtual, e nesse se sobressai aquele que mais escreve no twiter, compartilha fotos antes de todos no facebook, aquele que informa a todos o que está acontecendo em primeira mão, os que divulgam sua vida para os amigos. (LIMA, 2010, p. 1).

Pode-se notar, que com o uso inadequado das redes sociais e da internet, a violação da vida privada das pessoas acaba sendo um alvo fácil aos olhos dos criminosos, que aproveitam da falta de bom senso que muitos internautas possuem para cometer crimes que afetam de modo direto ou indireto a vida privada de cada uma.

Entretanto, no que concerne a qualquer forma de tecnologia, não se pode estabelecer que seja esta um instrumento do bem, ou em outra vertente, um caminho para a perdição, isso considerando sempre, que o uso do instrumento da tecnologia é que vai determinar qual o seu fim, sendo por excelência, neutro em sua substância. (LIMA, 2011, p. 46).

Ressalta Gisele Truzzi de Lima, que o fato de ficarem muito tempo online, e na maior parte usando redes sociais, faz com que os usuários sejam muito acessíveis na internet. E a mania de se expressar em demasia no meio virtual pode ocasionar situações reais, com publicação de comentários e conteúdos indevidos, fotos publicadas e vídeos que causam constrangimento, etc. (LIMA, 2010, p. 3). Existe inclusive tratamento psicológico para pessoas que são viciadas em estarem conectadas à internet, as quais juntam milhares de fotos nos seus computadores pessoais ou que passam até 35 horas, sem descanso, ligados à internet (ARRAIS; VILLAS BOAS apud CRESPO, 2011, p. 26).

Todos esses atos mencionados por Gisele Truzzi de Lima no tópico anterior afrontam à privacidade do indivíduo, que é um direito resguardado por meio da Constituição expressamente.

Prevê o texto constitucional brasileiro que são assegurados, a todos os brasileiros e estrangeiros que aqui residem, o direito a ter sua vida particular sem deturpações, na forma do inciso X, do artigo 5º, *in verbis*: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". (CF, Art. 5º, X).

Segundo entendimento de Tulio Lima Vianna, o direito fundamental à privacidade deve ser interpretado, não só como uma proteção de um interesse particular de alguém, mas como fundamento do Estado Democrático de Direito. A garantia à privacidade é também estendida à liberdade, quando se diminui o exercício do poder de disciplinar, e ainda garantia à igualdade, quando se restringe a filtragem característica do exercício do biopoder. O surgimento das modernas tecnologias de monitoração eletrônica, registro informático e reconhecimento biométrico, um Estado só resguardará um pouco de liberdade e igualdade de seus cidadãos se der como garantia a todos o direito de ter privacidade. (VIANNA, 2006, p. 157).

Nas palavras do Consultor Legislativo da Câmara Bernardo E. F. Lins:

> A privacidade na Internet relaciona-se, de forma análoga à imprensa, à revelação de fatos privados embaraçosos e ao uso de métodos questionáveis para coleta de informações. No primeiro caso, a similaridade com o veículo de imprensa é clara: será violação à privacidade a divulgação, através da Internet, de dados ou fatos que atentem contra a intimidade, a vida privada, a honra e a imagem de uma pessoa. Tal divulgação poderá ser feita por um "site", por correio eletrônico ou por arquivo disponível para cópia. No entanto, a Internet traz um agravante: a rede é mundial e o fato poderá ser divulgado em escala nunca antes alcançada por outros meios de comunicação de massa. Tal circunstância levanta, inclusive, aspectos de natureza técnica: os fatos podem ser divulgados a partir de países que, por não dispor de legislação para tal, não punirão a ocorrência, dando um caráter de impunidade à atitude delituosa. (CÂMARA DOS DEPUTADOS, 2000, p. 7).

Disciplina Tulio Lima Vianna acerca do direito à privacidade que:

> O direito à privacidade, concebido como uma tríade de direitos – direito de não ser monitorado, direito de não ser registrado e direito de não ser

> reconhecido (direito de não ter registros pessoais publicados) – transcende, pois, nas sociedades informacionais, os limites de mero direito de interesse privado para se tornar em um dos fundamentos do Estado Democrático de Direito. (VIANNA, 2006, p. 84).

Conforme entendimento dos autores aqui citados, com o uso das redes sociais por meio da internet, qualquer um se torna um alvo fácil nas mãos dos criminosos, onde estes irão agir de acordo com o que é exposto pelo usuário nas redes. As pessoas tem se tornado muito dependentes da vida online, entretanto, é necessário buscar conhecer melhor esse meio de comunicação, pois a ignorância no mundo virtual leva muitas pessoas a viverem na escuridão tecnológica.

Crime cibernético

Os crimes cometidos contra os dados informáticos e sistemas de computadores privados ou públicos, chamados de crimes cibernéticos próprios, precisavam de uma lei que os disciplinasse no Brasil, para que os agentes criminosos atuantes desta seara pudessem ser devidamente punidos.

Como escreve Greco (2013, p. 94), a lei é a única fonte do Direito Penal, quando se pretende proibir ou tornar obrigatórias condutas sob ameaça de uma penalização. O que não estiver expressamente proibido é algo admissível no Direito Penal.

Importante destacar, que os crimes cometidos em meio ambiente virtual ou contra os dados e sistemas de funcionamento de uma máquina informatizada, são consequência da evolução dos equipamentos de comunicação eletrônicos/informatizados e da internet.

Assegura Ulrich Sieber, professor da Universidade de Wurzburg e grande especialista no assunto, os crimes cometidos por meio eletrônico surgiram na década de 1960, época na qual apareceram na imprensa e na literatura científica os primeiros casos de crime usando o computador, que eram constituídos principalmente por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, sendo denunciados principalmente em matérias de jornais. (FERREIRA, 2001, p. 209).

Entretanto, afirma Lima (2011, p. 7), que os crimes de computador surgiram nas últimas décadas do século XX, em meados dos anos 70, seguindo o aumento do uso de computadores, onde eram consideradas condutas criminosas as que eram feitas pelo uso de um computador estivesse este ligado a rede ou não, e nesta seara estariam inclusos os crimes de manipulação de dados de instituição financeira, a cópia ilegal de programas de computador, a revelação de segredo de informação computadorizada, tendo como exemplo, a recente divulgação pela Internet da declaração do imposto de renda do ex-presidente da República.

Questionava Paulo Lima, em 2011 no livro “Crimes de Computador e Segurança Computacional”, sobre a necessidade de se ter uma lei punindo os crimes cibernéticos no País.

> Em que pese a existência da chamada “Lei do Software” (Lei Federal nº 9.609, de 19 de fevereiro de 1998), muito há que se caminhar no sentido de um sistema jurídico protetor de dados eletrônicos e sistemas informáticos. Não há, ainda, uma figura típica para reprimir as condutas criminosas

> cometidas por meio de computador ou contra seus dados e sistemas. As normas existentes em nosso ordenamento jurídico não protegem de forma plena, por exemplo, delitos contra a honra cometidos por meios informáticos ou violação de correspondência eletrônica. (LIMA, 2011, p. 5).

Cumpre informar, que no fim do ano de 2012, o Estado brasileiro, ganhou duas novas leis disciplinando especificamente sobre crime cibernético, que traz uma penalização aos agentes criminosos atuantes no setor informático. São estas, as leis 12.735 e 12.737, de 2012, sancionadas pela Presidente Dilma Rosselff em 30/11/12 e publicadas no DOU dia 03/12/12, com início para entrada em vigor a partir de 120 dias após sua publicação, conforme determina o próprio texto das leis. (PLANALTO, 2012).

Com a aprovação das mencionadas leis, pode hoje o Brasil punir condutas criminosas que atentem contra a própria máquina e os dados informáticos, afetando a vida de quem utiliza desta tecnologia sem malícia, pois conforme será visto neste capítulo, há dois tipos de crimes cibernéticos, um que não possuía lei punindo-os e o outro que era punido de forma semelhante aos demais crimes tradicionalmente previstos na legislação penal.

Conceito de crime

A figura do crime dentro do Direito Penal possui certas particularidades, sem as quais não há que se falar em conduta criminosa. Para que efetivamente exista uma sanção a alguém, faz-se necessário que o fato por esta praticado esteja previamente previsto em lei. Desta forma, insta aqui demonstrar o que a doutrina e a lei disciplinam acerca do conceito de crime.

O legislador quando da edição do Código Penal, não definiu crime, conforme se pode perceber da redação do artigo 1º do citado código, onde é feita apenas uma explicação entre o fato considerado criminoso e sua previsão legal, dizendo que uma conduta humana só é punível como crime aos olhos da lei se esta lesar bem jurídico importante, e restar prevista na lei penal antes do fato típico ser cometido pelo indivíduo. (CP, art. 1º).

É preciso mencionar também que a lei de introdução ao Direito Penal (Decreto – Lei n. 3.914/41), não define crime, fazendo apenas uma diferenciação do que é crime e contravenção que se materializa na questão das penas e sua forma de aplicação, quando diz em seu artigo 1º:

> Considera-se crime a infração penal a que a lei comina pena de reclusão ou

> de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente.

Conforme comenta Heleno Fragoso, essa lei de introdução, sem ter preocupação de forma científica e doutrinária, se limitou em tão somente dar ênfase as características que diferenciam as infrações penais que são consideradas crimes das que são vistas como contravenções penais, as quais de forma notória se restringe à natureza da penalidade de prisão que é aplicada. (FRAGOSO apud BITENCOURT, 2012, p. 271).

Hoje, o conceito dado ao crime surge da doutrina. Não há um conceito de crime fornecido pelo legislador, restando-nos, no entanto, o conceito doutrinário. Não foram poucos os doutrinadores, que por muitos anos, tentaram encontrar uma forma melhor de conceituar o crime. Os conceitos mais difundidos são: formal, material e analítico. (GRECO, 2013, p. 140).

Formalmente crime é aquele resultante da inclusão de uma conduta ao texto legal, deste modo, tudo o que o legislador diz ser conduta criminosa, então será, sem ater-se ao conteúdo do ilícito. “Considerar a existência de um crime sem levar em conta sua essência ou lesividade material afronta o princípio constitucional da dignidade da pessoa humana”. (CAPEZ, 2012, p. 134).

Materialmente se conceitua o crime como aquilo que a sociedade vê como uma conduta que pode ou deve ser proibida por lei, pois que ofendendo um bem jurídico protegido de alguém, mereça receber uma penalização. (NUCCI, 2012, p. 174).

Capez (2012, p. 134), diz que crime sob esse aspecto (material) é aquele que busca fazer firme qual a substância do conceito, ou seja, entender a razão de determinado fato humano ser considerado criminoso ou não.

Ressalta Nucci (2012, p. 175), que o crime formal nasceu, a partir do conceito material de crime, só que formalmente previsto em lei.

No que concerne ao aspecto analítico pode ser citada a visão de Capez (2012, p. 134), para quem o crime sob esse aspecto é fato típico e antijurídico, entendendo desta forma que a culpabilidade do agente não integra a conduta criminosa. Para ele o aspecto analítico:

> É aquele que busca, sob um prisma jurídico, estabelecer os elementos estruturais do crime. A finalidade deste enfoque é propiciar a correta e mais justa decisão sobre a infração penal e seu autor, fazendo com que o julgador

> ou intérprete desenvolva o seu raciocínio em etapas. Sob esse ângulo, crime é todo fato típico e ilícito. (...).

Há também alguns autores, a exemplo de Mezger e, entre nós, Basileu Garcia, que asseguram que a punibilidade também faz parte de tal conceito, sendo o crime, pois, uma ação típica, ilícita, culpável e punível (GRECO, 2013, p. 143). Para esses autores, o crime analiticamente deve conter quatro elementos particulares da conduta, sem os quais não há que se falar em crime.

No entanto, a maioria dos doutrinadores entende que para poder mencionar a figura do crime é preciso que o agente tenha praticado uma ação típica, ilícita e culpável (GRECO, 2013, p. 144).

Assis Toledo adepto do conceito tripartido de crime, assim escreve:

> Substancialmente, o crime é um fato humano que lesa ou expõe a perigo bens jurídicos (jurídico-penais) protegidos. Essa definição é, porém, insuficiente para a dogmática penal, que necessita de outra mais analítica, apta a pôr à mostra os aspectos essenciais ou os elementos estruturais do conceito de crime. E dentre as várias definições analíticas que têm sido propostas por importantes penalistas, parece-nos mais aceitável a que considera as três notas fundamentais do fato-crime, a saber: ação típica (tipicidade), ilícita ou antijurídica (ilicitude) e culpável (culpabilidade). O crime, nessa concepção que adotamos, é, pois, ação típica, ilícita e culpável. (TOLEDO apud GRECO, 2013, p. 143).

Nas palavras de Zaffaroni:

> delito é uma conduta humana individualizada mediante um dispositivo legal (tipo) que revela sua proibição (típica), que por não estar permitida por nenhum preceito jurídico (causa de justificação) é contrária ao ordenamento jurídico (antijurídica) e que, por ser exigível do autor que atuasse de outra maneira nessa circunstância, lhe é reprovável (culpável). (ZAFFARONI apud GRECO, 2013, p. 144).

Desta maneira, conforme foi aqui explicado, verifica-se que a maioria doutrinária segue o conceito analítico de crime na forma tripartida, pois entendem que assim o crime é melhor estudado, e ainda por ser neste conceito onde são verificados com clareza os três elementos que o crime deve possuir de forma particular, e que são inseparáveis. Assim o crime precisa ter três elementos: fato típico, ilícito e culpável, sem os quais não há crime.

Conceito de crime cibernético

O conceito atribuído aos crimes que se utilizam dos dispositivos informáticos para cometer ilícitos penais, com ou sem o auxílio da rede de transmissão de dados, varia de acordo com o entendimento de cada doutrinador acerca desses ilícitos e do seu meio de execução, tendo por isso várias nomenclaturas esparsas na doutrina.

A fenomenologia criminal no que concerne às TIC (Tecnologias de Informação e Comunicação) é cada vez mais profunda e diversa, e sua presença muda sempre, adaptando-se às novas potencialidades tecnológicas e sociais. (CASABONA apud CRESPO, 2011, p. 46).

Conforme Costa (2011, p. 51), “trouxe a internet um novo mundo, denominado digital. Nele as pessoas navegam, se comunicam e de um mundo virtual praticam condutas e consequências em um mundo real.” Deste modo, vê-se que com base na afirmação do autor acima citado, a internet pode ser muito útil, mas a partir dela muitas condutas efetuadas virtualmente poderão ter efeitos exteriorizados no mundo natural.

Klaus Tiedemann denomina “criminalidade informática” todas as formas de comportamento ilegal que venham a, de qualquer forma, provocar danos sociais, por intermédio de um computador. (TIEDEMANN apud LIMA, 2011, p. 9).

Crime de Computador é a nomenclatura utilizada por Paulo Lima, porque entende que o computador é a ferramenta básica para o cometimento desses crimes. Do mesmo modo, diz que se o computador for usado como um instrumento facilitador da pratica criminosa, também há de ser considerado um crime deste tipo. (LIMA, 2011, p. 8).

Ricardo Martin entende de forma diferente sobre o conceito de crime informático, usando esta nomenclatura por acha-la simples e porque para ele é a expressão que mais equivale ao termo inglês *computer crimes*, dizendo ser este tipo de crime toda ação investida de dolo, que seja prejudicial a pessoas ou entidades, usando para essa efetivação, os dispositivos usados rotineiramente para realizar tarefas de informática. (MARTIN apud LIMA, 2011, p. 10).

Crespo (2011, p. 50-51) adota o nome de crimes digitais, apesar de haver muitas contrariedades na doutrina, fundamentando sua nomenclatura ao fato de que ser a informática uma das coisas a serem reguladas ou ainda porque a informática é um pressuposto de outro meio onde se cometem ilícitos hodiernamente – a telemática.

Contudo, apesar de ser adepto da nomenclatura crimes digitais, Marcelo Crespo

concorda com o nome delitos informáticos, dos quais são adeptos Rossini e Bonilha, dizendo que às condutas praticadas por meio da informática não se pode atribuir ligação unicamente ao computador, uma vez que se verificam delitos cometidos com o uso das telecomunicações, da telemática. Contudo, já que a telecomunicação precisa da informática, não há equivoco quanto a nomenclatura "*delitos informáticos*" em vez de dizer "*delitos telemáticos*". (CRESPO, 2011, p. 49, grifo nosso).

Ivette Senise Ferreira, usando o nome crime da informática, diz ser este "toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão." (FERREIRA apud COSTA, 2011, p. 51).

Segundo Peritos convidados pela OCED (Organização para a Cooperação Econômica e Desenvolvimento da Organização das Nações Unidas – ONU) para Paris, em maio de 1983, "o termo *crimes de computador* define, como qualquer comportamento antijurídico, não ético ou não autorizado, relacionado com o processamento de dados e/ou transmissão de dados". (COMPUTER RELATED CRIMINALLITY apud LIMA, 2011, p. 12). Opera-se aqui, uma similitude com o conceito acima trazido pela doutrinadora Ivette Senise Ferreira.

Sandra Gouvêa tem preferência pelo uso da expressão "crimes por meio da informática", dando como justificativa a sua escolha a razão de que os computadores não são os únicos instrumentos capazes de serem usados nas práticas criminosas. (GOUVÊA apud CRESPO, 2011, p. 48).

Por fim, conforme muito bem explicado por Ivette Senise Ferreira, não há um consenso acerca do conceito de crime cibernético entre os estudiosos porque:

> As várias possibilidades de ação criminosa na área informática, assim entendida em seu sentido lato, abrangendo todas as tecnologias da informação, do processamento e da transmissão de dados, originaram uma forma de criminalidade que, apesar da diversidade de suas classificações, pode ser identificada pelo seu objeto ou pelos meios de atuação, os quais fornecem um denominador comum, embora com diferentes denominações nos vários países ou nos diferentes autores. (FERREIRA 2001, p. 208).

Verifica-se então, que não há uma nomenclatura sedimentada pelos doutrinadores acerca do conceito de crime cibernético. De uma forma ou de outra o que muda é só o nome atribuído a esses crimes, posto que devem ser observados o uso de dispositivos informáticos, a rede de transmissão de dados para delinquir, o bem jurídico lesado, e ainda deve a conduta ser típica, antijurídica e culpável.

Bem jurídico

O bem jurídico na seara da informática poderá ser diferente em relação aos bens jurídicos tutelados no Direito Penal tradicional, no entanto merecem proteção por este ramo do direito se for um bem indispensável para o indivíduo vivente do meio social.

Para o Direito Penal, o conceito de bem jurídico possui características mais específicas. Tudo isso considerando o caráter secundário do Direito Penal, que apenas deve preocupar-se de proteger e tutelar os bens mais importantes e indispensáveis nas relações em sociedade. (LIMA, 2011, p. 2).

O Direito Penal só é legítimo para privar alguém de sua liberdade, se cumprir uma série de requisitos impostos pela legislação. Primeiramente, o limite de poder de punir do Estado se acha no princípio da legalidade, e como esse, para que haja limitação do direito de liberdade de um indivíduo, é preciso que quando este cometer conduta criminosa, tenha sido esta tutelada como ilícita antes mesmo de haver sua execução, e reprimida pela legislação penal. (LIMA, 2011, p. 1).

Existem várias interpretações para o que se chama de "*bem jurídico*", mas a doutrina majoritariamente entende que este é uma limitação do poder de punir do Estado. (CRESPO, 2011, p. 54, grifo nosso).

A evolução grandiosa da informática estabeleceu um importante ponto de referência na história da comunicação e das relações sociais, buscando novas ideias no que tange a bens jurídicos, até mesmo influenciando nas classificações sobre os fatos que sejam crimes digitais. (CRESPO, 2011, p. 56).

Os crimes realizados por meio de dispositivos informáticos afetam não só os bens que já eram juridicamente amparados pelo Direito Penal, como alcança uma enormidade de bens jurídicos novos. Nesse sentido, são as palavras de Crespo (2011, p. 56), que diz:

> Ao considerarmos as condutas ilícitas por meio da informática, verificamos a possibilidade de lesão a outros bens jurídicos. Assim, pode-se falar em condutas dirigidas a atingir não só aqueles valores que já gozam de proteção jurídica, como a vida, a integridade física, o patrimônio, a fé pública, mas, também as informações armazenadas (dados), a segurança dos sistemas de redes informáticas ou de telecomunicações.

No entendimento de Lima (2011, p. 3) "há de ser considerado, de um lado, que parte da nova criminalidade informática somente tem utilizado meios computadorizados

para a prática de infrações penais comuns, com ataques a bens jurídicos já tradicionalmente protegidos pelo ordenamento penal (...)".

Por outro lado, ainda segundo Lima (2011, p. 4) não são todas as condutas realizadas por meio de computadores, que recaem sobre esses bens jurídicos já tradicionalmente conhecidos, pois a nova delinquência na seara da informática recai também sobre objetos relativos de fato à informática, como os *hardwares*, programas, dados, documentos eletrônicos, etc.

Desta forma, da acepção trazida pelo autor supracitado nos dois parágrafos anteriores, pode-se perceber que os criminosos na área informática usam deste meio para atingir tanto bens jurídicos tradicionais, quanto bens jurídicos novos, (a própria máquina e seus artefatos que fazem parte de sua composição).

Consoante Roriva Del Canto, o principal bem jurídico nos crimes digitais é a informação, e de forma suplementar os dados ou os sistemas. Essa ideia, parte do fundamento de que os dados são apenas a representação eletrônica ou digital da informação, mesmo que os valores variem, e os sistemas são os mecanismos materiais de funções automáticas de armazenamento, tratamento e transferência. (CANTO apud CRESPO, 2011, p. 57).

É importante então, com base nos entendimentos aqui apresentados que seja observado qual o bem jurídico lesado, quando se está diante de um crime cometido pelo meio virtual ou contra os dados e sistemas de dispositivos informáticos.

Classificação dos crimes

A classificação dos crimes cibernéticos não é unívoca em toda a doutrina, variando de acordo com cada autor estudioso do tema. A informática é uma área que vive em constante processo de evolução, onde sempre há uma novidade tecnológica capaz de deixar os equipamentos informáticos cada vez melhores e visado pelos criminosos.

No presente trabalho tecer-se-á considerações sobre a classificação mais usada atualmente entre os doutrinadores.

Assim, temos Ferreira (2001, p. 214-215) que adota a classificação de crimes informáticos elaborada por Hervé Croze e Yves Bismuth, a qual é adotada também por muitos, onde os citados autores fazem uma distinção entre duas categorias desses crimes informáticos, quais sejam: os atos dirigidos contra um sistema de informática, por qualquer motivo; os atos que atentam contra outros valores sociais ou outros bens jurídicos, cometidos através de um sistema de informática.

Compartilha do mesmo entendimento, Vicente Greco Filho, tendo em vista que para ele:

> 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 (...). (GRECO FILHO apud LIMA, 2011, p. 22).

Esta também é a classificação seguida por Crespo (2011, p. 63) porque entende ser a mais objetiva e sujeita de se enquadrar às condutas ilícitas mais atuais é a que adota Ferreira e Greco, assim representada: a) condutas perpetradas contra um sistema informático. b) condutas perpetradas contra outros bens jurídicos.

Seguindo então o que atualmente a doutrina tem utilizado no que concerne à divisão dos crimes cibernéticos, será adotada no presente trabalho a nomenclatura de crimes próprios (contra o computador e dados) e crimes impróprios (cometidos por meio de computadores). No caso dos crimes próprios o presente trabalho explanará apenas sobre a conduta criminosa de invasão de dispositivo informático e as modificações ao Código Penal, trazidas pela Lei 12.737/12.

Crimes próprios

Crimes informáticos próprios são consoante Castro (2003, p. 10), aqueles que para serem realizados necessitam da informática. Sem ela é impossível a execução e consumação da infração. Na verdade, os crimes informáticos próprios nasceram com a evolução desta ciência, são tipos novos, que afetam a informática, onde esta é o bem juridicamente resguardado.

Existem muitas opções de ataques que podem ser realizados contra um computador. Dentre as muitas áreas vulneráveis, há aquelas em que a ação delitiva atua na unidade por onde entram os dados, na saída dos dados eletrônicos, na unidade centralizada onde são processados os dados, num dispositivo de armazenamento ou ainda na transmissão dos dados. (LIMA, 2011, p. 32).

Segundo entendimento de Crespo (2011, p. 57), “não há como negar que, além da informação, os dados, a confiabilidade e segurança dos sistemas e redes informáticas e de comunicação sejam novos paradigmas de bem jurídicos a serem tutelados pelo Direito Penal”.

Impende destacar aqui, que o Brasil possui recente legislação para punir os crimes cibernéticos no País (Leis 12.737/12 e 12.735/12), sancionadas pela Presidente Dilma

Rosselff, dia 30 de novembro de 2012.

Segundo entende o Delegado Higor Jorge, “a aprovação destas leis prevendo especificamente crimes cibernéticos é um avanço para a segurança cibernética do país, pois tipifica condutas indevidas que há muito tempo já deviam ser consideradas criminosas”. (REVISTA DA DEFESA SOCIAL & PORTAL NACIONAL DOS DELEGADOS, 2013).

A respeito da Lei 12.735/12, tem-se que esta entrou no ordenamento jurídico brasileiro para alterar o Código Penal, o Código Penal Militar e a Lei 7.716/89 para tipificar as condutas praticadas por meio do uso de sistema eletrônico, digital ou similares, que sejam praticados contra sistemas informatizados e similares e dá outras providências, trazendo:

> Art. 4º: Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado, e ainda por meio do disciplinado no artigo 5º: O inciso II do 3o do art. 20 da Lei nº 7.716/89, passa a vigorar com a seguinte redação: “art. 20, § 3º: a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio”. (PLANALTO, 2012).

Quanto à Lei 12.737/12, (Lei dos crimes cibernéticos), é interessante mencionar que esta é conhecida como “Lei Carolina Dieckmann”, atriz da Rede Globo, que foi vítima de invasão indevida de imagens suas que estavam contidas em seu computador de uso privado. Episódio este, que ensejou por tornar rápido o andamento de projetos que já tramitavam com o objetivo de regulamentar essas práticas de invasão efetuadas em meios informáticos para tornar moderno o Código Penal Brasileiro. Antes desse fato, era necessário tentar tipificar as condutas nos crimes já existentes, nem sempre com excelência. (CABETTE, 2013).

A Lei 12.737/12 fez incluir os artigos 154-A e 154-B no Código Penal Brasileiro, que versam sobre crimes contra os dispositivos informáticos e alterou os artigos 266 e 298, já constantes do Código, mas que não eram punidos como crimes cibernéticos antes da aprovação desta lei.

Consoante Oliveira (2013), uma vez que consiste em uma novatio legis incriminadora, a nova lei é irretroativa (não será aplicada aos fatos ocorridos antes de sua entrada em vigor), sendo aplicada somente aos fatos posteriores à sua entrada em vigor, isso respeitando a garantia da irretroatividade da lei penal mais grave, conforme

consta no artigo 5º, inciso XL, da Constituição Federal do Brasil.

O artigo 154-A, do art. 2º da Lei 12.737/12 assim dispõe:

> 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.

Impende destacar, que a conduta retromencionada configura a única nova conduta criminosa trazida pela Lei 12.737/12 para o ordenamento jurídico brasileiro, vez que em seus parágrafos, a lei traz apenas situações em que a pena será aumentada, observando certas particularidades no crime. E nos demais artigos além de prevê o período em que esta entraria em vigor, altera dispositivos existentes e fala sobre a ação penal que salvo exceção prevista no artigo 154-B, se procede por meio de representação.

O Delegado Sobral (2013), diz que para evitar criminalização em massa e indevida, a lei é clara quando diz que a invasão deve ter como objetivo do agente o acesso, a alteração, ou destruição dos dados e informações que devam ser zeladas, ou que o sistema esteja protegido, de modo que não esteja vulnerável a que outra pessoa instale nele vulnerabilidades.

Ressalta o Delegado Cabette (2013), que o bem jurídico tutelado neste crime é a liberdade individual, posto que o tipo penal encontra-se inserto no capítulo que trata dos crimes contra a liberdade individual – artigos 146 a 154, do CP, na seção IV que trata dos crimes contra a inviolabilidade dos segredos (artigos 153 a 154- B, CP). Pode-se afirmar que também se tutela neste crime, a privacidade das pessoas, no que concerne a sua intimidade e vida privada, que é bem jurídico protegido no art. 5º, inciso X, da Constituição Federal.

O parágrafo 1º, da Lei 12.737 de 2012 por sua vez assim dispõe: “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*”. (PLANALTO, 2012). Sobre esse dispositivo legal argumenta o Delegado Sobral (2013), que “tal disposição deixa claro que o tipo penal não alcança pesquisadores ou desenvolvedores de software que trabalham na melhoria da segurança dos sistemas, pois vincula a existência de crime ao conhecimento do uso ilegal do produto

produzido ou distribuído”.

Já o parágrafo § 2o da lei em comento, disciplina que a pena terá um aumento de um sexto a um terço se da invasão, resultar um prejuízo econômico. (LEI 12.737/12, 2012). A invasão que este parágrafo se refere, é a mesma trazida pelo artigo 154-A, com a seguinte ressalva, se houver um prejuízo econômico, não será a pena do *caput* do artigo acima citado, mas sim a que o legislador previu no parágrafo.

O entendimento de Cabette (2013), acerca do parágrafo 2º acima citado é que:

> O incremento da lesão patrimonial produz agravamento do desvalor do resultado da conduta, justificando a exacerbação punitiva. O § 2º. é bem claro, de forma que não há se cogitar de aplicação de aumento considerando eventual dano moral. Somente o prejuízo de caráter econômico – financeiro alicerça o aumento.

No que concerne ao § 3º, do artigo 154-A (Lei 12.737/12), vê-se que este prevê, que se da invasão ocasionar na conquista de conteúdo de comunicações eletrônicas particulares, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido, o agente receberá uma pena de reclusão de 6 (seis) meses a 2 (dois) anos, e multa, isso caso a conduta não configure crime mais grave. (LEI 12.737, 2012).

No que se refere ao parágrafo 4º do dispositivo legal em estudo, temos a seguinte previsão: “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”. (LEI 12.737, 2012).

Em conformidade com o parágrafo 5º da Lei em comento, tem-se que este, por sua vez majora a pena de um terço à metade se o crime for cometido contra altas autoridades do poder do País, tais como: o Presidente da República, governadores e prefeitos, o Presidente do Supremo Tribunal Federal, o Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou ainda dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (LEI 12.73712).

Também esta lei, no artigo 3º, inova quando disciplina a alteração do artigo 266, do Código Penal, que agora passa a ter novo nome e passa a prever como crime, a conduta que interromper ou dificultar o restabelecimento do serviço telemático ou da informação. E ainda diz que se o crime acontecer em momento de calamidade

pública, a pena é dobrada. (LEI 12.737/12, art. 3º, §§ 1 e 2º). O nome do crime agora passa a ser “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública”. A inovação é correta e já tardava, vez que os meios de comunicação há muito tempo superaram os simples serviços de telefonia e telegrafia. (CABETTE, 2013).

E por último a lei 12.737 alterou o artigo 298 do Código Penal incluindo o parágrafo único que equipara a documento particular o cartão de crédito ou débito. Para Cabette (2013) trata-se de uma alteração que já estava precisando existir há bastante tempo, pois a utilidade de negociação dos mencionados cartões e o constante uso diário, além do fato de serem estes objeto de falsificação e adulterações, que na falta de norma regulamentando tal conduta referente aos cartões como crime, tornava difícil verificar sobre a natureza ou não do documento.

Não se pode esquecer que apesar da criação dessa lei e do crime de invasão de dispositivo informático, não se pode deixar de mencionar que já existiam algumas leis que disciplinavam os crimes próprios, como é o caso da Lei do Software e outras leis esparsas, porém ainda não havia nenhuma que disciplinasse os atentados contra o dispositivo em si.

Diante disso, pode-se verificar que a nova Lei dos crimes cibernéticos (12.737/12), introduziu uma inovação no ordenamento jurídico, quando prevê a conduta de invasão de dispositivo informático de uma pessoa, burlando o sistema que protege a máquina, sem a devida autorização, como um crime.

Crimes impróprios

São crimes informáticos impróprios consoante Castro (2003, p. 10), “aqueles que podem ser praticados de qualquer forma, inclusive através da informática”.

O uso da internet não é por si só um meio novo de que se valem os criminosos para delinquir, mas é uma ferramenta que associada aos dispositivos informáticos pode ser usada por qualquer pessoa sem habilidades especializadas, que usam esses dispositivos cometendo ilícitos no meio virtual, afetando bens jurídicos comuns, diferentes do mundo informático.

Neste sentido Crespo (2011, p. 94) escreve que há dois tipos de crimes digitais: os próprios e os impróprios. No que tange aos delitos classificados como impróprios, não há grandes diferenças quanto ao *modus operandi*. Em outras palavras, embora o modo pelo qual se realiza a ação criminosa seja outro, não se entrever a necessidade de conhecimentos técnicos específicos.

Ressalta Peck (2002, p. 125) que a maioria dos crimes realizados na rede, também acontecem no mundo real. A internet surge apenas como um facilitador, especificamente por proporcionar que a pessoa não seja identificada.

Inúmeras são as condutas que podem ser efetuadas pelo meio informático, contudo será feita uma explanação apenas de alguns desses crimes, pois que o presente trabalho não visa ampliar o estudo acerca dos crimes impróprios, que são aqueles que são punidos pela legislação comum, constante do Código Penal.

Merecem destaque, os crimes contra a honra, os quais encontram-se previstos nos artigos 138 a 140, do Código Penal, e versam sobre a conduta de caluniar, difamar e injuriar, uma pessoa. Todas essas condutas podem ser cometidas por meio do uso de dispositivos informáticos com a internet.

Um dos crimes bastante comum no meio informático é a pornografia infantil, que nada mais é que a divulgação na rede de transmissão de dados, de fotografias, imagens, figuras que exponham as crianças e menores de idade, ligados a atos obscenos, que motivem o desejo sexual. (LIMA, 2011, p. 34).

Os principais crimes que englobam a pornografia infantil restam previstos no Estatuto, nos artigos 240 e seguintes. O nosso Código Penal, também pune condutas envolvendo relações sexuais com menores, como exemplo o estupro de vulnerável, constante do artigo 217-A. (CRESPO, 2011, p. 90).

Outro crime que pode ser cometido pelo meio informático é o crime de ameaça. Consoante Crespo (2011, p. 88), “é crime intimidar, amedrontar alguém mediante a promessa de causar-lhe mal injusto e grave. A lei brasileira, no art. 147 do Código Penal busca proteger a liberdade da pessoa no que toca a paz de espírito, ao sossego, ao sentimento de segurança”.

No Código Penal existem diversos crimes, que o indivíduo poderia também, em tese, executá-los pelo meio informático, dentre os quais temos: crime de estelionato (art. 171), falsificação de documento público (art. 297), falsidade ideológica (artigo 299), dentre outros. (LIMA, 2011, p. 27-28).

Sujeitos do crime

Faz-se mister estudar os sujeitos dos crimes cibernéticos a fim de que seja possível a compreensão sobre quem são os indivíduos que cometem crimes no âmbito da informática, por abusarem dos bons conhecimentos que possuem na área, e quem são os que sofrem a lesão causadas por esses agentes criminosos do mundo virtual.

Sujeito ativo

Castro (2003, p. 11-12) afirma que, “a princípio qualquer pessoa pode ser sujeito ativo dos crimes de informática. Um estelionato praticado através da Internet, por exemplo, não requer nenhuma qualidade especial do agente. Como este, a maioria dos crimes de informática é comum em relação ao sujeito”. Desta forma, para essa autora verifica-se que o agente não precisa gozar de habilidades particulares para cometer crimes por meio da internet.

De início, é o criminoso de informática uma pessoa que conhece a fragilidade dos sistemas, dos programas de computador e de tudo que circula neste ambiente, devendo ter habilidades de planejar o crime neste ambiente, visualizando as chances que acabam por tornar fácil sua conduta criminosa e sua invisibilidade (anonimato), depois que descobrirem sua conduta. (LIMA, 2011, p. 40).

Apesar de ter quem considere ser o criminoso da informática qualquer pessoa, como é o caso da Doutrinadora Carla Rodrigues Araújo de Castro, citada no primeiro parágrafo, Lima (2011, p. 40) afirma que de todo modo, ainda são os especialistas em informática, são os habilidosos operadores de computadores e sistemas, muitos ainda menores de idade para fins penais, são esses os criminosos eletrônicos. Estes são os delinquentes de rede, que são conforme designado pelos autores como: hackers, crackers, phreaker e carders.

Para Crespo (2011, p. 95):

> *Hacker* é o nome genérico dado aos chamados “piratas” de computador. Essa expressão surgiu nos laboratórios de computação do MIT (Massachusetts Institute of Technology), onde estudantes passavam noites em claro averiguando tudo o que se podia fazer com o computador.

Os *hackers* são pessoas que realizam condutas nem sempre criminosas, eles usam do grande conhecimento dos sistemas, e o utilizam no mais das vezes para invadir esses sistemas, com o intuito de se promover, elevar seu ego. (DOAUN apud COSTA, 2011, p. 119).

Desta forma, da acepção do autor supra pode-se perceber que nem sempre um hacker age com malícia quando invade um sistema, e por isso, não podem ser sempre taxados de criminosos. No entanto, são eles considerados habitualmente como os reais criminosos desta área. É o que diz também Crespo (2011, p. 95):

> Apesar da fama de “criminosos virtuais”, nem todo *hacker* deseja o prejuízo

> alheio. Há aqueles que se dizem "*hackers* do bem", pois invadem os computadores e deixam mensagens informando a vítima do risco existente, aconselhando-a a providenciar uma proteção mais efetiva. Outros passam a trabalhar em empresas a fim de desenvolver programas que sejam capazes de frear as invasões.

Na visão de Lima (2011, p. 41) "são os *hackers*, em regra, invasores dos sistemas eletrônicos que, por espírito de emulação, estariam desafiando seus próprios conhecimentos técnicos e a segurança de sistemas informatizados de grandes companhias e organizações governamentais".

Os *crakers*, por sua vez são considerados os verdadeiros criminosos da rede. Posto que utilizam do diferenciado conhecimento que possuem, para invadir sistemas, destruindo sites, e ainda fazem da internet ferramenta importante para conseguirem roubar valores e informações. (CRESPO, 2011, p. 96).

Com relação aos *phreakers*, são aqueles que agem na área dos telefones. Eles atuam no setor de telecomunicações, fraudando o sistema que opera as ligações, podendo por meio do computador ouvir as conversas de outrem, bem como usar o telefone desta pessoa em proveito próprio, com a realização de ligações gratuitas. Poderá conseguir ligar a partir da invasão aos sistemas de telefonia, confundindo os operadores da linha, sem necessariamente usar a linha particular de alguém. No entanto a fraude é paga por um usuário da operadora de telefonia. (CRESPO, 2011, p. 97).

Os *carders*, são consoante Lima (2011, p. 44) criminosos que roubam o número do cartão de crédito, que conseguem nos sites onde as pessoas donas desses cartões costumam fazer compras pela internet, ou ainda podem conseguir por outros meios ilícitos, com a finalidade de fazer compras pela rede.

Há ainda os *lammers* e os *wannabes*, que segundo Crespo, os primeiros são pessoas sem conhecimento específico da rede, mas pensam ser hackers prontos e capazes de realizar grandes invasões. E os segundos aqueles que tem um pouco de conhecimento, mas ainda não podem agir como um racker. (CRESPO, 2011, p. 97).

Verifica-se então, que segundo todos os autores mencionados, o *hacker*, a quem todo mundo atribui o adjetivo de criminoso da rede, na verdade não o é sempre. Esses, muitas vezes ajudam a desmascarar os *crakers*, intitulados como os verdadeiros delinquentes virtuais. Os *crakers*, usam do grande conhecimento que possuem com o fim de obter vantagem as custas da uma lesão a bem jurídico de outrem, contudo, não são esses os únicos criminosos.

Sujeito passivo

Inicialmente, é fundamental definir que o sujeito passivo ou a vítima dos crimes de computador, são aquelas sobre as quais recai a conduta criminosa omissiva ou comissiva do sujeito ativo, e em relação aos crimes informáticos, podem as vítimas ser indivíduos, instituições de créditos, governos e outras que usem sistemas automatizados de informação, estejam conectados ou não à internet. (LIMA, 2011, p. 36).

Consoante entendimento de Castro (2003, p.12), o sujeito passivo também pode ser qualquer pessoa. Seja quem for conectado à Internet pode receber um vírus e ter destruídos seus programas. Contudo são as empresas as maiores vítimas neste tipo de crime.

A vítima de um crime de computador como a maior parte das pessoas que já sofreram fraudes comuns, muitas vezes é vítima de seu preconceito e de sua própria ignorância no que concerne às máquinas computadorizadas. Geralmente à vítima não percebe na mesma hora que está sendo vítima de um criminoso do setor informático, por não entenderem a tecnologia informatizada e suas funcionalidades. (LIMA, 2011, p. 36).

Quanto às grandes empresas, Lima (2011, p. 37) argumenta que mesmo quando as vítimas são elas, com o intuito de evitar que estas não sejam alvos da publicidade negativa sobre os seus sistemas de segurança, geralmente não há comunicação à polícia, ou nem são providenciadas as iniciativas judiciais. Apesar disso, acredita-se que as instituições financeiras, são as principais vítimas dos crimes cibernéticos.

Segundo Aras (2002, p. 122), “qualquer profissional que pretenda ser bem-sucedido, qualquer empresa ou empreendimento que busque o êxito, deverá estar na rede e cercar-se de conhecimentos e especialistas em diversos campos, a fim de que se tornem visíveis e alcançáveis os horizontes desse mar cibernético”.

Observa-se desta forma, que apesar de existirem no mundo dos crimes cibernéticos seres humanos como vítimas, são as empresas, o governo, bancos e outros setores empresariais os maiores alvos dos criminosos da rede, que são pessoas habilidosas no âmbito da informática.

Competência de modo geral

O instituto da competência para julgar ações penais, no âmbito do Direito brasileiro é atribuído tão somente às pessoas, que imbuídas de poder jurisdicional, devem aplicar aos casos concretos a lei, na medida em que forem competentes para assim agirem.

Nesse mister, pode-se destacar as palavras de Edilson Mougenot Bonfim, que afirma que todo juiz é revestido de poder jurisdicional, por meio da Constituição. Contudo, não são todos os juízes que têm aptidão para julgar todos os conflitos. A extensão do poder jurisdicional que é devida a cada juiz possui limites, consoante alguns critérios que a lei elege, fixando-se, desta maneira, a competência para cada julgador (BONFIM, 2013, p. 267-268).

Assim, ainda que a Constituição atribua a cada juiz o poder jurisdicional, este poder não poderá ser exercido pelos julgadores sempre que assim quiserem, fazendo-se necessário então que sejam observados critérios específicos que a própria lei regula, e que deixa estabelecida a competência devida a cada juiz.

Jurisdição

Antigamente, as pessoas resolviam todas as coisas que lhes desagradavam, uma com as outras dentro da sociedade por meio do exercício de sua própria justiça. É a chamada “autotutela” que fazia parte da vida de muitos, e ainda hoje pode ser observada. A autotutela acontece quando as pessoas agem por conta própria fazendo sua justiça ao invés de pedir ajuda de quem de fato possui prerrogativa para resolver conflitos – o Estado-Juiz.

A vida no meio social gera conflitos que muitas vezes não é possível serem evitados. E na maior parte, esses conflitos são resolvidos pelas próprias partes que litigam, quer por meio de transações, quer por renuncias e outras formas de autocomposição. Acontece que a autotutela está proibida, salvo quando diante da legítima defesa, estado de necessidade, e até prisão em flagrante, e caso uma das partes tenha resistência a pretensão da parte adversa, assim, faz-se necessário que o Estado, por intermédio do processo, solucione este conflitos entre pessoas adversas, atribuindo a cada uma o que lhe cabe, e fazendo com que a paz e a ordem voltem para o meio social. (LIMA, 2013, p. 293).

Consoante Capez (2012, p. 50), a autotutela existe desde o início das primeiras civilizações e se caracteriza pelo uso da força bruta com o intuito de satisfazer

interesses. A própria repressão aos atos criminosos era feita ora em regime de vingança ou de justiça particular, ora pelo Estado, mas sem a oposição de órgãos imparciais.

Acrescenta Tourinho Filho (2012, p. 79), que o Estado uma vez possuidor do poder nas mãos para administrar a justiça, surge também o dever de garanti-la. Assim, se alguém tem seu direito lesionado, estando impedido de fazê-lo ser respeitado por meio da força, poderá recorrer ao Estado-Juiz para restaurá-lo.

Ainda segundo Tourinho Filho (2012, p. 80) temos que a *jurisdição* surge, como uma necessidade do Direito, com o objetivo de impedir que a "autodefesa", cheia de excessos e sem limites, conduzisse a sociedade a uma desordem grandiosa, e ao mesmo tempo, como uma garantia da liberdade perante "a los excesos del autoritarismos sin freno". É verdade, que a autotutela ainda existe, mas de forma rigorosa dentro dos limites que não podem ser evitados.

Desta forma, uma vez que o Estado-Juiz atua em nome da justiça, por meio da figura do juiz, deve este primar por exercer a competência para julgar os litígios que lhes cabem por meio do poder jurisdicional, fazendo reinar a paz e a justiça, de acordo com o Direito, sem favorecer uma parte mais que a outra.

Segundo Capez (2012, p. 252), a palavra jurisdição advém do latim *juris* (direito) e *dictio* (dizer) e quer dizer a função de dizer o direito. Definem a jurisdição Távora; Alencar (2013, p. 239), dizendo que esta "é o poder-dever pertinente ao Estado-Juiz de aplicar o direito ao caso concreto. Como a autotutela foi banida, em regra, do ordenamento, coube ao Poder Judiciário a missão constitucional de certificar o direito, dirimindo as demandas que lhe são apresentadas (...)".

Tourinho Filho (2012, p. 79) por sua vez, afirma que essa função do Estado-Juiz, consistente em fazer imperar a norma, a qual por força do Direito vigente, deve regular determinada situação jurídica, é chamada de jurisdição.

Para Nucci (2013, p. 258) a jurisdição: "é o poder atribuído, constitucionalmente, ao Estado para aplicar a lei ao caso concreto, compondo litígios e resolvendo conflitos".

O Poder Jurisdicional, na hora de aplicar a lei processual penal ao caso concreto, necessita para ser exercido de um terceiro imparcial, capaz de dirimir os conflitos existentes entre as partes, sem influenciar na decisão que deve ser justa, e que muitas vezes nem poderá ser alterada. Neste sentido, Távora; Alencar (2013, p. 240), asseguram que:

> De fato, a concretização do direito exige um órgão supra-partes,

> desinteressado, que atue de forma imperativa e tenha condição de criativamente solucionar o conflito objetivamente apresentado, maximizando a pacificação do litígio, em decisão apta à imutabilidade pela coisa julgada.

A jurisdição possui como características, a inércia, a substitutividade, a lide, a atuação do direito e a imutabilidade.

Nas palavras de Távora; Alencar (2013, p. 246-247), sobre o instituto da inércia tem-se que em regra, os órgãos jurisdicionais, não agem se não forem provocados (*ne procedat judex ex officio*), e esta provocação é feita por meio do uso do instituto da ação. No que concerne a característica da substitutividade, tem-se que uma vez que a autotutela foi banida, incumbe ao Estado, em substituição à vontade das partes, resolver os conflitos.

Quanto à lide, diz Francesco Carnelutti que: "apesar das divergências doutrinárias, é entendimento corredio a pressuposição da lide para o exercício jurisdicional, ou seja, a presença do conflito de interesses qualificado pela pretensão resistida" (CARNELUTT apud TÁVORA; ALENCAR, 2013, p. 246). A definitividade por sua vez, é pregada no intuito de fortalecer os laços da paz social, o exercício da jurisdição, desemboca rumo ao provimento final, chamado sentença, que nesta situação é imutável depois de transitar em julgado, não poderá ser modificado, exceto, no exemplo da revisão criminal pro réu. Já sobre a atuação do direito, diz-se que a atividade jurisdicional tem por fim aplicar o direito ao caso concreto, realizando o restabelecimento da paz social violada em decorrência da infração cometida. (TÁVORA; ALENCAR, 2013, p. 246).

É preciso destacar também alguns princípios que norteiam a jurisdição, e que influenciam no exercício desta por parte do Juiz, que a usa quando é competente para julgar ações.

Conforme Nucci (2013, p. 259) são os seguintes:

> Indeclinabilidade: o juiz não pode abster-se de julgar os casos que lhe forem apresentados; b) improrrogabilidade: as partes, mesmo que entrem em acordo, não podem subtrair ao juízo natural o conhecimento de determinada causa, na esfera criminal; c) indelegabilidade: não pode o juiz transmitir o poder jurisdicional a quem não o possui; d) unidade: a jurisdição é única, pertencente ao Poder Judiciário, diferenciando-se apenas no tocante à sua aplicação e ao grau de especialização, podendo ser civil – federal ou estadual; penal – federal ou estadual; militar – federal ou estadual; eleitoral

ou trabalhista.

Cada princípio acima mencionado possui sua importância e participação não só na atuação do Juiz (Magistrado) que é aquele possuidor de competência aos olhos da Lei para aplicar o direito ao caso concreto, mas também no uso da competência que lhe cabe de acordo com os termos legais acerca do processo, e de seu andamento.

Ressalta Eugênio Pacelli de Oliveira, que a jurisdição penal, de posse do Estado, realiza, portanto, o importante encargo de aplicar o Direito Penal aos fatos que transgridem bens, direitos e valores admitidos pela sociedade, com a medida e proporcionalidade delineadas pela lei de forma prévia. (OLIVEIRA, 2011, p. 203).

Resta claro, então que conforme o aduzido por todos os autores aqui mencionados, a jurisdição é o poder que o Estado, na figura do Juiz exerce por meio da competência que lhe cabe, para aplicar o direito ao caso concreto, sem ultrapassar os limites impostos pela legislação.

Conceito de competência

No tocante à competência, afirma Lucchini, “a competência vem a ser a medida da jurisdição, distribuída entre os vários magistrados, que compõem organicamente o Poder Judiciário do Estado”. (LUCCHINI apud CAPEZ, 2012, p. 254).

Renato Brasileiro de Lima, por sua vez diz que, “compreende-se a competência, por conseguinte, como a medida e o limite da jurisdição por meio dos quais o órgão jurisdicional poderá aplicar o direito objetivo ao caso concreto”. (LIMA, 2013, p. 294). Da mesma forma Capez (2012, p. 254), escreve que, “a competência é, assim, a medida e o limite da jurisdição, dentro dos quais o órgão judicial poderá dizer o direito”.

Entende Tourinho Filho (2012, p. 111), que apesar da jurisdição ser uma só, como poder de soberania que o Estado possui, é evidente que não pode ser exercida por um só juiz sem ter limites. Se a área do Estado fosse escassa e a quantidade de pessoas pequena, da mesma forma como acontece com munícipios pequenos, poderia se entender que um ou dois juízes fossem suficientes para resolver os conflitos que estivessem ali.

Segundo Capez (2012, p. 254) é claro, no entanto, que um juiz apenas não possui condições físicas e materiais de julgar todas as causas, diante do que a lei distribui a jurisdição por vários órgãos do Poder Judiciário. Assim, cada órgão imbuído de jurisdição só poderá aplicar o direito se estiver dentro dos limites que lhe foram dados

nessa distribuição.

Na verdade, seria impossível que somente a um só órgão do Poder Judiciário fosse atribuído o encargo de dar solução a todos os conflitos existentes, onde o número é altíssimo, que surgem num país vasto como o Brasil, por exemplo, que contém uma população de 160 milhões de almas. Disso decorre a criação de vários Órgãos Jurisdicionais, todos realizando aquela função específica de aplicar o direito objetivo frente a uma pretensão. (TOURINHO FILHO, 2012, p. 112).

Vê-se então, que segundo os autores, a competência é repartida para melhor atender as demandas de um grande contingente populacional que existe no país, e apesar da jurisdição ser uma só, a função de exercê-la com a aplicação do direito diante de um caso concreto, é repartida entre os vários órgãos com poder jurisdicional existente.

Soberania e a lei processual penal no espaço

O Estado brasileiro possui como um de seus fundamentos a soberania, isto quer dizer, que o nosso país não é subordinado a qualquer outro, podendo reger suas leis e aplicá-las a todos que nele vivem de forma livre. A soberania é fundamento que rege o país, sedimentado no inciso I, do artigo 1º, da Constituição Federal Brasileira.

No âmbito processual penal brasileiro é importante ser observado se não há qualquer regra de outro Estado tentando ultrapassar os limites impostos pela legislação do Brasil, e desta forma burle a sua soberania. Segundo ensina Bonfim (2013, p. 130) a possibilidade de aplicação da lei processual de um Estado dentro dos limites territoriais de outro, implicaria, de alguma maneira, desrespeito à soberania de um Estado por outro. Logo, as regras que regem o exercício de poder em certo Estado, via de regra, não vigem fora de seus limites territoriais. Tem vigência, na parte específica do direito processual, o princípio da territorialidade.

O princípio da territorialidade no âmbito do processo penal está previsto no Código de Processo Penal, com a disciplina de que o processo penal será regido em todo o território nacional brasileiro, ficando ressalvados por este Código, os tratados, as convenções e regras de direito internacional; as prerrogativas constitucionais do Presidente da República, dos Ministros de Estado, nos crimes conexos com os do Presidente da República, e dos Ministros do Supremo Tribunal Federal, nos crimes de responsabilidade; os processos de competência da Justiça Militar; os processos da competência do tribunal especial; os processos por crimes de imprensa. (CPP, Art. 1º, inciso I a V).

Da redação dada pelo artigo supracitado, pode-se perceber que o Brasil para fins de

Direito Processual Penal, não é subordinado a qualquer regra de direito que não tenha sido por este acordado em tratado ou convenção com outras nações, possuindo assim como regra, liberdade na aplicação de suas leis, no território nacional.

Impende destacar que o princípio da territorialidade existente no âmbito do Direito Penal brasileiro, determina que seja a lei brasileira aplicada, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime que for efetuado dentro do território nacional. (CP, Art. 5º).

Em contrapartida, o princípio da extraterritorialidade também do mesmo diploma legal, em seu art. 7º, pode ser verificado quando ocorrerem crimes que atentem contra a vida ou a liberdade do Presidente da República; o patrimônio ou a fé pública da União, Distrito Federal, Estado, Território, Município, empresa pública, sociedade de economia mista, autarquia ou fundação criada pelo Poder Público; contra a administração pública, por quem esteja a seu serviço e de genocídio, quando for o agente brasileiro ou domiciliado no Brasil. E ainda, quando ocorrerem crimes que, por tratado ou convenção tenha decidido por reprimir, quando praticados por brasileiro, e praticados em aeronaves ou embarcações pertencentes ao Brasil, mercantes ou de propriedade particular quando estiverem em território estrangeiro, e neste não sejam julgados. (CP, Art. 7º, I e II).

Conforme Capez (2012, p. 112) esse princípio compõe-se na aplicação da lei brasileira aos crimes realizados em outros países. A jurisdição é do território, na proporção em que não pode ser exercida no território pertencente a outro Estado, exceto quando houver regra de permissão, por meio do direito internacional costumeiro ou convencional. Respeitando-se o princípio da soberania, não pode um país fazer suas regras serem obrigatórias a outros.

No que concerne ao processo penal entende Nucci (2013, p. 142) que o princípio da territorialidade significa que a todo delito que aconteça no território nacional, deve ser aplicada a lei processual penal, materializada por meio do artigo 1º do Código de Processo Penal, da mesma forma que é usada em Direito Penal (CP, art. 5º). É regra que resguarda a soberania nacional, uma vez que não haveria sentido algum aplicar regras de uso procedimental do estrangeiro para investigar e punir um crime ocorrido dentro do território brasileiro.

No entanto conforme Renato Brasileiro de Lima, enquanto à lei penal são aplicados os princípios da territorialidade e o da extraterritorialidade incondicionada ou condicionada, o Código de Processo Penal adota o princípio da territorialidade ou lex fori. E isso acontece por um motivo claro: a atividade exercida por meio da jurisdição é um dos aspectos da soberania nacional, portanto, não pode ser exercida além das

fronteiras do respectivo Estado. (LIMA, 2013, p. 57).

É importante ressaltar que no que tange às leis processuais penais, o princípio que vigora para sua aplicabilidade no espaço é o da territorialidade absoluta, de modo a se excluir a possível aplicação da lei processual de outro país em nosso território, bem assim, de serem aplicadas as leis processuais daqui fora dos limites compreendidos como território nacional. (BARROS, 2011, p. 108).

Entende Bonfim (2013, p. 131) que pela aplicação do princípio da territorialidade, não ficam excluídos do olhar do Poder Judiciário brasileiro os crimes que aconteceram em outro país. O princípio será aplicado toda vez que o processo penal estiver com andamento processual em território brasileiro, sendo irrelevante se o fato que nele se discute, teve sua execução no todo ou em parte no estrangeiro.

Entretanto consoante Nucci (2013, p. 143), como uma regra de exceção a territorialidade, se acontecer do Brasil firmar tratado, convenção ou faça parte de uma organização mundial, onde as regras internacionais são o seu norte, deve a lei processual penal do território nacional brasileiro ser afastada para que outra, advinda de tais fontes, seja aplicada em seu lugar.

Desta forma, tendo em vista a soberania que o Estado brasileiro possui, cabe a aplicação da lei processual brasileira ao caso concreto que tenha incidência dentro dos limites territoriais internos do país, sendo necessário visualizar as exceções, por exemplo, quando houver norma decorrente de tratado ou convenção a que o Brasil seja parte, onde serão aquelas normas a serem aplicadas. Contudo em regra, aplicar-se-á a lei processual penal brasileira.

Delimitação da competência

Consoante prevê o Código de Processo Penal no artigo 69 e incisos, a competência para julgamento é determinada com base em alguns critérios, quais sejam: o lugar da infração; o domicílio ou residência do réu; a natureza da infração; a distribuição; a conexão ou continência; a prevenção e a prerrogativa de função. (CPP, Art. 69, I a VII).

No decorrer do tempo, a doutrina primou por sistematizar os critérios adotados na lei para repartir as competências entre os órgãos jurisdicionais. As teorias que foram mais aceitas dizem que a fixação da competência é um procedimento lógico de concretização, isto é, pedem um raciocínio que caminha de critérios mais gerais para os mais específicos. (BONFIM, 2013, p. 269).

Nesse diapasão, a doutrina identifica como critérios mais abstratos de fixação da competência dois elementos: as características da lide, que diz respeito a relação jurídica material que forma o objeto do processo e os atos processuais. O primeiro elemento refere-se à competência material e o segundo à competência funcional. (BONFIM, 2013, p. 269).

É preciso fazer constar aqui, todavia, que apesar dos critérios: conexão, continência, prevenção e distribuição, constarem da redação do mencionado artigo e incisos do Código de Processo Penal, como critérios de determinação de competência, eles não serão no presente trabalho explanados com muita ênfase, tendo em vista, serem os dois primeiros institutos complexos, precisando por isso de um estudo próprio sobre eles e os dois últimos por serem de fácil entendimento e simplicidade não há necessidade de aprofundar o estudo sobre estes.

Há ainda que se mencionar a existência de dois tipos de competência, quais sejam: a competência absoluta e relativa. Segundo Lima (2013, p. 301) embora não exista expressa disposição em lei acerca do assunto, doutrina e jurisprudência pensam da mesma forma, e dividem as espécies de competência em absoluta e relativa.

Competência absoluta e relativa

A competência de determinado juiz pode ser fixada de maneira absoluta ou relativa. É chamada de competência absoluta a que não admite ser prorrogada. A competência relativa por sua vez, admite. Será a competência de juízo absoluta ou relativa com base nos critérios que a determine. (BONFIM, 2013, p. 271).

Segundo Nucci (2013, p. 262), a divisão entre competência absoluta e relativa – a primeira sendo improrrogável, enquanto a segunda permitindo a prorrogação – é dada pela doutrina e confirmada pela jurisprudência, ainda que não exista expressa disposição legal sobre o assunto.

Os critérios de competência absoluta ou constitucional são previstos em favor do interesse público. Desta forma, casual desatendimento, não irá implicar em convalidação dos atos que forem realizados no curso do processo. Em contrapartida, a competência relativa atende, principalmente o interesse das partes. Em consequência, se forem violados os ditames da lei para se fixar a competência relativa, se não for arguida tempestivamente, acarretará em preclusão, e em virtude disso a prorrogação da competência, de modo que o juiz que era incompetente passará a ser competente, por vontade das partes. (TÁVORA; ALENCAR, 2013, p. 280).

Acrescente-se ainda, que as competências ratione materiae e ratione personae, e da

mesma forma a funcional, são de competência absoluta. Já, a competência em razão do território (*ratione loci*), será competência relativa. (BONFIM, 2013, p. 271).

Competência material

A doutrina tradicionalmente distribui a competência considerando aspectos diferentes: a) *ratione materiae*: estabelecida em razão da natureza do crime praticado; b) *ratione personae*: de acordo com a qualidade das pessoas incriminadas; c) *ratione loci*: de acordo com o local em que foi praticado ou se deu o resultado do crime, ou local onde reside o autor. Essa classificação está de acordo com a do Código de Processo Penal, onde em seu artigo 69, e incisos, prevê que a competência se determina: a) incisos I e II: pelo local onde aconteceu a infração ou onde o réu possui residência ou domicílio (*ratione loci*); b) inciso III: pela natureza da infração (*ratione materiae*); c) inciso VII: pela prerrogativa de função (*ratione personae*). (CAPEZ, 2012, p. 254-255).

Competência em razão do lugar

A regra disciplinada pelo processo penal, é que a competência será determinada em razão do lugar onde se consumar a infração, ou, na hipótese de tentativa, pelo lugar onde foi realizado o último executório. (CPP, Art. 70, *caput*).

Segundo Nucci (2013, p. 263) se trata de competência territorial, e portanto, relativa, e sujeito à sofrer prorrogação, caso não seja suscitada a tempo.

É importante ressaltar que é considerado como local da infração, aquele onde tiver ocorrido o resultado da prática delitiva. O critério usado aqui é diferente do que é determinado pelo artigo 6º do Código Penal, onde estabelece que o local do crime é aquele no qual ocorreu a ação ou a omissão no todo ou em parte, ou ainda onde se produziu ou deveria ter sido produzido o resultado. A definição trazida pelo artigo 6º do Código Penal não se aplica na hora de determinar o foro competente para julgar, onde esta é regra processual, mas sim à determinação da lei penal (material), é por isso que se diz que a lei processual adotou a teoria do resultado, enquanto a lei material adotou a teoria da ubiquidade. (BONFIM, 2013, p. 287).

Entende ainda o mesmo autor supra, que o legislador tem razões para eleger como foro competente para julgar o lugar onde teve consumação a prática criminosa, conforme explica no texto abaixo:

> A opção do legislador, ao eleger o foro competente o local da consumação do delito, é calcada em dois motivos. O primeiro leva em conta razões de política criminal: para que a repressão penal atinja sua finalidade

> exemplificativa, é mais adequado que o julgamento da causa ocorra no lugar em que houve a violação da norma, em que, via de regra, o delito causa maior repercussão social. É a melhor forma de o Estado demonstrar à população local a prevalência da ordem jurídica vigente. O segundo motivo é de ordem instrumental, pois o lugar da infração é onde mais provavelmente se encontrarão os vestígios e provas do crime. (BONFIM, 2013, p. 288).

No mesmo sentido, Lima (2013, p. 492) entende que a justificativa que se dá para que tramite o processo de acordo com o lugar onde se consumou a infração, é o fato de que deve o agente ser processado e se possível condenado no lugar onde realizou a perturbação da ordem jurídica, e se fizeram sentir os efeitos de sua infração penal, objetivando restabelecer a paz, no meio social que foi afetado. Há também outra justificativa importante, que se funda no sentido de ser mais fácil colher provas onde se consumou o delito.

Argumenta Oliveira (2011, p. 265) por sua vez que:

> ao que se nota, ao legislador do Código de Processo Penal pareceu inoportuna a adoção da teoria da *ubiquidade*, em razão da possibilidade da maior incidência de dupla territorialidade (ou lugar do crime) nas ações penais, o que reclamaria a existência de um critério objetivo para resolver acerca da maior utilidade de um (lugar da ação) ou outro (lugar do resultado) foro.

De todo modo, entende Oliveira (2011, p. 265) contudo, que a questão poderia ser solucionada de outra forma, adotando-se até mesmo a teoria da atividade, pelo lugar da ação, que seria muito mais indicada para atender o que exige a questão de provar. Diz ainda, que a teoria da ubiquidade é superior a que é seguida pelo Código de Processo Penal, e que se revela, a nosso aviso, a mais adequada.

Para Lima (2013, p. 493):

> Enquanto o dispositivo do art. 70 do CPP tem como destinatário os crimes praticados, integralmente, dentro do território brasileiro, o art. 6º do CP funciona como uma regra para a aplicação da norma penal no espaço, ou seja, quando o crime atingir mais de uma nação. Destarte, aplicar-se-á a teoria da ubiquidade ao delito que tenha tido inicio em um país estrangeiro, findando-se em território nacional, ou vice-versa. Preserva-se, assim, a soberania brasileira para processar e julgar o referido delito, desde que uma parte da infração penal tenha tocado o território nacional.

A jurisprudência também por algumas vezes , vem abrandando a teoria do resultado, e tem admitido como uma exceção a competência do local onde se deu a conduta criminosa, quando for necessária para fins de prova. (BONFIM, 2013, p. 288).

A competência determinada em razão do lugar, também gera alguns questionamentos nos chamados crimes à distância ou crimes plurilocais.

No caso dos chamados crimes plurilocais, em que o ato executório do crime começa em um lugar e termina em outro, sendo ambos dentro do território nacional, a regra a ser aplicada é a do art. 70, do CPP. Assim, a competência será determinada pelo lugar onde se consumar a infração, ou se for tentativa, onde for realizado o último ato de execução. Exemplo disso, acontece quando o agente esfaqueia a vítima em Marília e esta morre em São Paulo. O foro competente é São Paulo. (CAPEZ, 2012, p. 276).

Já no tocante aos crimes à distância, em que o crime tem início dentro do território nacional, e termina em um país estrangeiro, explica Bonfim (2013, p. 288) que nestes casos de forma exclusiva o Código de Processo Penal adotou a teoria da ubiquidade. Acrescenta Nucci (2013, p. 264) que com isso fica resguardada a soberania brasileira para levar o agente a julgamento, desde que qualquer parte da infração tenha tido contato com o solo brasileiro, o que se constitui um prestígio ao princípio da territorialidade.

Outro ponto a ser aqui destacado, é no que tange aos crimes de menor potencial ofensivo, onde os criminosos estão sujeitos ao disciplinado pela Lei 9.099/95, adota-se a teoria da atividade, onde consta previsto no artigo 63 desta Lei o seguinte: “A competência do juizado será determinada pelo lugar em que foi praticada a ação penal”. (CAPEZ, 2012, p. 276).

Por todo o exposto, verifica-se que a regra prevista no artigo 70, do Código de Processo Penal, aplica-se a muitos tipos de crimes e situações, encontrando segundo alguns autores certos entraves com a regra do artigo 6º do Código Penal que nada tem a ver com questão do lugar aludido na lei processual penal. Assim, é que prevalece que a competência em razão do lugar deve levar em conta o lugar onde se deu o resultado, como previsto nesta lei processual.

Competência em razão da matéria

A competência poderá ser determinada em razão da natureza da infração, conforme previsto no artigo 69, inciso III, do Código de Processo Penal. Isso acontece, porque conforme Nucci (2013, p. 268) “por vezes, a lei deixa de considerar principal o critério do lugar da infração ou do domicílio do réu para eleger princípio diverso, que

é o da natureza da infração penal. É a competência em razão da matéria (*ratione materiae*)".

Para Oliveira (2011, p. 67) a natureza infração é o segundo critério para se apontar a competência para julgar ações penais:

> Isso porque, nas cidades de maior porte, a jurisdição obedece,a diversas outras repartições, conforme o disposto nas leis de organização judiciária, distribuindo-se a competência criminal por varas especializadas. É o caso, nos grandes centros, de Varas Criminais de Tóxicos, de Crimes de Trânsito etc., que, ao lado dos Juizados Especiais Criminais e do Tribunal do Júri, competentes para o processo e julgamento dos crimes dolosos contra a vida, reclamam a sua competência em razão da natureza da infração penal.

Importante destacar que é esse o critério que a Constituição Federal adota ao determinar que os crimes dolosos contra a vida, devem ser de forma necessária levados a julgamento perante o Tribunal do Júri, (Art. 5º, XXXVIII, d). Ademais, o critério da natureza da infração, também é adotado nas leis de organização Judiciária (art. 74, *caput*, do Código de Processo Penal), cuja elaboração fica por conta dos Estados da Federação. (BONFIM, 2013, p. 269).

Conforme bem ressalta Nucci (2013, p. 268) vários juízes de um lugar poderiam ser competentes, mas poderia existir simulataneidade quando um deles surge como habilitado para julgar do processo, em virtude da natureza da infração. Pode-se citar como exemplo, a existência da Justiça Militar, no momento em que um crime militar, acontecer, o processo já segue direto para essa Vara, sem precisar que fossem feitas outras verificações. Se por acaso, tivesse mais de uma Vara competente na Comarca ou Região, se usa, então o critério geral, qual seja, o lugar da infração ou domicílio do réu.

Essa delimitação é feita pela Constituição Federal, que atribui à Justiça Militar, o processamento e julgamento de crimes militares, consoante artigo 124. Também delimita a competência de julgamento e processamento da Justiça do Trabalho, com base no artigo 114, e incisos, bem como a competência de processamento e julgamento da Justiça Federal, disciplinadas no art. 109, da CF, e incisos. (CF).

Portanto, consoante às palavras de Edilson Mougenot Bonfim, uma vez que tenha sido firmada a jurisdição competente, e determinada a competência territorial, é importante identificar qual o juiz é competente para tomar conhecimento do processo, caso existam no mesmo foro juízes com acúmulo de jurisdição. Um dos critérios para ser resolvida tal questão, é primar pela adoção da competência pela natureza da infração.

(BONFIM, 2013, p. 294).

Vê-se aqui então, que a competência em razão da matéria, é definida pelo próprio texto constitucional e também pelas leis de organização judiciária do Estado/Município, como uma forma de melhor definir as atribuições de julgamento dos órgãos da justiça do país, pois uma vez que se tenha definido a quem compete julgar tal matéria, fica mais fácil encaminhar diretamente um feito ao juízo competente.

Competência em razão da função

A competência pela observação da função exercida por quem será julgado é conhecida como competência em razão da função, ou *ratione funcionae* (*ratione personae*). Para Tourinho Filho (2012, p. 177), esta competência resume-se no poder que é atribuído a certos Órgãos Superiores da Jurisdição de processar e julgar pessoas específicas.

Em virtude da importância das funções que são desempenhadas por determinados agentes, a Constituição Federal, as Constituições dos Estados e as leis infraconstitucionais conferem a estes o direito de serem julgados por Tribunais. É a chamada competência *ratione funcionae* (LIMA, 2013, p. 451).

Nota-se, que a competência por prerrogativa de função se dá não em razão da pessoa que exerce a função, mas como um meio que objetiva proteger a função exercida. E é disso que decorre, a preferência por chamar competência em *ratione funcionae* a ter que dizer em *ratione personae*. (LIMA, 2013, p. 451-452).

Ressalta Tourinho Filho (2012, p. 177) “tal competência é também conhecida pela denominação de competência originária *ratione personae* (ou *ratione mumeris*), vem prevista na Constituição Federal, nas Constituições locais , em leis de Organização Judiciária (é o caso da competência do STM) e no CPP (arts. 84 usque 87)”.

Nas palavras de Tourinho Filho (2012, p. 177), existem pessoas que exercem cargos importantes para o Estado, e é em observância a esses cargos e funções que exercem no cenário político-jurídico de nosso país, que tem essas pessoas direito a foro privilegiado, ou seja, não serão julgadas e nem processadas como qualquer pessoa do povo, pelos órgãos comuns, mas sim por órgãos superiores, de instância superior.

Argumentam Távora; Alencar (2013, p. 275), que o foro privilegiado está derramado principalmente na Constituição Federal ou Constituições estaduais e como estas regras constitucionais foram firmadas em razão do interesse público, predomina o entendimento de que a prerrogativa por foro de função não afronta o princípio do juiz

natural. Todavia, em caso de haver embate entre prerrogativa constante da Constituição do Estado e regra de competência disciplinada pela Constituição Federal, dada a hierarquia entre as regras, a prerrogativa ficará afastada.

Nucci (2013, p. 275) por sua vez discorda com essa posição de que a prerrogativa de foro não afronta o princípio do Juiz natural, quando escreve que a doutrina, de maneira geral dar como uma justificativa para a existência de foro privilegiado, uma forma de dar especial relevo ao cargo ocupado pelo agente e jamais pensando em estabelecer desigualdades entre os cidadãos. Contudo, não estamos convencidos. Se todos são iguais aos olhos da lei, seria necessário uma particular e importante razão para que fosse afastado o criminoso do juiz natural, entendido este como o competente para julgar todos os casos semelhantes ao que foi praticado.

Contudo, a maioria doutrinária entende que não há uma afronta ao princípio da igualdade, sedimentado pela Constituição Federal, no *caput* do art. 5º. Neste sentido explica Tourinho Filho (2012, p. 178) que:

> Não se trata de um privilégio, o que seria odioso, mas de uma garantia, de elementar cautela, para amparar, a um só tempo, o responsável e a justiça, evitando, por exemplo, a subversão da hierarquia, e para cercar o seu processo e julgamento de especiais garantias, protegendo-os contra eventuais pressões que os supostos responsáveis pudessem exercer sobre os órgãos jurisdicionais inferiores.

Neste diapasão, com base no que fora aduzido pelos autores retromencionados, pode-se verificar que a competência determinada em razão do cargo ou função de uma pessoa, o qual possui relevante valor para o cenário político e jurídico do país, não é uma forma de afrontar o princípio do juiz natural, sendo uma forma de evitar que estas pessoas por exercerem importantes funções no país, consigam influenciar os julgadores.

Competência em razão do domicílio ou residência do réu

Algumas vezes quando não for possível aplicar a regra geral constante do artigo 70, do CPP, para a determinação da competência, terá lugar a regra subsidiária da competência com base no domicílio ou residência que o réu possuir.

Essa determinação de competência está prevista no artigo 72, §1º e §2º, do Código de Processo Penal que dispõe:

> Art. 72. Não sendo conhecido o lugar da infração, a competência regular-se-

> á pelo domicílio ou residência do réu.
>
> § 1º Se o réu tiver mais de uma residência, a competência firmar-se-á pela prevenção.
>
> § 2º Se o réu não tiver residência certa ou for ignorado o seu paradeiro, será competente o juiz que primeiro tomar conhecimento do fato.

A regra do domicílio ou residência do réu, é conforme Nucci (2013, p. 266) regra aplicada de forma subsidiária, quando não se sabe ao certo qual o lugar onde a infração se consumou. Por isso é que se chama de foro supletivo ou foro subsidiário.

Segundo Tourinho Filho (2012, p. 157), a hipótese é de difícil ocorrência, uma vez que o desconhecimento do *locus delicti commissi* não é comum. No entanto, como isso é passível de acontecer, o legislador preferiu usar desse foro subordinado: domicílio ou residência do réu.

Importante esclarecer que, segundo os ensinamentos de Lima (2013, p. 506) nos termos do que prevê o artigo 72, § 1º, do CPP, caso o réu possua mais de uma residência, a competência será fixada pela prevenção. Obstante a lei ser silente, prevalece que o mesmo raciocínio será estendido ao réu que possua vários domicílios, ou na hipótese de vários corréus com domicílio e residências diferentes.

Na hipótese prevista pelo § 2º, do artigo 72, do CPP na qual o agente criminoso não possui um local exato como sua residência na qual se configurará a competência pela prevenção. Entende Tourinho Filho (2012, p. 159) que em vez de se aplicar o disposto no § 2º do art. 72, deverá ser invocado o que diz o *caput* do art. 72, isto é, deverá ser processado em seu domicílio, e, nos termos do § 8º do art. 7º da Lei de Introdução, considera-se, nesse caso, domicílio o lugar onde a pessoa se ache.

Explica Capez (2012, p. 290) que será verificada a competência por prevenção toda vez que existir dois ou mais juízes igualmente competentes, sob a ótica de todos os critérios, para o julgamento da lide. Neste caso, a prevenção chega como uma solução para determinar qual o juízo competente. Se trata de uma prefixação da competência, que acontece quando o juiz fica sabendo da prática de uma infração penal antes de qualquer outro que do mesmo modo seja competente, sendo imprescindível que determine alguma medida ou pratique algum ato no processo ou inquérito.

Acrescenta Bonfim (2013, p. 292) que a prevenção tem incidência quando havendo vários juízos igualmente competentes, se tornará prevento o que tenha antecedido aos demais na prática de algum processo ou de medida a este relativa, mesmo que seja anterior ao oferecimento de denúncia ou queixa. A prevenção é disciplinada no artigo

83, do CPP.

Outro ponto a ser aqui demonstrado, diz respeito ao artigo 73, do Código de Processo Penal, na hipótese em for caso de exclusiva ação privada, o querelante poderá optar pelo foro do domicílio ou da residência do réu, ainda quando não conhecido o lugar da infração. Segundo Lima (2013, p. 506) este é o chamado foro de eleição no processo penal, na medida em que o querelante pode escolher pelo foro do domicílio ou da residência do réu, mesmo se for conhecido o lugar onde foi efetuada a infração penal. Pela própria redação do art. 73, do CPP, pode-se compreender que esse dispositivo não se aplica a ação penal privada subsidiária da pública, nem também à ação penal incondicionada ou condicionada.

Disciplina Oliveira (2011, p. 270) que como se vê, a exceção que traz a regra nas ações privadas, tem olhar especial na proteção à vítima e pode ser explicada pela rapidez do tramitar do processo que é exigido nesses tipos de ações penais, onde se espera do autor uma atuação diligente, sob o risco da decadência (art. 38), e em vigiando continuamente o regular andamento da causa, sob pena de perempção (art. 60, I, II e III).

Assim, aqui se observa que a regra do domicílio do réu somente será usada quando não se sabe o lugar onde aconteceu o crime, sendo por isso uma regra subsidiária à regra geral (lugar onde o fato se consumou), ou onde ocorreu o último ato de execução do delito. Por outro lado, se não é sabido onde o agente reside ou é domiciliado realmente, deve-se adotar o critério da prevenção e do mesmo modo quando o réu não possui um lugar certo como residência ou não se saiba o paradeiro deste, será determinada a competência para aquele juiz que primeiro souber do fato criminoso, e tenha feito alguma diligência no processo.

Conexão, continência e distribuição

Neste tópico serão feitas breves considerações acerca dos institutos da conexão, continência e distribuição, que conforme o previsto no art. 69, do Código de Processo Penal são também critérios de determinação de competência.

Importante destacar por oportuno, que na doutrina há quem entenda serem os institutos da conexão e continência formas pelas quais se é possível modificar a competência e não determina-la, como prevê a lei processual penal. É o que assevera Bonfim (2013, p. 296), quando diz que apesar do texto da lei fazer referência à conexão e à continência como causas que determinam a competência, a doutrina as considera critérios de modificação da competência.

Conceituando conexão Capez (2012, p. 286), diz que esta é o vínculo, o nexo que é determinado entre dois ou mais fatos, tornando-lhes entrelaçados por alguma razão, o que pede a sua reunião no mesmo processo, com o objetivo de serem julgados pelo mesmo juiz, em face do mesmo conjunto de provas e com isso sejam evitadas decisões controversas.

O instituto da conexão poderá ser de três tipos: conexão intersubjetiva, conexão objetiva e conexão probatória. Todas estas formas estão previstas nos incisos de I a III, do artigo 76, do Código de Processo Penal, de forma respectiva.

A respeito da continência, temos que esta estará configurada quando, "não é possível a cisão em processos diferentes, porque uma causa está contida na outra". (CAPEZ, 2012, p. 287). A continência poderá ser: por cumulação subjetiva, que é quando duas ou mais pessoas são acusadas pela mesma infração ou ainda por cumulação objetiva, nos casos onde ocorra concurso formal de crimes, consoante previsto no artigo 70, do CP, e também nas hipóteses de erro na execução e resultado diferente do pretendido, ambas previstas nos arts. 73 e 74, do Código Penal. (BONFIM, 2013, p. 298).

No que tange a distribuição, disciplinada no artigo 75 do Código Processual Penal, temos: "a precedência da distribuição fixará a competência quando, na mesma circunscrição judiciária, houver mais de uma um juiz igualmente competente". (CPP, Art. 75). Assim, quando existir mais de um juiz na Comarca, que seja igualmente competente para julgar matéria criminal, sem existir qualquer critério diferenciador em razão da natureza da infração. Será então, por meio de um processo seletivo casual, que se determina pela sorte, é feita a escolha do magistrado. (NUCCI, 2013, p. 291).

É preciso salientar que distribuir, significa repartir, dividir. Assim a distribuição como critério para se determinar a competência, é uma repartição, uma divisão realizada entre juízes que sejam igualmente competentes. Ademais, é de se notar muito facilmente, que a distribuição não é um critério para que seja fixado o foro, mas sim para que seja determinada a Vara. (TOURINHO FILHO, 2012, p. 172).

Entendendo de modo diverso, Renato Brasileiro de Lima afirma que: "consiste a distribuição, portanto, em um critério de fixação de competência entre juízes igualmente competentes pertencentes a uma mesma comarca ou circunscrição judiciária". (LIMA, 2013, p. 528).

Como pôde ser aqui observado pelas ideias trazidas pelos autores supracitados, os institutos da conexão e continência não são vistos como critérios de fixação da competência para julgamento, como traz o texto da lei no artigo 69, do Código de

Processo Penal. E por tal razão, é que não foram no presente trabalho abordados com tanta ênfase, merecendo desta forma um trabalho específico sobre ambos. A distribuição por sua vez, é mais simples de ser entendida, pois nada mais é do que uma forma que se encontrou de repartir os feitos entre os juízes igualmente competentes para julgá-los, para que nenhum deles fique sobrecarregado.

Competência nos crimes cibernéticos

Conforme já demonstrado nos capítulos anteriores, a internet/informática ocasionou o surgimento de crimes cometidos tanto pelo meio virtual que atingem bens jurídicos tradicionalmente já tutelados há bastante tempo no Código Penal, quanto crimes contra bens jurídicos novos (os componentes dos dispositivos informáticos, seus dados e sistema), que possuem legislação recentemente adotada para tutelá-los.

Importante mencionar também, que os criminosos atuantes na área informatizada veem nesta, uma nova forma de delinquir, devido às vulnerabilidades deixadas pelos usuários sem conhecimento, que se utilizam da tecnologia informática para realizar as coisas mais básicas do dia-a-dia sem precisar sair de casa (a exemplo do pagamento de contas), e que do mesmo modo, passam o dia conversando com amigos reais e virtuais por meio de sites de relacionamento, mas normalmente não se preocupam em proteger sua privacidade. E por tais situações é que acabam permitindo aos criminosos, especialistas nesta área informatizada a faceta de cometer crimes na internet ou contra esta.

Não se pode olvidar, que o ambiente virtual permite a observância de “certo anonimato” daquele que visa praticar crimes neste meio, tendo em vista que uma pessoa poderá executar um crime de um computador que esteja num endereço qualquer dentro do território nacional, porém isso por si só não poderá determinar que a pessoa que for encontrada neste lugar é a mesma que usou esse dispositivo para delinquir.

É importante mencionar ainda, que os crimes efetuados pelo meio virtual poderão atingir várias cidades de um mesmo território, e até mesmo chegar a ultrapassar seus limites internos, atingindo outras nações, fato em que necessitam de colaboração de todos os países atingidos pela prática delituosa, para que efetivamente seja possível punir o criminoso.

Os crimes efetuados com o uso da internet e contra os dispositivos informáticos podem ter um alcance a nível mundial, e apesar das leis que hoje disciplinam repressão a esses crimes e da previsão na Lei 12.735/12 para a criação de uma polícia especializada para cooperar com a sanção aos seus agentes, isso ainda não se faz efetiva no Brasil.

Para isso acontecer é preciso investimento do governo, que deve agir com efetividade na aplicação de penalização aos agentes criminosos dos crimes cibernéticos. Conforme noticiado pelo site Agência Câmara Notícias, o delegado Sobral defendeu

que fosse implementada uma estratégia nacional de segurança cibernética que incluísse todos os entes federativos (União, Estados e Munícipios), os poderes Executivo, Legislativo e Judiciário e o terceiro setor, que inclui indústria, academia e sociedade civil. Consoante ele, em outros países, como os Estados Unidos, Inglaterra e Espanha, indústria, agências de investigação, polícia e universidades agem juntos no combate aos crimes virtuais. No Brasil isso não acontece. “Não temos integração das instituições aqui”, disse. (CÂMARA DOS DEPUTADOS, 2013).

É preciso primeiramente entender que ambiente é esse onde se praticam as condutas criminosas referentes a crimes cibernéticos, como este funciona, qual é o lugar do crime, qual o tempo em que este se prolifera e sua duração no espaço, para que após tais considerações seja possível explicar com clareza como se dá a competência para julgar ações penais envolvendo crimes cibernéticos, até mesmo porque todos esses fatores citados anteriormente e que serão a seguir estudados, estão diretamente ligados à competência para julgamento de tais crimes, sem esquecer é claro de verificar até onde vai o poder de punir e julgar do Estado Brasileiro.

Ciberespaço

Os crimes cibernéticos causam prejuízos reais à vida das pessoas ou empresas, porém os criminosos não precisam tocar no território (solo), para efetuar uma conduta criminosa, isso porque o meio onde são realizados tais delitos é um território abstrato (que não se pode tocar), diferentemente dos crimes tradicionais, onde a própria legislação penal traz o conceito de território físico e tudo o que dele faz parte.

Explica Kaminiski (2000, p. 40) o que é ciberespaço tendo como base a definição da Unesco, consoante o texto abaixo:

> Segundo a definição da Unesco, o ciberespaço é um novo ambiente humano e tecnológico de expressão, informação e transações econômicas. Consiste em pessoas de todos os países, de todas as culturas e linguagens, de todas as idades e profissões fornecendo e requisitando informações; uma rede mundial de computadores interconectada pela infraestrutura, de telecomunicações que permite à informação em trânsito ser processada e transmitida digitalmente.

Desta forma, ciberespaço é o território onde acontecem os crimes por meio do uso da rede de internet, é o lugar onde se realizam as condutas criminosas que dão vida aos crimes cibernéticos, onde estes são capazes de ultrapassar os limites territoriais de um país até chegar em outro, ou ainda atingir localidades dentro de um mesmo Estado,

isso porque o meio virtual proporciona essa amplitude da criminalidade.

O termo espaço pode significar a princípio um sentido de finitude, o que não corresponderia ao ciberespaço, tendo em vista que não possui limites geográficos descritíveis. (COLLI, 2010, p. 29-30).

Ressalta Colli (2010, p. 95) que o ciberespaço permite àqueles que estejam inclusos neste ambiente a liberdade de trafegar internacionalmente e o acesso a dados remotos, ficando usuários e máquinas em lugares distintos.

É importante destacar que, o ciberespaço não é uma coisa que sai do poder da jurisdição do mundo real. Usuários de computadores, sistemas provedores, conexões em rede e centrais de dados podem encontrar-se reunidos todos no mesmo país, e assim, pertencerem a uma mesma jurisdição. (CORREA, 2002, p. 72).

O fato de que alguns componentes presentes no ciberespaço, encontrando-se num mesmo país (lugar), poder fazer parte de uma mesma jurisdição, é explicada por Corrêa (2002, p. 72), da seguinte forma:

> A questão reside no fato de a Internet residir em um grande número de jurisdições diferentes. Surgem duas grandes controvérsias: a primeira diz respeito á efetiva responsabilidade de determinado país por determinado crime, e a segunda à competência do poder de polícia para dirimir eventuais problemas.

Argumenta Peck (2002, p. 33), que o problema não reside tão somente no âmbito da internet, mas em toda a sociedade globalizada e convergente, onde diversas vezes não se faz possível se determinar o território em que aconteceram as relações jurídicas, os fatos e os efeitos.

Desta forma, com o surgimento do meio ambiente virtual, surgem questões obscuras no que tange à aplicação da lei penal no tempo e no espaço, isso ocorre por conta de ter no que tange ao território uma definição diferente do trazido pelo Código Penal. Neste sentido são as palavras de Crespo (2011, p. 117) que explica:

> Justamente o surgimento do denominado “mundo virtual” ou “ciberespaço”, apresentando novas concepções de tempo e espaço, gerou empecilhos à correta aplicação da lei penal, vez que a tradicional concepção de território (como espaço físico) ganha outra denotação, qual seja, a de espaço virtual, ambiente onde há transcendência dos limites territoriais físicos.

Assim, não sendo o ciberespaço de fato um território, se caracteriza especificamente

pelo fluxo de informações por intermédio de redes de comunicação. Com isso, o que fica sendo importante é a localização da informação, tendo em vista ser esta a indicadora do território, sendo preciso considerar ainda que, em diversos casos, os crimes realizados nesse "ambiente virtual" tem caráter transnacional, fato esse que vem a exigir dos países maior compromisso para combater esse tipo de criminalidade. (CRESPO, 2011, p. 117).

Desta forma, como se pode observar de tudo o que foi aduzido pelos autores supracitados, o ciberespaço não é um território de fato, mas sim um meio por onde são processadas as informações, os dados que se quer transmitir a outra pessoa que esteja em um lugar diferente daquele de onde estão partindo as informações. É claro que existe um território virtual, e não um território físico, onde seja possível saber com certeza de onde partiu um crime e onde ele se consumou, pois no território virtual, a localização real do criminoso as vezes pode ser bem difícil de ser descoberta.

Lugar e tempo do crime cibernético

É necessário para uma boa interpretação acerca da determinação da competência de julgamento dos crimes cibernéticos, entender primeiramente qual o lugar que se considera para fins jurídicos, como sendo o local onde são cometidos tais crimes, seja por meio da internet/dispositivos ou contra estes, uma vez que os crimes desta seara, são capazes de ultrapassar os limites territoriais internos do nosso país, e ainda faz-se importante verificar qual o tempo de realização desse tipo de crime.

O aumento das redes de computadores, possuindo como grande representante a internet, permitiu que se ultrapassasse os limites fixados pelos critérios da territorialidade e da nacionalidade na prática de certos crimes. (MORENO HERNÁNDES apud COLLI, 2010, p. 95).

Os crimes digitais podem ser realizados de forma parcial em vários países, fazendo com que se divida o *iter criminis*. Questões envolvendo a presença física para o cometimento dos delitos, bem como limites territoriais ganham novas expectativas, de maneira que certas características são mais constantes, como: a velocidade da prática do crime, a distância a partir da qual se realizam os crimes, a quantidade de dados envolvidos, e como consequência, questões envolvendo à prova do processo também ganham ênfase. (CRESPO, 2011, p. 117).

Identificamos, que não obstante esses crimes serem transnacionais, existem mecanismos para que sejam processados. Ademais, é interessante que existam casos

específicos em certos países, que firmam tratados autorizando a perseguição de criminosos ainda que dentro de sua soberania. (CORRÊA, 2002, p. 72).

Conforme já explicado no capítulo anterior, possui o Brasil total soberania sobre seu território, nele podendo aplicar suas leis penais e processuais penais sem precisar de autorização de outro país estrangeiro. Essa soberania é um fundamento previsto pela Lei maior do Estado (Constituição Federal), sendo exercida pela união indissolúvel dos Estados, Distrito Federal e Municípios.

Assim, por meio da Soberania dos Estados, se impõe que sejam aplicadas suas leis em todo o território, que é considerado como: superfície terrestre, espaço aéreo e águas dos territórios. Acontece que o crime em alguns casos, poderá ultrapassar os limites do Estado, fato este bastante comum no que concerne aos crimes cibernéticos, sobretudo, com o uso da internet. (CASTRO, 2003, p. 13).

A aplicação da Lei penal no espaço deve observar, de acordo com a doutrina cinco princípios, quais sejam: princípios da territorialidade, nacionalidade, proteção, da representação e da justiça universal. Tais princípios estão previstos no texto da lei penal, do artigo 5º a 7º, do Código Penal brasileiro.

De forma breve Castro (2003, p. 13) explana sobre cada um desses princípios, conforme abaixo:

> A lei penal no espaço é regida pelos seguintes princípios:
>
> a) Princípio da Territorialidade, através do qual aplica-se a lei do Estado aos fatos ocorridos dentro do território nacional.
>
> b) Princípio da Nacionalidade, a lei do Estado é aplicável aos seus cidadãos onde quer que esteja.
>
> c) Princípio da Defesa, a lei do Estado é aplicável em razão da nacionalidade do bem jurídico tutelado.
>
> d) Princípio da Justiça Penal Universal, a lei do Estado é aplicável a qualquer crime, independentemente da nacionalidade do agente, do bem jurídico lesado e do local do fato.
>
> e) Princípio da Representação, a lei do Estado é aplicável em aeronaves e embarcações privadas, quando realizado o crime no estrangeiro.

Entende Costa (2011, p. 138) que apesar de as condutas efetuadas por meio da

internet não possuírem um território físico certo ou uma nacionalidade que não está conceituada no ciberespaço, é verdade que o agente possui uma personalidade existente de fato, que ultrapassa aquela utilizada no mundo virtual e produz resultados no mundo real.

Argumenta Roberto Chacon de Albuquerque, que olhando de uma forma prática, uma pessoa que vive no Brasil pode alterar dados que estejam guardados na Itália, deslocando-os para a Alemanha, visando obter vantagem ilícita. Do mesmo modo que um vírus pode ser criado por um país e espalhado para milhares de computadores por toda a terra. A transmissão de dados pode incluir vários países, de tal forma que o lugar do crime seja definido de forma quase fortuita. (ALBUQUERQUE apud CRESPO, 2011, p. 117).

Assim, o uso da internet permite sejam estas informações lançadas a qualquer parte do mundo num espaço de tempo recorde, pois com a velocidade que possui a rede de tráfego de dados (internet), qualquer informação chega muito rapidamente ao seu destinatário.

Existem três teorias para explicar a questão do lugar do crime, conforme as palavras de Capez: (2011, p. 122) quais sejam:

1. Teoria da atividade, onde o lugar do crime é o da ação ou omissão, sem ter importância o local onde ocorreu o resultado;
2. Teoria do resultado, onde o lugar do crime é o que se configurou o resultado, sem ter importância o lugar da conduta;
3. Teoria da ubiquidade ou mista, em que o lugar do crime pode ser tanto o local do crime como o do resultado. Será, desta forma, onde se deu qualquer momento do *iter criminis*. Tal teoria é conhecida também por teoria mista. Os simples atos de preparação não configuram objeto de cogitação para determinar o *locus delicti*, posto que não é típico.

A determinação do lugar do crime é essencial para aplicação ou não da lei brasileira e para a determinação da competência. O CP adotou a teoria da ubiquidade para delimitar qual o lugar do crime. (CASTRO, 2003, p. 14).

Destarte, o artigo 6º, do Código Penal dispõe: “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”. (CP, art. 6º). Desta maneira, para que a lei do Brasil seja aplicada é necessário que o crime tenha tocado o território nacional. (HUNGRIA apud CASTRO, 2003, p. 14).

Outra questão importante para o estudo da competência de julgamento dos delitos da área informática, diz respeito ao tempo no ciberespaço, posto que com a utilização da internet toda a informação trafega de um lugar para outro de forma muito célere, entretanto, nem sempre quem julga está atualizado com os avanços da tecnologia.

Assegura Peck (2002, p. 31-32) que primeiramente, toda norma tem um elemento tempo certo, o qual dizemos ser a vigência, ou seja, a duração dos efeitos de uma lei dentro do Ordenamento Jurídico. Todavia, o elemento tempo no Direito Digital, vai além do conceito de vigência e engloba a capacidade do judiciário responder a um determinado fato.

Conforme previsto no Código Penal, o crime tem seu tempo de realização previsto no artigo 4º, que diz: “considera-se praticado o crime no momento da ação ou omissão, ainda que outro seja o momento do resultado”. (CP, Art. 4º). Aplica-se aqui então a teoria da ação ou atividade para a questão do tempo do crime.

Acrescente-se ainda o que escreve Kaminiski (2000, p. 42) sobre como o tempo no âmbito da internet poderá influenciar nas decisões dos magistrados diante de um caso concreto:

> A velocidade da Internet é a principal dificuldade para veteranos magistrados que têm a competência de julgar um caso envolvendo a Internet, argumenta Stuart M. Benjamin(7), professor associado da Faculdade de Direito da Universidade de San Diego, publicado em dezembro na *Texas Law Review*. Benjamin sugere que os julgadores irão se deparar com uma situação difícil, onde os "fatos", como narrados na lide, tornar-se-ão ultrapassados assim que o processo retornar às prateleiras do Cartório.

Todavia, algumas pessoas poderão falar “bem, nós não nos importamos se os fatos mudaram. Nós queremos que o Supremo Tribunal Federal ou o Tribunal de Justiça digam o Direito”. Porém, muitas decisões relevantes, tendo como base dados que já não servem por estarem defasados são um mau serviço para todas as partes. (KAMINISKI, 2000, p. 42).

Necessário se faz então, que o magistrado, as partes e quem tenha interesse em uma lide envolvendo crimes cometidos por meio do ambiente virtual e contra as ferramentas nele existentes, estejam atualizados com o que acontece a todo instante na rede mundial de computadores pelo uso da internet, porque as mudanças das informações no meio virtual muitas vezes poderão ser diárias e constantes, dificultando o julgamento das lides.

Competência territorial para julgar os crimes cibernéticos

Neste tópico será estudada como se dá a competência territorial nos crimes cibernéticos, onde se observará para tal verificação “o lugar de consumação ou o lugar do último ato de execução”, referente a tais crimes dentro do território nacional. Esta verificação será feita com base na doutrina e na jurisprudência, pois a lei em si, não menciona como será feita a fixação da competência para julgar os delitos em comento.

Para isso, é necessário de início, ter em mente que os crimes cibernéticos não causam efeitos apenas no território nacional brasileiro, pois devido ao fato de o meio utilizado para a realização de tais delitos gozar de uma rapidez considerável, poderão tais crimes alcançar também outros territórios, ou seja, poderão afetar outros países.

Consoante Ferreira (2001, p. 212-213):

> A mobilidade dos dados nos sistemas de informática, que facilita largamente que os delitos sejam cometidos à distância, usando-se um computador num determinado país e ocorrendo os resultados em outro, bem como os atentado às redes de telecomunicações internacionais, que atravessam vários países, o uso indevido de programas importados, a necessidade de proteção dos exportados, tudo isso provocou a internacionalização da questão, que deve ser discutida pelos diversos países para a harmonização das normas penais aplicáveis e de outras medidas de caráter extra-penal.

Desta maneira, há a necessidade de o Brasil buscar cooperação internacional para punir tais crimes e para julgá-los, uma vez que devido ao modo como se efetua um crime cibernético e o meio utilizado para a sua consumação, pode fazer com que tal conduta criminosa alcance não somente o território nacional, mas vários lugares do mundo.

Importante destacar, que o Brasil faz parte de alguns tratados e convenções, que permitem a aplicação das regras constantes da lei processual penal às condutas criminosas que tenham tido início no território nacional, ainda que seu resultado tenha se dado em outro país, podendo citar como exemplo a Convenção sobre o crime de racismo e a pornografia infantil.

De acordo com o manual prático de investigação de crimes cibernéticos, no que tange à pornografia infantil, o Decreto Legislativo nº 28, de 24/09/90 e o Decreto

Presidencial nº 99.710, de 21/11/90 incorporaram ao Direito da nação brasileira a Convenção da ONU, sobre o Direito da Criança. E o crime de racismo tipificado pela Lei nº 7.716/89, é prática proibida por força da Convenção sobre a eliminação de todas as maneiras de discriminação racial, que foi confirmada pelo Brasil no ano de 1968 e vigente no território brasileiro a partir da edição do Decreto-Presidencial nº 65.810, datado de 8/12/1969. (MPF/SP, 2006).

Em se tratando de convenções, é importante esclarecer, que o Brasil não é país integrante de uma das convenções mais importantes sobre crimes cibernéticos – Convenção de Budapeste –, convenção esta usada como parâmetro pelos países que a integram no tocante à aplicação das leis penais e processuais penais aos crimes cometidos pela internet ou contra os dispositivos informáticos (crimes cibernéticos próprios).

A Convenção de Budapeste, resultou de um trabalho feito pelo Conselho da Europa, onde estava sendo colocada como prioridade a proteção da sociedade contra a criminalidade no ciberespaço. Sugeria-se que fosse escolhida uma legislação comum que tivesse como objetivo uma maior cooperação entre os Estados da União Europeia, sendo que referida tarefa já estava em desenvolvimento desde a década de 1990. (FERNANDES, 2013, p. 144).

A Convenção de Budapeste, em seu artigo 22, item 1 dispõe sobre a matéria relativa à competência, da seguinte forma:

> 1. Cada parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infracção penal definida em conformidade com os artigos 2º a 11º da presente Convenção, sempre que a infracção seja cometida:
>
> a) No seu território; ou
>
> b) A bordo de um navio arvorando o pavilhão dessa Parte;
>
> c) A bordo de uma aeronave matriculada nessa Parte e segundo suas Leis; ou
>
> d) Por um dos seus cidadãos nacionais, se a infracção for punível criminalmente onde foi cometida ou se a infracção não for da competência territorial de nenhum Estado. (BUDAPESTE, 2001).

Os citados artigos 2º a 11º, da referida Convenção de Budapeste referem-se respectivamente aos crimes de: acesso ilegítimo; interceptação ilegítima; interferência

em dados; interferência em sistemas; uso abusivo de dispositivos; falsidade informática; burla informática; infrações relacionadas com a pornografia infantil; infrações relacionadas com a violação do direito de autor e dos direitos conexos; tentativa e cumplicidade. (BUDAPESTE, 2001).

É notável, que apesar de o Brasil não fazer parte de tal convenção, já legisla em conformidade com o que esta disciplina no tocante aos crimes cibernéticos, no que toca às regras de aplicação da lei do país aos crimes que no território nacional aconteçam, conforme se pode observar na legislação penal brasileira.

Ressalta-se que com a efetivação da Convenção de Budapeste, adotada no ano de 2002 pelo Conselho da Europa, e a abertura da assinatura para todos os países que quiserem, ficou demonstrada a atualidade desta nova modalidade de crime e a necessidade de ser ele combatido por todos que compõe a sociedade a nível mundial, uma vez que não atinge somente a Europa, mas todo o mundo. (FERNANDES, 2013, p. 144).

Consoante entendimento do procurador Marcelo Caiado, é necessário estabelecer um vínculo com outros países, uma vez que por vezes os crimes não são locais. Por isso ele é defensor de que o Brasil assine a Convenção de Budapeste sobre o Cibercrime, cuja aprovação data de 2001. A convenção já foi assinada por 43 países, tendo sido confirmada apenas por 22 destas nações que aderiram – grupo que inclui países da União Europeia (como França, Itália, Portugal e Espanha) e Estados Unidos, Canadá, Japão, África do Sul, Austrália, Chile e Argentina, por exemplo (AGÊNCIA CÂMARA NOTÍCIAS, 2013).

Com base no que foi aqui aludido pelos autores retro, percebe-se muito claramente a importância de o Brasil aderir às convenções ou tratados internacionais, para a aplicação da lei penal e processual penal, quando um crime cometido pelo meio virtual tenha tido incidência no estrangeiro, e por sua vez haja tocado também o território brasileiro.

Doutrina x jurisprudência

É preciso destacar primeiramente, que muitos são os crimes que podem ser cometidos por meio dos dispositivos informáticos e contra estes, entretanto, a legislação processual penal não traz expressamente nada relativo à competência para julgar tais delitos. Assim, é que não será estudada a aplicação da lei processual penal perante todos os crimes cibernéticos, mas tão somente diante dos mais balizados pela doutrina e jurisprudência, conhecidos por crimes cibernéticos impróprios.

A competência para julgar ações penais no âmbito da informática deve observar qual o território e a jurisdição sobre a qual o crime se encontra. Segundo entendimento de Celso Valin, o maior problema está no fato de ter a rede caráter internacional. Na internet não há fronteiras, desta forma, uma coisa que esteja publicada nela, estará do mesmo modo em todo o mundo. Como, então, determinar o juízo competente para estudar um caso referente a um crime ocorrido na rede? (VALIN apud ARAS, 2001).

Como bem determina o artigo 70, do Código de Processo Penal, a regra para determinação da competência é feita em razão do lugar onde a conduta criminosa se consumou, ou em se tratando de tentativa, no lugar em que for praticado o último ato de execução. Acrescentam Távora; Alencar (2013, p. 262) que esta disposição deve ser completada pelo disposto no inciso I, do artigo 14, do Código Penal, que entende consumado o crime quando estão reunidos todos os elementos de sua definição legal.

A regra que aparenta ser simples, se torna complexa intervindo, tanto a doutrina quanto a jurisprudência para resolver tal problema. (TOURINHO FILHO, 2012, p. 133).

Levando em conta que o crime cibernético é realizado num meio, em que o alcance da conduta criminosa não será apenas de ordem local, mas algumas vezes internacional, se faz necessário estudar tais crimes, observando se seus efeitos tem incidência somente no território nacional, ainda que em lugares diferentes (crime plurilocal) ou se o alcance foi aquém dos limites do nosso país, alcançando outras nações, situação em que estaremos diante de um crime à distância.

Segundo Lima (2013, p. 496) crimes plurilocais são aqueles onde a infração penal tem a ação e o resultado ocorrendo em lugares diferentes, contudo ambos acontecem dentro do território nacional. Já os crimes à distância são as infrações penais onde sua ação ou omissão acontecem dentro do território brasileiro, porém, o seu resultado se materializa no estrangeiro, ou vice-versa.

Importa ressaltar aqui, que nos crimes plurilocais onde a conduta tenha sido efetuada em mais de um local, será considerado o local dos últimos atos executórios para a definição da competência sob a égide de crime na forma tentada. (OLIVEIRA, 2011, p. 267).

No tópico lugar do crime, foi visto que para o Direito Penal a teoria adotada, é a da ubiquidade para aplicação da lei penal (CP, art. 6º); já para o Direito Processual Penal, segue-se a teoria do resultado, onde a lei processual penal será aplicada quando o lugar de consumação ou último ato executório do crime tenha sido no território nacional, de acordo com o artigo 70, do CPP. Assim, não se pode invocar a regra do

artigo 6º, do Código Penal, quando o assunto é competência em razão do lugar para julgar os processos envolvendo crimes.

Neste sentido Tourinho Filho (2012, p. 147) explica que:

> Nem se pode, nem se deve invocar a regra do artigo 6º do CP, segundo a qual" 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", porquanto essa norma diz respeito, apenas e tão somente, às hipóteses em que se deve aplicar a lei brasileira, tendo em vista o ordenamento jurídico de outros Estados soberanos.

Assim, para que seja determinada a competência em razão do lugar em consonância com o previsto pela lei processual penal brasileira no tocante aos crimes cibernéticos, é necessário saber antes de qualquer coisa saber se o lugar onde se deu o resultado ou teve o ultimo ato de execução do crime (tentativa) faz parte da composição do território nacional brasileiro.

Segundo Tourinho Filho (2012, p. 133) é, pois no foro (território) onde a infração se deu por satisfeita que o culpado deve ser jugado e processado. "É aí, como dizia Garraud, que se fazem sentir os efeitos de sua atividade ou inação criminosa e onde cumpre tranquilizar os interesses alarmados".

Conforme Castro (2003, p. 107) se o Brasil for competente, deve ser aplicada a regra que estabelece o CPP, onde para qual a competência é, de regra, determinada com base no lugar onde o crime se consumou, ou se for tentativa, pelo lugar onde foram realizados os últimos atos de execução do crime. (art. 70). Daí é que surge a importância de se identificar o local onde se consumou o delito, tarefa esta muitas vezes difícil nos crimes de informática.

Sendo assim, quando for possível localizar a máquina utilizada pelo agente criminoso na execução do crime, estará resolvida a questão da competência. Tem-se como exemplo: Roberta construiu uma homepage no laboratório de informática da Universidade Veiga de Almeida, Rio de Janeiro, e inseriu mensagem discriminatória contra um determinado grupo de religiosos. Competente para o processo e julgamento será a comarca do Rio de Janeiro. (CASTRO. 2003, p. 107).

É preciso salientar, que quando não se conhecer o lugar da consumação, a regra que deve ser aplicada é a regra secundária para se fixar a competência: o domicílio ou residência do réu, conforme art. 72, CPP. No caso em que o réu possua mais de um lugar de residência, a competência se firmará pela prevenção (art. 72, § 1º, CPP) e, se

o réu não tiver lugar certo onde resida ou não se conhecer o lugar onde se encontre, será competente o primeiro magistrado que conhecer do fato (art. 72, §, 2º, CPP). (CASTRO, 2003, p. 107-108).

De acordo com o que fora aduzido pela autora supra, a regra geral de determinação da competência prevista no artigo 70, do CPP estará afastada quando ocorrer uma das situações aludidas no parágrafo anterior, operando-se então a fixação da competência pela regra do domicílio do réu, prevenção ou pelo juiz que primeiro tomar conhecimento da conduta.

Importante acrescentar ainda, que a prevenção determinará a competência também nos seguintes casos:

> a) Quando incerto o limite entre duas comarcas, se a infração for praticada na divisa, a competência será firmada pela prevenção (art. 70, § 3º).
>
> b) No caso de crime continuado ou permanente, praticado em território de duas ou mais jurisdições, a competência será também firmada pela prevenção (art. 71). (CAPEZ, 2012, p. 277).

Ressalta Tourinho Filho (2012, p. 160) que são desnecessárias repetir que tais regras somente serão invocadas quando não for conhecido o locus delicti, isto é, se não for possível de forma alguma determinar o espaço geográfico (comarca, município ou distrito) onde foi cometida a infração.

A teoria do resultado ganha importância nos crimes plurilocais, que são aqueles em que os atos executórios acontecem em local diverso do resultado, mas sempre dentro do território nacional. Cita como exemplo, uma carta com injuria que é escrita em Teresina e enviada a João Pessoa, onde a vítima vive. Nesta situação, a competência relativa ao território, será dada à João Pessoa, lugar onde veio a consumar a infração. (TÁVORA; ALENCAR, 2013, p. 262).

No que tange aos crimes à distância explica Capez (2012, p. 277) que no caso de um crime ser efetuado em território nacional e o resultado ocorrer em outro país aplica-se a teoria da ubiquidade, prevista no artigo 6º do Código Penal; o foro competente para julgar a ação será tanto o do lugar onde foi efetuada a ação ou omissão quanto o lugar onde se produziu o resultado. Desta forma, o foro competente será o do lugar onde foi praticado o último ato de execução no Brasil (art. 70, §1º,), ou o lugar no estrangeiro onde se produziu o resultado. Exemplo: o agente escreve uma carta injuriosa em São Paulo e a envia para a vítima, que lê a carta que ofende a sua honra em Buenos Aires. O foro competente será tanto o de São Paulo, quanto o de Buenos Aires.

Desta forma, quando diante de crimes onde haja conjugação de ações e resultados em diferentes países, a teoria da ubiquidade mostra-se a mais correta no que concerne à aplicabilidade da lei penal no espaço, tendo em vista que há mais possibilidade de serem evitados conflitos negativos de jurisdição e de serem resolvidos os problemas dos crimes á distância, onde tanto a ação quanto o resultado ocorrem em lugares diferentes. (BACIGALUPO apud COLLI, 2010, p. 99).

Explicada a situação em que a regra imposta pelo artigo 70, do CPP deverá incidir no que tange aos crimes cibernéticos e quando esta deverá ser afastada para que seja feita a determinação da competência pelas demais regras (art. 72, CPP), faz-se necessário saber agora quem é o juízo competente para realizar tal julgamento nessas localidades inerentes ao território nacional. Para isso, é preciso agora analisar a matéria a ser julgada, para saber qual será o órgão competente.

A Constituição Federal, no artigo 109, inciso IV elenca a competência da Justiça Federal para o processo e julgamento de crimes:

> Art. 109. Aos juízes federais compete processar e julgar:
>
> IV – 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 e ressalvada a competência da Justiça Militar e da Justiça Eleitoral.
>
> V – os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente. (CF, art. 109, IV e V).

O Manual prático de investigação de crimes cibernéticos do MPF/SP, nos termos do artigo 109, IV, da Constituição Federal, diz que compete aos juízes federais processar e julgar os crimes que sejam cometidos em prejuízo de bens, serviços ou interesses da União, suas entidades autárquicas ou empresas públicas. Desta forma, é competência da Justiça Federal julgar os crimes eletrônicos que sejam realizados contra os entes da Administração Federal indicados nesse inciso. Pode ser mencionado como um exemplo o contrato eletrônico, o dano ou a falsificação de dados que se encontrem em sistemas informatizados mantidos por órgão ou entes da administração pública federal. (MPF/SP, 2006).

No que concerne à previsão do inciso V, do artigo 109, da Constituição, vale lembrar que as condutas típicas previstas no artigo 241, do Estatuto da Criança e do Adolescente e também o crime de racismo (tipificado na Lei 7.716/89) possuem

previsão em convenções internacionais de direitos humanos. Como a consumação do crime geralmente ultrapassa os limites do território nacional quando dois crimes são praticados por meio da Internet, a competência para julgar tais crimes cabe à Justiça Federal. (MPF/SP, 2006).

Assim, para que se atraia a competência da Justiça Federal, é imprescindível que a prática criminosa prevista em tratado ou convenção internacional exceda a simples repercussão interna, e atinja patamares internacionais (BONFIM, 2013, p. 282).

Ressalte-se ainda, que de acordo com esse manual prático de investigação dos crimes cibernéticos do MPF/SP, outros crimes que não sejam abrangidos pelas hipóteses acima citadas – a exemplo dos crimes contra a honra de pessoa privada, praticados por meio da rede – deverão ser investigados e também processados na seara das Justiças Estaduais, uma vez que o simples fato de ter sido o crime efetuado pela internet por si só não é capaz de justificar a competência da Justiça Federal. (MPF/SP, 2006).

Neste sentido a Jurisprudência do Superior Tribunal de Justiça já decidiu um conflito de competência em que havia ausência das hipóteses que a Constituição prevê, nos incisos IV e V, conforme se pode observar no julgado abaixo:

> CONFLITO NEGATIVO DE COMPETÊNCIA. CRIME DE INJÚRIA PRATICADO POR MEIO DA INTERNET, NAS REDES SOCIAIS DENOMINADAS ORKUT E TWITTER. AUSÊNCIA DAS HIPÓTESES DO ART. 109, INCISOS IV E V, DA CF. OFENSAS DE CARÁTER EXCLUSIVAMENTE PESSOAL. COMPETÊNCIA DA JUSTIÇA ESTADUAL.
>
> 1 - O simples fato de o suposto delito ter sido cometido por meio da rede mundial de computadores, ainda que em páginas eletrônicas internacionais, tais como as redes sociais "Orkut" e "Twitter", não atrai, por si só, a competência da Justiça Federal.
>
> 2 - É preciso que o crime ofenda a bens, serviços ou interesses da União ou esteja previsto em tratado ou convenção internacional em que o Brasil se comprometeu a combater, como por exemplo, mensagens que veiculassem pornografia infantil, racismo, xenofobia, dentre outros, conforme preceitua o art. 109, incisos IV e V, da
>
> Constituição Federal.
>
> 3 - Verificando-se que as ofensas possuem caráter exclusivamente pessoal,

> as quais foram praticadas pela ex-namorada da vítima, não se subsumindo, portanto, a ação delituosa a nenhuma das hipóteses do dispositivo constitucional, a competência para processar e julgar o feito será da Justiça Estadual.
>
> 4 - Conflito conhecido para declarar a competência do Juízo de Direito do Juizado Especial Cível e Criminal de São Cristóvão/SE, o suscitado. (CC, 121431/SE, Rel. Ministro MARCO AURÉLIO BELLIZZE), TERCEIRA SEÇÃO, julgado em 11/04/2012, DJe 07/05/2012).

E quando há conflito de competência territorial? Já foi dito, que um crime cibernético pode ter efeitos tanto nos limites territoriais do Brasil quanto em outros países. Ocorre que nesses casos, poderá ser indagada a existência de um conflito de competência para o processo e julgamento de tais crimes.

Acerca de tal conflito de competência envolvendo crimes cibernéticos explica Colli (2010, p. 102-103) que:

> Apesar da teoria da ubiquidade resolver o problema quanto à definição do *lucus comissi delicti* – considerando como lugar do crime tanto o de sua ação ou omissão como o de seu resultado – , em um eventual conflito de competência referente a um cibercrime, a questão deve ser analisada com maior atenção. E isto se deve ao fato de que em uma infração penal desta natureza podem existir diversos critérios a orientar o local onde, de fato, houve a consumação.
>
> Dentre estes critérios pode-se citar: a) local onde se encontrava o sujeito ativo do crime (quem, por exemplo, publica um vídeo de pornografia infantil na rede); b) local onde se encontrava o sujeito passivo do crime (quem visualiza aquele vídeo); c) o local do servidor que armazena o vídeo (tendo em vista que é ali que estão os dados acessados); d) ou ainda, não há como se estabelecer onde ocorreu a infração, pois ocorrida em ambiente que não possui locus definido (intangibilidade online). (COLLI, 2010, p. 102-103).

Segundo Capez (2012, p. 283) a análise da competência territorial no que concerne a conduta de divulgação de imagens de menores por meio da rede de computadores (internet), a exemplo da pedofilia, é pela jurisprudência do STJ, determinada em favor da Justiça Federal, conforme abaixo:

> Crime praticado por meio da rede mundial de computadores (internet): No

> caso do crime de pedofilia, já decidiu o STJ pela competência da Justiça Federal: “1 — A consumação do ilícito previsto no art. 241 do Estatuto da Criança e do Adolescente ocorre no ato de publicação das imagens pedófilo pornográficas, sendo indiferente a localização do provedor de acesso à rede mundial de computadores onde tais imagens encontram-se armazenadas, ou a sua efetiva visualização pelos usuários. 2 — Conflito conhecido para declarar competente o Juízo da Vara Federal Criminal da Seção Judiciária de Santa Catarina” (STJ, 3ª Sec., CC 29.886/SP, rel. Min. Maria Thereza de Assis Moura, j. 12-12-2007, DJ, 1º fev. 2008, p. 1).

Pela ementa deste julgado trazido pelo autor Fernando Capez, verifica-se que o Superior Tribunal de Justiça decidiu a competência territorial para a matéria relacionada à pornografia infantil, entendendo que a consumação da conduta de divulgação de “imagens pedófilo pornográficas”, se dá no momento em que estas são lançadas na rede. Assim, o local competente será aquele de onde partiu a conduta.

Não obstante a visível liberdade trazida pela teoria da ubiquidade – pois permite que se atribua o locus comissi delicti tanto ao lugar onde ocorreu a ação quanto ao lugar do resultado do crime – há que se levar em consideração que os Tribunais Superiores conforme se demonstrará a seguir tem mitigado a aplicação desta teoria quando se tratar de crimes cibernéticos. (COLLI, 2010, p. 103).

> 1) Pornografia Infantil pelas redes sociais
>
> PROCESSUAL PENAL. CONFLITO DE COMPETÊNCIA. PUBLICAÇÃO DE PORNOGRAFIA ENVOLVENDO CRIANÇA OU ADOLESCENTE ATRAVÉS DA REDE MUNDIAL DE COMPUTADORES - ORKUT. ART. 241 DO ECA. PECULIARIDADES DO CASO CONCRETO. DÚVIDAS QUANTO AO LOCAL DE ONDE EMANARAM AS IMAGENS PEDÓFILO-PORNOGRÁFICAS. ART. 72, § 2º, DO CPP. COMPETÊNCIA FIRMADA PELA PREVENÇÃO EM FAVOR DO JUÍZO ONDE AS INVESTIGAÇÕES TIVERAM INÍCIO.
>
> 1. No caso, não há divergências acerca da transnacionalidade necessária à determinação da competência da Justiça Federal, já que se trata de site de relacionamento internacional - OrKut – que possibilita a qualquer pessoa dele integrante o acesso dos dados constantes da página em qualquer local do mundo.
>
> 2. Não se olvida que a jurisprudência desta Corte posicionou-se no sentido de que o delito capitulado no art. 241, da Lei n. 8.069/1990 se consuma com

o ato de publicação das imagens. Contudo, ao que se tem, na hipótese, configurada dúvida quanto ao local do cometimento da infração, pois não foi possível apurar de onde se partiu (local) a publicação das imagens e tampouco o responsável pela divulgação das fotos contendo pornografia infantil.

3. Ante a regra contida no § 2º do art. 72 do Código de Processo Penal, firmar-se-á a competência, no caso, pela prevenção, em favor do Juízo Federal de São Paulo onde as investigações tiveram início.

4. Conflito conhecido para declarar a competência do Juízo Federal da 8ª Vara Criminal da Seção Judiciária de São Paulo - SP, o suscitado. (CC, 130134/TO, Rel. Ministra MARYLZA MAYNARD (DESEMBARGADORA CONVOCADA TJ/SE), TERCEIRA SEÇÃO, julgado em 09/10/2013, DJe 21/11/2013).

2) Furto mediante fraude.

CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSO PENAL.

FRAUDE ELETRÔNICA NA INTERNET. TRANSFERÊNCIA DE VALORES DE CONTA-CORRENTE DA CAIXA ECONÔMICA FEDERAL. CRIME DE FURTO MEDIANTE FRAUDE.

1. O delito de furto mediante fraude, previsto no art. 155, § 4º, inciso II, do CP, consistente na subtração de valores de conta-corrente mediante fraude utilizada para ludibriar o sistema informatizado de proteção de valores mantidos sob guarda bancária, deve ser processado perante o Juízo do local da conta fraudada. Precedentes.

(...)

(CC 119.914/DF, Rel. Ministra ALDERITA RAMOS DE OLIVEIRA (DESEMBARGADORA CONVOCADA DO TJ/PE), TERCEIRA SEÇÃO, julgado em 12/12/2012, DJe 01/02/2013).

3) Crime contra a honra.

CONFLITO NEGATIVO DE COMPETÊNCIA. CRIME CONTRA A HONRA. CALÚNIA.

OFENSAS PUBLICADAS EM BLOG NA INTERNET. COMPETÊNCIA DO LOCAL ONDE ESTÁ SEDIADO O SERVIDOR QUE HOSPEDA O BLOG.

1. O art. 6º do Código Penal dispõe que o local do crime é aquele em que se realizou

qualquer dos atos que compõem o iter criminis. Nos delitos virtuais, tais atos podem

ser praticados em vários locais.

2.Nesse aspecto, esta Corte Superior de Justiça já se pronunciou no sentido de que a

competência territorial se firma pelo local em que se localize o provedor do site onde se hospeda o blog, no qual foi publicado o texto calunioso.

3. Na hipótese, tratando-se de queixa-crime que imputa prática do crime de calúnia,

decorrente de divulgação de carta em blog, na internet, o foro para processamento e

julgamento da ação é o do lugar do ato delituoso, ou seja, de onde partiu a publicação do texto tido por calunioso. Como o blog denominado Tribuna Livre do Juca está hospedado na empresa NetRevenda (netrevenda.com), sediada em São Paulo, é do Juízo Paulista, ora suscitante, a competência para o feito em questão.

4. Conflito conhecido para declarar competente o Juízo de Direito da Vara do Juizado Especial Criminal do Foro Central da Barra Funda - São Paulo/SP, o suscitante.

(CC 125.125/SP, Rel. Ministra ALDERITA RAMOS DE OLIVEIRA (DESEMBARGADORA CONVOCADA DO TJ/PE), TERCEIRA SEÇÃO, julgado em 28/11/2012, DJe 12/12/2012).

4) Fórum de mensagens.

CONFLITO DE COMPETÊNCIA. PROCESSUAL PENAL. RACISMO PRATICADO ATRAVÉS DE PUBLICAÇÃO DE MENSAGENS

RACISTAS EM SÍTIO DE RELACIONAMENTO. INTERNET.

IDENTIFICAÇÃO DOS AUTORES. NECESSIDADE. LOCAL DO CRIME. LUGAR DE ONDE FORAM ENVIADOS OS TEXTOS OFENSIVOS. AUSÊNCIA DE DADOS APTOS A PROVAR A ORIGEM DAS OFENSAS. CONTINUIDADE DO PROCEDIMENTO INVESTIGATÓRIO.

PREVENÇÃO. COMPETÊNCIA DAQUELE JUÍZO QUE PRIMEIRO CONHECEU DA INVESTIGAÇÃO.

1. A competência para processar e julgar os crimes praticados pela internet, dentre os quais se incluem aqueles provenientes de publicação de textos de cunho racista em sites de relacionamento, é do local de onde são enviadas as mensagens discriminatórias.

2. Na espécie, mesmo após recebidas as informações da empresa proprietária do sítio, não houve como identificar, por enquanto, os autores das ofensas, o que impõe, obviamente, a manutenção do feito no âmbito daquele juízo que primeiro tomou conhecimento da investigação.

3. Conflito conhecido para declarar a competência do JUÍZO FEDERAL DA 4A VARA CRIMINAL DA SEÇÃO JUDICIÁRIA DO ESTADO DO RIO DE JANEIRO, o suscitado.

(CC 107.938/RS, Rel. Ministro JORGE MUSSI, TERCEIRA SEÇÃO, julgado em 27/10/2010, DJE 08/11/2010).

Importante trazer aqui as palavras de Oliveira (2011, p. 266-267) o qual entende que felizmente, a jurisprudência vem abrandando, de forma excepcional, o rigor da teoria do resultado, para permitir a competência do juízo onde foi praticada a ação delituosa, ainda que tenha sido outro o lugar da consumação, frente à necessidade de se preservar o máximo possível o conjunto de provas disponível.

Com base no aqui aludido, fica claro que a Jurisprudência sedimentada no Brasil no que concerne aos crimes cometidos por intermédio da internet/dispositivos informáticos, usa da teoria da ubiquidade, mas não para descobrir e determinar o lugar do crime para aplicação da lei penal, como disciplina o artigo 6º, do CP, e sim como uma forma de fazer com que sejam preservadas as provas que surgem dessas incidências criminosas, decidindo algumas vezes pelo local em que se encontre o provedor de acesso, noutro pelo local onde se satisfez o crime, e também pelo critério da prevenção.

Considerações finais

O presente trabalho monográfico buscou estudar institutos presentes na legislação penal, sob a ótica da doutrina e jurisprudência no que concerne aos crimes cometidos por meio da internet/dispositivos informáticos ou contra esta, visando entender se a regra geral prevista na legislação processual penal, que prima pela teoria do resultado, onde o lugar é a regra na determinação da competência para o processo e julgamento dos crimes tradicionais, poderia também ser aplicada aos crimes cibernéticos.

Conforme visto no decorrer deste trabalho, a internet surgiu na sociedade munida de muitos benefícios para a vida em sociedade, influenciando principalmente na comunicação entre as pessoas, na realização de questões profissionais e educacionais online, na resolução de coisas simples do cotidiano de cada pessoa como: pagar contas, realizar inscrições de concursos e outros, sem precisar que estas saiam de seus lares. No entanto, com a internet surgiram também muitos problemas que acabaram por afetar diretamente a vida dessas pessoas, e também das empresas, fazendo-se necessário que o poder judiciário tivesse um olhar mais preciso frente a tais conflitos envolvendo a rede de tráfego de dados, objetivando resolvê-los.

Importante deixar claro, que a internet e os equipamentos tecnológicos que desta se utilizam para a efetiva comunicação pessoas/mundo, a exemplo do computador, surgiram em épocas diferentes. A primeira por volta dos anos de 1960, por ocasião da guerra fria, quando pensando em proteger-se de um ataque nuclear, os EUA, decidiu criar uma rede por onde fosse possível a comunicação entre vários lugares do mundo e o segundo, nos anos 80, tendo vindo com este os crimes cometidos por meio do seu mau uso ou uso inadequado.

O uso do computador por meio da internet permite às pessoas uma constante interação no meio social, principalmente pelo acesso as redes sociais, como facebook, twiter, whatsapp, porém com o encantamento que as pessoas veem nestes sites de relacionamento, acabam por não se preocuparem em proteger sua vida pessoal, seus dados, que são colocados à disposição de quem quiser ver na rede, ocasionando assim uma grande quantidade de infrações criminosas.

Desta forma, necessário se fazia criar leis capazes de deixar o cidadão que vive no meio social e que usa o meio virtual, protegido do olhar criminoso daqueles que por possuírem um avançado conhecimento da rede e suas nuances, conseguem cometer infrações, e muitas vezes nem ser percebido pelas autoridades da justiça.

O Estado brasileiro já vinha punindo os crimes praticados pelo meio virtual de forma

análoga aos crimes tradicionalmente previstos no Código Penal, tendo em vista que o uso da informática para cometer crimes é visto pelos criminosos apenas como mais um meio apto a realizar os crimes que neste código já são disciplinados. Tais crimes cometidos por meio do uso da tecnologia informática são definidos pela maioria doutrinária como crimes cibernéticos impróprios, pois a informática nestes é apenas uma nova ferramenta capaz de atingir bens jurídicos tradicionalmente tutelados.

Além dos crimes cibernéticos impróprios, há também os crimes que afetam a própria máquina informática e seus dados, sistemas e equipamentos próprios desta tecnologia, os quais são chamados pela maioria doutrinária como crimes cibernéticos próprios, uma vez que neste tipo de crime o bem jurídico afetado é a própria informática/informação. Tais crimes precisavam de um olhar mais apurado do legislador, pois ainda que já existissem algumas leis presentes no ordenamento jurídico brasileiro, como a Lei do Software, fazia-se necessário a criação de uma lei mais específica atribuindo aos criminosos da rede, sanções adequadas e previstas previamente em lei.

Assim, no final do ano de 2012 foi aprovada a Lei 12.737, chamada de lei dos crimes cibernéticos, que trouxe a tipificação de um único crime cibernético próprio, qual seja o de invadir dispositivo informático, driblando sistema de segurança (colocado pelo próprio usuário), com o fim de obter vantagem ilícita, sem a autorização do dono do dispositivo. Tal lei, traz também condutas que aumentam a pena atribuída ao tipo penal de invadir dispositivo informático, e ainda modificou dispositivos constantes no Código Penal, referentes a conduta de falsificar documento particular, incluindo o cartão de crédito ou débito como documento particular no qual incidirá a aplicação da lei penal, e a interrupção de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.

No mesmo dia e ano foi aprovada a Lei 12.735/12, que trouxe ao ordenamento jurídico pátrio a autorização para que os órgãos judiciários, com base em regulamento, estruturem equipes e setores especializados no combate aos crimes cometidos na rede de computadores e dispositivos da informática.

As mencionadas leis trouxeram ao ordenamento jurídico brasileiro importante inovação, dando suporte ao poder judiciário no combate aos crimes cibernéticos no território brasileiro, porém ainda são deficientes, de modo a não solucionar totalmente o problema da criminalidade efetuada no meio virtual e contra as informações particulares guardadas nos dispositivos informáticos.

É possível, todavia que com a aprovação recentemente do marco civil da internet no país, as mencionadas leis possam ter mais efetividade na sociedade brasileira. É de

suma importância a lei que rege a internet ter sido aprovada no Estado brasileiro, pois que quando esta entrar em vigor, os criminosos poderão sentir-se amedrontados de realizar crimes na rede, pois haverá maiores restrições no uso da internet. Contudo, como não é o objetivo deste trabalho discutir tal lei, fica aqui uma opção para mais um trabalho de monografia sobre o tema, com um apanhado feito depois da inclusão do marco civil na sociedade brasileira.

Os criminosos atuantes na seara da informática, recebem nomes específicos, pois não são consideradas pessoas comuns, mas sim pessoas especializadas no âmbito da tecnologia informatizada, conhecedores dos mais variados tipos de programas computacionais, capazes de afetar a vida de usuários comuns e também de empresas. A doutrina atribui às pessoas que se utilizam dos conhecimentos aprofundados da tecnologia informatizada para a prática de crimes, comumente de *rackers*, *crakers*, e outros, entretanto consideram de fato, que os verdadeiros criminosos atuantes nesta seara, são os *crakers*.

A rede de tráfego de dados – internet e a informática tem facilitado a prática delitiva, permitindo muitas vezes que os criminosos não sejam encontrados de forma rápida e eficaz. Isso acontece porque as informações oriundas da rede de internet podem transitar de um país a outro em questão de segundos, fato este que dificulta de forma considerável a aplicação da lei processual penal aos agentes do crime virtual.

Apesar de um crime cibernético alcançar não só a esfera do território nacional, o poder judiciário já possui meios possíveis de achar o dispositivo de onde partiu a conduta criminosa e onde ela chegou, e isso resolve a questão da competência, porém não é fator determinante para se afirmar que o agente foi encontrado, pois a máquina pode ser encontrada na casa de alguém que possui uma residência certa, mas pode não ser possível aplicar o mesmo quando diante de uma infração advinda de dispositivo localizado em uma *lan house*.

Cada máquina/dispositivo informático como foi aqui estudado possui um número IP, que é o seu identificador, que uma vez rastreado poderá acabar por encontrar o dono do dispositivo do qual partiu uma conduta criminosa, porém esse número não é o mesmo sempre, dificultando ainda mais a descoberta de quem dele se apropriou.

No que concerne à determinação da competência em consonância com a lei processual penal brasileira, prevê esta que sejam observados alguns critérios para essa determinação. Entretanto, o presente trabalho verificou com ênfase o critério, no qual se observa o lugar em que a conduta criminosa se deu por satisfeita.

O sistema de repressão aos crimes cibernéticos no país, ainda é deficitário, e quando o

assunto é a competência para análise processual e o consequente julgamento de tais práticas delitivas não é de todo modo fácil determiná-la, uma vez que quando for possível descobrir o (lugar) onde se encontra o dispositivo do qual partiu a conduta criminosa e onde esta se consumou, estará solucionada a questão da competência para julgamento, pois aí incidirá a regra geral prevista no artigo 70, caso contrário, tal regra será afastada, para que sejam usadas as outras regras, de caráter subsidiário.

Desta forma, uma vez que é sabido o lugar onde se consumou a conduta criminosa praticada no meio virtual, estará resolvida a competência para julgar tal crime, porém se isso não for possível, deverá ser aplicada a regra em que a competência se define pelo lugar onde o agente criminoso resida ou possua domicílio. E se o agente criminoso não tiver um lugar certo onde resida, será aplicada a regra do lugar onde este se encontre e no último caso, a competência será determinada pela prevenção, situação em que apenas se fará possível quando o juiz dentre os que se conceituam competentes para julgar esses crimes, tenha além de conhecido do feito primeiro que os outros, tenha este já feito algum procedimento no decorrer do processo.

Isso tudo, poderá ser aplicado quando diante de crimes plurilocais, que são aqueles que tem sua ação e execução dentro do território nacional, porém quando diante de um crime à distância, a jurisprudência tem feito uso da observação da teoria da ubiquidade, pois que nestes crimes se houver conflito de competência entre o Brasil e outro, poderão ser competentes tanto o nosso país, quanto o outro país atingido pela conduta criminosa.

Nesse diapasão, a regra do artigo 70, do Código de Processo Penal, quando o assunto for um crime cibernético plurilocal será a este aplicada, atuando assim a teoria do resultado e nos crimes à distância, tem mitigado a jurisprudência o olhar para a teoria da ubiquidade (lugar do crime, art. 6º, CP), entendendo que se a conduta tocar o território nacional, então será possível o Brasil julgar esses crimes.

Quando então houver conflito de competência territorial, segundo a jurisprudência referente a alguns crimes cibernéticos, poderá a competência ser determinada: pelo lugar onde aconteceu o crime ou onde a máquina esteja, observando também que as vezes a consumação do crime se verifica pelo simples ato de publicar algo na rede, não importando até onde esta conduta alcançou, até mesmo porque prima-se as vezes pelo lugar onde foi cometida a infração (no Brasil) para que este seja competente no processo e julgamento de tal conduta criminosa, afim de que sejam preservadas as provas concernentes ao delito virtual.

Referências

ALMEIDA FILHO, José Carlos de Araújo; CASTRO, Aldemário Araújo. *Manual de Informática Jurídica e Direito da Informática*. Rio de Janeiro: Forense, 2005.

ARAS, Vladimir. Crime de Informática. Uma Nova Criminalidade. *Jus Navigandi*. Teresina, ano 6, n. 51, Outubro de 2001. Disponível em: < http://jus.com.br/artigos/2250/crimes-de-informatica>. Acesso em 18/04/14.

BARROS, Flávio Augusto Monteiro de. *Direito Penal*: Parte Geral. 9ª Ed. São Paulo: Saraiva, 2011. Vol. 1.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, 1988. Disponível em: <http:// www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm>. Acesso em 18/09/2013.

_____. Código Penal (1940). *Decreto-Lei nº 2.848*, de 7 de dezembro de 1940. Brasília, 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em 19/09/2013.

_____. Lei de Introdução ao Código Penal. *Decreto-Lei nº 3.914*, de 9 de dezembro de 1941. Vade Mecum OAB e concursos. São Paulo: Saraiva, 2013.

_____. Lei nº 12.737/12, de 30 de novembro de 2012. *Dispõe so*bre 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: Brasília, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 19/09/2013.

_____. Lei nº 12.735/12, de 30 de novembro de 2012. *Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências*: Brasília, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm.>. Acesso em 19/09/13.

BRASIL. Superior Tribunal de Justiça. *CC 130134/TO*, da 3ª Seção do Superior

Tribunal de Justiça, Brasília, 2013. Disponível em: <www.stj.jus.br>. Acesso em 22/05/14.

_____._____. *CC 119914/DF*, da 3ª Seção do Superior Tribunal de Justiça, Brasília, 2013. Disponível em: <www.stj.jus.br>. Acesso em 22/05/14.

_____._____. *CC 125125/SP*, da 3ª Seção do Superior Tribunal de Justiça, Brasília, 2012. Disponível em: <www.stj.jus.br>. Acesso em 22/05/14.

_____._____. *CC 121431/SE*, da 3ª Seção do Superior Tribunal de Justiça, Brasília, 2012. Disponível em: <www.stj.jus.br>. Acesso em 22/05/14.

_____._____. *CC 107938/RS*, da 3ª Seção do Superior Tribunal de Justiça, Brasília, 2012. Disponível em: <www.stj.jus.br>. Acesso em 22/05/14.

BITENCOURT, Cezar Roberto. *Tratado de Direito Penal*: Parte Geral. 18ª Ed. rev, ampl, e atual. São Paulo: Saraiva, 2012. Vol. I.

BONFIM, Edilson Mougenot. *Curso de Processo Penal*. 8ª Ed. atual. São Paulo: Saraiva, 2013.

BUDAPESTE, CONVENÇÃO. *Convenção sobre o Cibercrime*. Budapeste, 2001. Disponível em: <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_ Acesso em 16/03/14.

CAVALCANTE, Andrea de Fátima Araújo. *A Atipicidade dos Crimes Cibernéticos no Brasil e a Impunidade*: uma análise crítica. Trabalho de Conclusão de Curso (Direito). Caruaru: Favip, 2011. Disponível em: <http://repositorio.favip.edu.br:8080/bitstream/123456789/866/1/Monografia+Andrea· >. Acesso em 19/03/14.

CÂMARA. Agência Câmara Notícias. *Brasil está atrasado em estratégias de combate a crimes cibernéticos*, 2013. Disponível em: <http://www2.camara.leg.br/camaranoticias/noticias/CIENCIA-E-TECNOLOGIA/437788 BRASIL-ESTA-ATRASADO-EM-ESTRATEGIAS-DE-COMBATE-A-CRIMES CIBERNETICOS.html>. Acesso em 13/05/14.

CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e seus Aspectos Processuais*. 2ª Ed. rev, ampl e atual. Rio de Janeiro, 2003.

CABETTE, Eduardo Luiz Santos. Primeiras impressões sobre a Lei 12.737/12 e o

crime de invasão de dispositivo informático. *Âmbito Jurídico*. Rio Grande, XVI, n. 109, fevereiro de 2013. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12865>. Acesso em 19/10/2013.

CAPEZ, Fernando. *Curso de Direito Penal*: Parte Geral. 16ª Ed. 2ª tiragem. São Paulo: Saraiva, 2012. Vol. I.

_____. *Curso de Processo Penal*. 19ª Ed. São Paulo: Saraiva, 2012.

COSTA, Fernando Jose da. *Locus Delict nos Crimes Informáticos*. Tese de Doutorado da Usp. 2011. Disponível em: <http://www.teses.usp.br/teses/disponiveis/2/2136/tde-24042012-112445/pt-br.php.>. Acesso dia 04/03/2014.

CORRÊA, Gustavo Testa. *Aspectos Jurídicos da Internet*. São Paulo: Saraiva, 2002.

CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais*. São Paulo: Saraiva, 2011.

FACULDADE PROJEÇÃO. *Normas e padrões para elaboração de monografias da escola de ciências jurídicas e sociais da faculdade projeção*. Blog Acadêmico. Taguatinga, 2013. Disponível em: <http://www.faculdadeprojecao.edu.br/blogacademico>. Acesso em 18/10/2013.

FERREIRA, Aurélio Buarque de Holanda. *Mini Aurélio Século XXI*, Escolar. 4ª Ed. rev, ampl. Rio de Janeiro: Nova Fronteira, 2000.

FERNANDES, David Augusto. Crimes Cibernéticos: O Descompasso do Estado e da Realidade. *Revista da Faculdade de Direito da Universidade Federal de Minas Gerais*. Belo Horizonte, n. 62, pp. 139-178, jan./jun. 2013. Disponível em: <http://www.direito.ufmg.br/revista/index.php/revista/article/view/P.03042340.2013v6 Acesso em 18/03/2014.

FERREIRA, Ivette Senise. A Criminalidade Informática. In: LUCCA, Newton De; SIMÃO FILHO, Adalberto (Coord.). *Direito & Internet – Aspectos Jurídicos Relevantes*. São Paulo: Edipro, 2001. p. 207-237.

GRECO, Rogério. *Curso de Direito Penal*, Parte Geral. 15ª Ed. rev, ampl. e atual. Rio de Janeiro: Impetus, 2013. Vol. I.

JORGE, Higor Vinicius Nogueira. Especialista em investigação de crimes cibernéticos fala sobre nova lei. *Revista da Defesa Social & Portal Nacional dos Delegados*. 05 de abril de 2013. Disponível em: <http://www.delegados.com.br/juridicos/4029-especialista-em-investigacao-de-

crimes-ciberneticos-fala-sobre-nova-lei.html>. Acesso em 12/04/14.

KAMINISKI, Omar. A Informática Jurídica, a Juscibernética e a Arte de Governar. *Revista Consultor Jurídico*. 17 de julho de 2002. Disponível em: < http://www.conjur.com.br/2002-jul-17/informatica_juridica_juscibernetica_arte_governar>. Acesso em 19/04/14.

_____. (Org.). *Internet legal*: o direito na tecnologia da informação. Curitiba: Juruá, 2006.

LINS, Bernardo F. E. *Privacidade e Internet*. Consultoria Legislativa da Câmara dos Deputados. Março de 2000. Disponível em: <http://www2.camara.leg.br/documentos-e-pesquisa/publicacoes/estnottec/tema4/pdf/001854.pdf>. Acesso em 22/04/14.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Fundamentos de Metodologia Científica*. 4.ed. rev. e ampl. São Paulo: Atlas, 2001, capítulo 4, p. 83-113.

LIMA, Gisele Truzzi de. *Redes Sociais e Segurança da Informação*. Gisele Truzzi Advogada Disponível em: <http://www.truzzi.com.br/pdf/artigo-redes-sociais-e-seguranca-da-informacao.pdf>. Acesso em 03/04/2014.

LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional*. 2ª Ed. São Paulo: Atlas, 2011.

LIMA, Renato Brasileiro de. *Curso de Processo Penal*. Niterói: Impetus, 2013.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. *Manual de Direito Penal*: Parte Geral Arts. 1º a 120 do CP. 28ª Ed. rev e atual. São Paulo: Atlas, 2012. Vol. I.

NETTO FILHO, Dickson Cirilo Andrade. Crime virtual: crime contra o patrimônio no âmbito da internet, suas peculiaridades e controvérsias à luz do Código Penal de 1940. *Âmbito Jurídico*. Rio Grande, XV, n. 104, setembro de 2012. Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12231>. Acesso em 19/09/2013.

NUCCI, Guilherme de Souza. *Manual de Direito Penal*: Parte Geral e Parte Especial. 8ª Ed. rev, ampl, e atual. São Paulo: Revista dos Tribunais, 2012.

_____. *Manual de Processo Penal e Execução Penal*. 10ª Ed. rev, ampl, e atual. São Paulo: Revista dos Tribunais, 2013.

OLIVEIRA, Eugênio Pacelli de. *Curso de Processo Penal*. 15ª Ed. rev e atual. Rio de Janeiro: Lumen Juris, 2011.

OLIVEIRA, Natacha Alves de. Crimes praticados pelo sistema de informática: visão prospectiva e sistemática à luz da jurisprudência pátria. *Âmbito Jurídico*. Rio Grande, XVI, n. 115, agosto de 2013. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=13587>. Acesso em 12/04/2014.

PAESANI, Liliana Minard. *Direito e Internet*: liberdade de informação, privacidade e responsabilidade civil. São Paulo: Atlas, 2000.

PECK, Patrícia. *Direito Digital*. São Paulo: Saraiva, 2002.

MINISTÉRIO PÚBLICO FEDERAL. Procuradoria da República no Estado de São Paulo. *Manual Prático de Investigação, Crime Cibernético*. São Paulo, 2006. Disponível em: <mpto.mp.br/athenas/.../manual-de-atuacao-em-crimes-ciberneticos-mpf>. Acesso em 13/05/14.

SOBRAL, Eduardo Miguel. *Análise da Lei Carolina Dieckmann*. Disponível em: <http://www.emersonwendt.com.br/2013/02/artigo-analise-da-lei-carolina.html#.UzWh fldXot>. Acesso em 25/03/2014.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. *Curso de Direito Processual Penal*. 8ª Ed. rev, ampl, e atual. Jus Podivm, 2013.

TOURINHO FILHO, Fernando da Costa. *Processo Penal*. 34ª Ed. rev. São Paulo: Saraiva, 2012. Vol. I.

VIANNA, Tulio Lima. *Transparência pública, opacidade privada*: o Direito como instrumento de limitação do poder na sociedade de controle. Tese de doutorado para a UFPR. Curitiba, 2006. Disponível em: <https://www.academia.edu/1911163/Transparencia_publica_opacidade_privada_o_di Acesso 23/04/14.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. *Crimes Cibernéticos*: Ameaças e Procedimentos de Investigação. 2ª Ed. Rio de Janeiro: Brasport, 2013, p. 1-78.