Crime digital: as barreiras jurídicas para a resolução destes crimes no Brasil

Luiz Fabiano Appolinário*

Tales Manoel Lima Vialôgo**

1. INTRODUÇÃO

No mundo globalizado em que vivemos o direito está tão plugado ao meio virtual quanto os próprios aparelhos voltados à conectividade e navegação e, assim sendo, enfrenta tantos problemas, ou até mais, que o mundo não cibernético.

A tecnologia da comunicação digital passa por constantes revoluções desde a sua criação. Foi a partir do seu uso comercial, há pelo menos 20 anos com o lançado o primeiro browser para a Web, em 1994, que começou a popularização da *Internet* saindo do seu uso exclusivo no meio acadêmico e militar, passando a fazer parte do cotidiano das pessoas comuns.

*Advogado, bacharel em Direito pelas Faculdades Integradas de Bauru-SP, analista de sistemas pela Universidade do Sagrado Coração-USC/Bauru.

**Advogado, especialista em Direito Empresarial com ênfase em Direito do Trabalho pela ITE – Bauru, Mestre em Direito Constitucional pela ITE – Bauru, professor titular do corpo docente das Faculdades Integradas de Bauru-SP e da Universidade Paulista-Unip/Bauru.

O uso do e-mail, a interatividade nos sites, mídias sociais e a possibilidade de criar espaços virtuais exibindo, postando ideias, fatos e fotos em blogs, entre outras coisas, mudou a forma de dialogar entre as pessoas que têm o acesso a *Internet* em suas residências, dispositivos portáteis (celulares, tablets, etc.), no trabalho e até mesmo em "lan houses". "O exame de seus aspectos técnicos e sua repercussão no modo de vida apontam para uma transformação cultural de hábitos e comportamentos de grandes proporções". (MIRAGEM, 2008, p. 43 apud MORAES, 2011).

Tudo isso leva a um mundo diferente do que o operador do Direito está acostumado em seu cotidiano. Enfrentado situações que, fora do mundo virtual, teriam um caminho de certo modo comum a ser trilhado para a solução do conflito. Já no mundo virtual muita coisa ainda está suspensa, aguardando uma direção do judiciário ou mesmo uma atitude do legislador para que possa caminhar. Este entrave entre o mundo real, onde as leis se posicionam como amparo para a resolução de praticamente 100% das lides, e o mundo virtual que esbarra em legislações deficientes para a solução de problemas semelhantes, porém de realidade virtual, encontra-se a problemática aqui discutida.

O que se tem hoje em matéria de legislação para o mundo virtual são verdadeiros Frankensteins. São leis criadas no "susto" e que surtem pouco efeito frente às barreiras processuais ou falta de leis auxiliares que facilitem a aplicação da lei em questão. Como foi o caso da lei estadual 12.228/06 (lei das Lan Houses) e a lei federal 12.737/12, apelidada de lei Carolina Dieckmann. A primeira ainda tem uma aplicabilidade mais ampla prevendo sanções para o estabelecimento visando justamente o resguardo legal do mesmo, já a segunda foi criada baseando-se no escândalo gerado por fotos roubadas do equipamento de uma celebridade, o que causou furor e impacto na mídia, porém de aplicabilidade duvidosa sendo que 90% dos delitos descritos por esta lei já eram aplicados por analogia.

No dia 23 de abril deste ano, 2014, foi sancionada pela presidente Dilma Rousseff, a lei 12.965/14, conhecida como Marco Civil da *Internet*, que foi considerada a "Constituição da *Internet*" e estabeleceu princípios, criou direitos e deveres e deu garantias para o uso da *Internet* no Brasil, mas já chegou causando algumas inseguranças e controvérsias em seus artigos como por exemplo a chamada Neutralidade da Rede e seu alcance, assim como a responsabilização do provedor de conteúdo por postagens de terceiros.

O texto do artigo 9º da Lei 12.965/14, com a seguinte redação:

> Da Neutralidade de Rede
> Art. 9o O responsável pela transmissão, comutação ou roteamento tem o dever de

> tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.
> § 1o A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da *Internet* e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:
> I – requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e
> II – priorização de serviços de emergência.
> § 2o Na hipótese de discriminação ou degradação do tráfego prevista no § 1o, o responsável mencionado no caput deve:
> I – abster-se de causar dano aos usuários, na forma do art. 927 da Lei no 10.406, de 10 de janeiro de 2002 – Código Civil;
> II – agir com proporcionalidade, transparência e isonomia;
> III – informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e
> IV – oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.
> § 3o Na provisão de conexão à *Internet*, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados respeitado o disposto neste artigo (BRASIL, 2014).

Trata o assunto intitulado de Neutralidade da Rede, o que nada mais é do que a proibição de alterações na velocidade e qualidade da prestação do serviço por parte dos provedores quanto a conteúdos, destinos de acesso ou mesmo utilização de produtos da concorrente, como por exemplo, a diminuição da velocidade nas conexões de programas de Voz sobre IP (VOIP), como o SKYPE. A Neutralidade se tornou uma regra, e aquele provedor que descumprir deverá se explicar. Mas como toda regra tem suas exceções, o §1º do artigo supra citado e seus incisos, trazem a previsão de quando esta regra poderá ser quebrada, possibilitando, nestes casos, a diminuição na velocidade e qualidade do serviço prestado.

Outro ponto importante com a chegada do Marco Civil da *Internet* é o armazenamento dos registros de conexão por parte dos provedores, que deverão guardar os respectivos registros por período de 1 (um) ano conforme descrito no artigo 13 da Lei 12.965/14:

> Da Guarda de Registros de Conexão
> Art. 13. Na provisão de conexão à *Internet*, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
> § 1o A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
> § 2o A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.
> § 3o Na hipótese do § 2o, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial

> de acesso aos registros previstos no caput.
> § 4o O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2o, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3o.
> § 5o Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
> § 6o Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência (BRASIL, 2014).

Para o Direito esse é um grande avanço, pois poderá aumentar a probabilidade de se encontrar os autores dos delitos digitais, ressalvadas as disposições expressas de que estas informações só poderão ser prestadas mediante autorização judicial (FIGUEIREDO, 2014).

O Marco Civil da *Internet* foi um ato necessário para o momento jurídico que envolve os usuários brasileiros da *Internet*, e é considerado como o texto pioneiro no mundo a iniciar a tentativa de regulamentação do ambiente virtual, que está, em grande parte, desguarnecido legalmente, porém ainda longe de se tornar a solução para os problemas oriundos da *Internet*, pois terá de ser aplicado em alguns casos concretos a fim de que possa se criar uma segurança jurídica quanto ao assunto.

Com isso, as condutas visando burlar a fiscalização da lei só tendem a aumentar. Alem dos já conhecidos golpes bancários com roubo de senhas seja por invasão, seja por instalação de programas espiões, a rede mundial de computadores foi invadida por ondas de vinganças pessoais contra ex-companheiros, a chamada *"pornografia de vingança"*, *"cyberbulling"*, *"sexting"*. Afora demais usos irregulares da *Internet* que comprometem a vida pessoal, social e ate mesmo o ambiente de trabalho de inúmeras pessoas. Não se pode de modo algum achar que a culpa de todos esses fenômenos que vêm ocorrendo ultimamente é da *Internet*.

A falta de celeridade na apuração de denúncias muitas vezes impede que, se quer, chegue-se perto de resolver situações, que são, em sua totalidade, cometidas por pessoas, e essas sim usuárias da *Internet*.

Mas deve-se ter muita cautela, pois de acordo com Peck (2011):

> Sabemos que em computação forense as testemunhas máquinas não conseguem diferenciar culpa de dolo, ou seja, um computador não traz informações do contexto da situação. Tão pouco consegue dizer se foi sem querer, sem intenção. Um exemplo disso é o envio de e-mails contaminados com arquivos maliciosos. Muitas pessoas abrem ou até mesmo enviam e-mails com vírus e às vezes a máquina pode ter se tornado um computador zumbi ou até mesmo ser controlado remotamente por terceiros para gerar esse tipo de ação (PECK, 2011, p. 294).

A omissão dos provedores de acesso, que se baseiam nos artigos de proteção aos dados pessoais de seus usuários, em fornecer as informações pedidas e na maioria das vezes exigidas pelo judiciário, cria uma falsa blindagem aos criminosos, que por um período de tempo podem manter-se desconhecidos, e deste modo, impunes. Ferramentas de desvio de rastreamento ou ate mesmo "Túneis Virtuais" que posicionem falsamente um dispositivo conectado localmente como se em outra cidade, estado ou país estivesse, praticamente impossibilitam o desvendar do mistério.

Atualmente, há a necessidade urgente da atenção dos legisladores para esta nova realidade. Esta atenção deverá se voltar não só parar a realidade local ou nacional, mas de maneira que possamos através de acordos ou tratados internacionais, unir forças com outros países que sofrem com tais crimes mediante a impunidade gerada pela globalização. Mais do que nunca devemos nos empenhar para tentar eliminar os "estragos" gerados pela legislação despreparada para lidar com a nova realidade. Uma realidade de mudanças constantes e quase instantâneas, que a cada momento se torna mais invasiva e abusada.

2 CONCEITO DE CRIME

"Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal." Assim inicia-se o código penal em seu primeiro artigo, com sua redação de 11 de Julho de 1984.

A ciência jurídica tem acompanhado a evolução da humanidade que a cada dia rompe seus limites forjando assim novos objetivos a serem ultrapassados.

A evolução da sociedade obriga o Direito a ser, hoje, mais dinâmico do que em tempos remotos.

Não há no Código Penal Brasileiro atual uma definição de crime, sendo assim a doutrina desenvolveu alguns conceitos que são hoje utilizados por nossos operadores do direito. Segundo Mirabete (2012) existem três tipos de forma de conceituar o crime, que são o conceito formal, material e analítico.

O conceito formal é aquele que segue o que a lei preceitua, sendo assim o legislador define uma conduta como crime, um fato que possa ser punível, já existira o crime por si só, sem entrar em sua essência, em seu conteúdo, em sua matéria. Porém essas definições limitariam a visibilidade do crime em apenas um dos aspectos do crime, a ilegalidade a uma norma penal.

> Sob o aspecto formal, podem-se citar os seguintes conceitos de crime: "Crime é o fato humano contrário à lei" (Carmignani); "Crime é qualquer ação legalmente punível" (Miggiore); "Crime é toda ação ou omissão proibida pela lei sob ameaça de pena" (Fragoso); "Crime é uma conduta (ação ou omissão) contrária ao Direito, a que a lei atribui uma pena" (Pimentel). (MIRABETE, 2012, p.79).

Já o conceito material procura explicar o que é o crime, sob vários outros aspectos que chegam a envolver outras ciências extrajurídicas, como por exemplo, a Sociologia, a Filosofia, a Psicologia, etc.

Esse conceito procura uma definição de crime indagando a razão que levou o legislador a prever a punição dos autores de certos fatos e não de outros, fazendo assim uma análise mais profunda para definir o que é crime e não apenas ao aspecto externo do crime, como se delito for à ação ou omissão, imputável a uma pessoa, lesiva ou perigosa a interesse penalmente protegido, constituída de determinados elementos e eventualmente integrada por certas condições, ou acompanhadas de determinadas circunstâncias previstas em lei.

Mirabete (2012) diz que as referências nessas definições de crime, sob o aspecto material, a "valores ou interesses do corpo social", "condições de existência, de conservação e de desenvolvimento da sociedade" e "norma de cultura", apresentam problemas.

Faria Oliveira (2014) no artigo "A definição de crime", faz a seguintes citações:

> Manoel Pedro Pimentel (2012) afirma que resta ainda dificuldade em fixar o critério, segundo o qual o legislador consideraria conduta à norma de cultura. Por esse motivo não foi criado um conceito material inatacável de crime.
> O conceito analítico diz que o crime é a "ação típica, antijurídica e culpável".
> Segundo Battaglini crime é "o fato humano descrito no tipo legal e cometido com culpa, ao qual é aplicável a pena".
> Basileu Garcia já define crime como a "ação humana, antijurídica, típica, culpável e punível".
> Mesmo a punibilidade sendo a "possibilidade de aplicar-se a pena", ele não é elemento do crime.
> Segundo Hungria "um fato pode ser típico, antijurídico, culpado e ameaçado de pena, isto é, criminoso e, no entanto, anormalmente deixar de acarretar a efetiva imposição da pena".
> O conceito mais usado é o que diz que crime é a "ação típica, antijurídica e culpável", sendo utilizada tanto pelos autores que seguem a teoria causalista, como pelos que seguem a teoria finalista da ação.
> A culpabilidade para a teoria causalista consiste no vínculo subjetivo que liga a ação ao resultado, ou seja, no dolo, ou na culpa em sentido estrito por imprudência, negligência ou imperícia.
> Na teoria finalista a conduta ou ação é uma atividade que sempre tem uma finalidade.
> O conceito analítico abrange o dolo e a culpa em sentido estrito, sendo assim, o crime existe em si mesmo, por um fato típico e antijurídico, e a culpabilidade significa reprovabilidade ou censurabilidade de conduta.
> O crime tem os requisitos genéricos e os requisitos específicos. Os requisitos genéricos

> são a tipicidade e a antijuricidade, e os específicos são as circunstâncias elementares, que estão descritos no artigo 30 do CP, exemplo é o verbo que descreve a conduta, o objeto material, os sujeitos ativo e passivo, etc.(FARIA OLIVEIRA, 2014).

A definição de Crime Digital obrigatoriamente está encaixada entre esses conceitos citados acima acrescida apenas do meio em que será cometido. Mas é um assunto que será abordado em um capítulo à parte no decorrer deste trabalho.

3 SURGIMENTO DA INTERNET

A *Internet* não nasceu do dia para noite como alguns pensam. A nova geração humana sequer teve contato com o desenvolvimento da Rede Mundial de Computadores, que é resultado do avanço das comunicações por meio elétrico, iniciadas em 1605 com o desenvolvimento do alfabeto binário por Francis Bacon. Desde então a evolução das comunicações eletroeletrônicas caminhou a passos lentos se comparada com a evolução advinda do século XX.

Da descoberta de 1605 até a primeira transmissão de mensagens por telégrafo, que aconteceu em 1844, se passou mais de dois séculos. E a caminhada pela descoberta de novas tecnologias neste setor continuou lenta, pois o primeiro computador foi aparecer como algo concreto um século depois da primeira transmissão do telégrafo, em 1946. O ENIAC (Electronic Numerical Integrator Analyzer and Computer) que em português se traduz como "Computador Integrador Numérico Eletrônico". Segundo o site Wikipédia, o ENIAC começou a ser desenvolvido em 1943 durante a II Guerra Mundial para computar trajetórias táticas que exigissem conhecimento substancial em matemática, mas só se tornou operacional após o final da guerra. Esta máquina não tinha sistema operacional e seu funcionamento era parecido com uma calculadora simples de hoje. O ENIAC, assim como uma calculadora, tinha de ser operado manualmente, (ENIAC, 2104).

A calculadora efetua os cálculos a partir das teclas pressionadas, fazendo interação direta com o hardware, como no ENIAC, no qual era preciso conectar fios, relês e sequências de chaves para que se determinasse a tarefa a ser executada. A cada tarefa diferente o processo deveria ser refeito. A resposta era dada por uma sequência de lâmpadas.

Este invento foi a base para o que conhecemos hoje como *INTERNET*. Para que um invento desta magnitude se as informações ainda necessitavam ser compartilhadas pessoalmente, de pessoa a pessoa, o famoso boca a boca?

De 1946 até a data atual (2014) a busca foi intensa pela comunicabilidade e interação, pois um ditado antigo já dizia que "tempo é dinheiro", e isso realmente é verdade se olharmos a retórica de nossa história financeira mundial, onde quem tinha as melhores informações conseguia melhores resultados em seus investimentos e estas informações para serem as melhores precisavam chegar em menos "tempo".

Nesses 68 anos de historia do computador a revolução da indústria da informação foi a mais espantosa de todas. O que antes demorava horas e até mesmo dias para chegar de um lado ao outro do mundo, agora chega em segundos e muitas vezes até em tempo real com fotos, vídeos e detalhes minuciosos.

Esse poderoso meio de comunicação mundial nasceu como ARPANet, acrônimo em inglês de Advanced Research Projects Agency Network (ARPANet) do Departamento de Defesa dos Estados Unidos da América, foi a primeira rede operacional de computadores à base de comutação de pacotes, e o precursor da *Internet*.

A ARPANet foi desenvolvida no período conhecido como Guerra Fria, historicamente marcado por disputas estratégicas e conflitos indiretos entre Estados Unidos da América e a extinta União das Repúblicas Socialistas Soviéticas entre o final da segunda guerra mundial (1945) e a dissolução da União Soviética (1991). Como os dois países lutavam pelo poder político, militar, tecnológico e principalmente econômico nas zonas mundiais que mantinham influência, a ARPANet foi um meio de proteger e manter as informações militares dos EUA caso seu inimigo conseguisse atacar sua central de inteligência, o Pentágono (ARPANet, 2014).

A ARPANet foi a primeira a utilizar servidores descentralizados e espalhados sem uma central definida ou mesmo uma rota fixa, tornando a praticamente indestrutível, conceito utilizado até hoje pela *INTERNET*.

Segundo Ramalho Terceiro (2002):

> A *INTERNET* teve sua origem embrionária em plena guerra fria como arma militar norte-americana de informação. A idéia consistia em interligar todos os computadores as centrais de computadores dos postos de comando estratégicos americanos, precavendo-se, pois, de uma suposta agressão russa. Sendo atacado um desses pontos estratégicos, os demais poderiam continuar funcionando autonomamente, auxiliando e fornecendo informações a outros centros bélicos (RAMALHO TERCEIRO, 2002).

No final da década de 70, o protocolo até então utilizado pela ARPANet torna-se inadequado para o crescimento da rede devido a permissão de conectividade de universidades e outras instituições que desenvolviam assuntos relacionados com a Defesa de Estado e com isso em meados de 1975 a rede possuía aproximadamente

100 sites. Tal abertura levou a utilização do protoloco TCP/IP (Transmission Control Protocol/*Internet* Protocol) daí a origem do nome *INTERNET*. A ARPANet se dividiu em duas: a MILNet manteve seu propósito militar inicial e o restante da rede, agora aberta ao público, passa a se chamar *INTERNET*.

A parte mais utilizada da *INTERNET,* como conhecemos hoje, começa a ser desenvolvida em 1980 e só tem um projeto definitivo lançado em 6 de agosto de 1991 como World Wide Web ou simplesmente WWW, que teve seu primeiro navegador gráfico desenvolvido em 1993 e chamava-se MOSAIC. O projeto promissor teve uma aceitação de mercado muito boa e foi comercializado passando, em 1994, a se chamar NETSCAPE.

À partir deste marco a guerra comercial pela Word Wide Web estava declarada. Navegadores de desenvolvedores distintos brigam até hoje pelo mercado. A explosão dos chamados ".com" e a criação praticamente desenfreada de sites, portais de notícias, prestadores de serviços, entidades financeiras e as atuais mídias sociais trouxeram a tão sonhada economia de tempo e muitos problemas.

No Brasil a *Internet* deu seus primeiros passos no final da década de 80. Em 1989 o Brasil recebeu a autorização para utilizar o ".br" no final dos endereços WWW que eram registrados no país. Até o final de 1994 a *INTERNET* era utilizada apenas no meio acadêmico devido ao seu alto custo de conexão, pois a estrutura necessária para que usuários locais pudessem acessar a *INTERNET* foi disponibilizada pela Embratel apenas em maio de 1995 (MULLER, 2013).

Neste inicio conturbado o acesso era difícil, caro e restrito a poucos. Isso não entusiasmou muitos serviços além dos já conhecidos portais de noticias, sites de pesquisas científicas e correio eletrônico, o famoso e-mail. A popularização do acesso trouxe um novo foco comercial à *INTERNET*. Mais empresas passaram demonstrar interesse em oferecer seus serviços através da web. Devido ao seu baixo custo e a disseminação e compartilhamento de ideias de modo praticamente instantâneo, muitas pessoas aproveitaram a oportunidade para explorar as fragilidades deixadas pela expansão sem precedentes da rede mundial de computadores. Um dos maiores problemas do início da *INTERNET* foi o surgimento dos vírus de computador, programas de tamanho reduzidíssimo que desempenhavam várias funções, entre elas a de roubar usuários e senhas de e-mails, número e senhas de cartões de crédito, contas bancárias além de atrapalhar o funcionamento do computador e até sumir com arquivos pessoais.

Segundo Ramalho Terceiro (2002):

> Com a popularização da *Internet*, surgiu uma nova forma de revolução, trazendo consigo certas peculiaridades entre seus adeptos. Entre tais novidades surge a expressão linguística hacker, esta palavra em si é alvo de discórdia, uma vez que detém vários significados entre este submundo.
> Assim como o direito, a nossa língua sofre uma influência natural das transformações atuais, basta para comprovar o alegado, perguntar a alguém se já tomou conhecimento do que venha a ser um Hacker, ou seja, indivíduos que possuem conhecimentos específicos e aprimorados no setor informático, cuja essência de vida deste indivíduo é haraganear pela *Internet* "invadindo" computadores alheios, tanto o é, que consta no Dicionário Aurélio a definição do que seja hackers dispondo que é o "Indivíduo hábil em enganar os mecanismos de segurança de sistemas de computação e conseguir acesso não autorizado aos recursos destes, ger. a partir de uma conexão remota em uma rede de computadores; violador de um sistema de computação", urge salientar que a pouco expomos ser esta uma definição genérica, sendo o cracker o indivíduo agressor de computadores (RAMALHO TERCEIRO, 2002).

Os primeiros delitos digitais como roubo de senhas de e-mails, invasões por IP para downloads e destruição de arquivos pessoais, geraram confusão sobre como classificar tais crimes.

De acordo com Gouvêa (1997, p. 137-138):

> As controvérsias começam pela própria definição do tema. Afinal, quais são os crimes praticados por meio da informática – todos aqueles em que o computador ou outros recursos da informática são usados para a prática de condutas delituosas ou apenas aqueles em que os sistemas informática são atingidos?
> Parece claro que a atenção deve ser voltada para estas duas espécies de conduta, pois apresentam peculiaridades que as tornam diferentes de qualquer outro ramo do Direito, merecendo assim, um estudo à parte.

Aos poucos essas controvérsias foram sendo sanadas e os crimes digitais, cibernéticos ou informáticos começaram a ser delimitados pelo princípio da analogia.

3.1 A RELEVÂNCIA DA INTERNET

O crescimento do número de usuários da rede mundial de computadores, a *Internet*, trouxe relevante importância para esta, tornando-a um dos principais meios de comunicação, oferecimento de serviços, venda de produtos, entre outros. Tudo isso visando a comodidade do usuário que pode desfrutar de serviços bancários, por exemplo, sem precisar se deslocar até o estabelecimento. Mas esta comodidade também o torna o meio mais comum para o cometimento dos crimes na área virtual. A *Internet* que até tempos remotos, era uma ceara para poucos, alcançou uma popularidade meteórica, colocando o nosso país como quinto país

com o maior número de internautas do mundo:

> Com 68 milhões de visitantes únicos na *Internet*, o Brasil ultrapassou a Rússia em 2014, sendo agora a 5ª maior audiência digital do mundo. É o que revelou um levantamento produzido pela ComScore, empresa especializada em análise de dados e estatísticas envolvendo *Internet*. O estudo, intitulado "Brazil Digital Future in Focus 2014", compila tendências sobre uso da *Internet* no país, envolvendo temas como mobile, redes sociais, publicidade e e-commerce.
>
> A pesquisa aponta que o Brasil representa 40% dos 169 milhões de internautas da América Latina. Praticamente dois terços desses brasileiros (65%) têm menos de 35 anos, sendo 51% homens e 49% mulheres. São Paulo, Rio de Janeiro, Minas Gerais e Rio Grande do Sul são os estados com a maior quantidade de internautas, mostrando também o maior crescimento na base de usuários de *Internet* de 2013 a 2014.
>
> Referente ao tempo online a pesquisa mostrou que os brasileiros passam, em média, 29,7 horas por mês na *Internet*, ou, sete a mais que a média mensal mundial de 22,7 horas, e quase oito a mais que a média da América Latina, de 21,9 horas (E-COMMERCE NEWS, 2014).

Tais números provam que a cada dia mais serviços são disponibilizados na rede atraindo assim mais usuários, o que afirma a *Internet* como parte da realidade vivida pela quase totalidade de sujeitos de diretos no mundo todo.

Esta importância alcançada pela *Internet* a coloca como uma das principias vias de aumento no cometimento de crimes cada dia mais diversos e contundentes. Vendas de produtos falsificados a preços bem inferiores, por exemplo, possibilitam maior movimentação monetária e garantia de lucros dobrados, ao mesmo tempo em que as obrigações fiscais ficam prejudicadas, uma vez que não são recolhidos os tributos devidos ao Estado, que não possui maneiras de controlar as transações efetuadas.

E o que dizer do ramo do direito do trabalho, onde diversas pessoas utilizam-se da comodidade de trabalhar em casa por conta da versatilidade oferecida pela ferramenta aqui debatida, visando aumentar sua rentabilidade familiar, ou mesmo pessoal, trabalhando de forma on line. Escolas que oferecem ensino a distância (EAD) caminham nesta mesma linha.

O velho sistema de correio não foi totalmente abandonado, mas vem sendo massivamente substituído pelo uso do correio eletrônico, possibilitando maior velocidade nas comunicações.

Hoje se pode afirmar e dizer que a *Internet* se tornou um mal necessário. O mundo atual sem tecnologia deixaria grande parte da população enlouquecida devido a dependência criada por esta. A grande maioria dos usuários das inúmeras formas de utilização da *Internet*, dizem que são viciados em tecnologia, e que se sentiria alienada e até com crises de abstinência pela falta de interação tecnológica.

São exatamente estas variadas formas de utilização que possibilitam às mentes

criminosas aplicarem seus golpes. Engana-se quem atribui aos criminosos virtuais termos como vagabundo, pois praticar tais atos requer um alto nível de conhecimento e tempo para adquiri-lo com o intuito de que a atividade delitiva torne-se anônima, eficaz e impunível, uma vez que os operadores não detêm conhecimento suficiente para elaborar um conjunto probatório capaz de demonstrar com segurança a autoria do delito.

Não se pode mistificar o uso da *Internet* como sendo apenas um alvo para o cometimento de crimes e, desta maneira, esquecer seus fins lícitos e de imensa importância, pois a modernidade não permite mais imaginar a vida contemporânea sem as relações desenvolvidas através do mundo virtual, encurtando distâncias e reduzindo seu tempo de realização destas relações.

4 EVOLUÇÃO DO CRIME

Anteriormente conceituamos crime sob a luz de um dos grandes doutrinadores da nossa época, Julio Fabbrini Mirabete. Neste capítulo faremos uma breve menção à necessidade do surgimento das legislações como divisor de águas entre o que as sociedades consideram "certo" ou "errado". Desde os primórdios, ao se moldar costumes e elaborar leis, sempre esteve presente uma das principais preocupações do homem que vive em sociedade, que é limitar e regular o procedimento das pessoas diante das mais diversas condutas consideradas como nocivas e reprováveis.

Um dos regulamentos escritos mais antigos que se tem notícia é o código sumeriano de "Ur-Nammu" que data de aproximadamente 2100 A.C, no qual podemos ver alguns artigos dos quais preconizam penas para atos delitivos. O Código de Hamurabi, uma compilação maior e posterior, dentre outros regramentos penais contra o crime, adota a chamada Lei de Talião ou a conhecida lei do olho por olho, dente por dente, que concedia aos parentes da vítima o direito de praticar com o criminoso a mesma ofensa e no mesmo grau por ele cometida (MIRABETTE, 2012).

Até a idade média a noção de crime não era muito clara, frequentemente confundida com outras práticas reprováveis que se verificavam nas diversas esferas legais, administrativas, contratuais, sociais, e até religiosas.

Até a consagração do princípio da reserva legal em matéria penal ou "*nullum crimen nulla poena sine lege*" (não há crime, não há pena, sem lei), crime e pecado se confundiam pela persistência de um vigoroso direito canônico que às vezes confundia (e até substituía) a legislação dos Estados.

Tal princípio tem grande influência sobre a formulação atual de várias legislações

penais que, em verdade, não proíbem nenhuma prática, mas simplesmente tipificam condutas e preconizam as respectivas penas àqueles que as praticam.

Desta maneira é correto afirmar que não há lei alguma que proíba alguém de matar uma pessoa. O que há é uma lei que define e tipifica esta ação definindo-a como crime, e lhe dá as diversas penas aplicáveis àquele que a praticou, levando ainda em conta as diversas circunstâncias atenuantes ou agravantes presentes em cada caso.

As legislações evoluíram acompanhando o desenvolvimento das sociedades, porém as diversas maneiras de se praticar os mesmos crimes acabam por evoluir de forma que tais leis acabam ficando obsoletas ou mesmo não prevendo determinada forma de execução, o que acaba impedindo a aplicação de algumas sanções pela impossibilidade da tipificação do meio utilizado na conduta anteriormente descriminada. Este é o caso de alguns crimes digitais.

4.1 CRIME DIGITAL

Os crimes digitais são relatos recentes quando pensamos em história do crime. Os primeiros indícios sobre delitos digitais ou crimes informáticos como também são conhecidos, datam do século XX. Em 1960 as primeiras queixas foram levadas a público sobre crimes de sabotagem e manipulação de sistemas. Já na década de 1970 surgiu a figura do hacker, responsabilizado por invasões de sistemas e furto de softwares. Mas os crimes digitais começaram a expandir atingindo as mais diversas vertentes possíveis na década de 1980. Os crimes de pirataria, pedofilia, invasão de sistemas e o surgimento e propagação dos temidos vírus de computador (CARNEIRO, 2012).

Os vírus de computador são programas com um tamanho praticamente desprezível e que se multiplicam com uma rapidez que acompanha a evolução da tecnologia.

Segundo o site Segurança Uol, uma das definições de vírus é a seguinte:

> São programas desenvolvidos para alterar nociva e clandestinamente softwares instalados em um computador. Eles têm comportamento semelhante ao do vírus biológico: multiplicam-se, precisam de um hospedeiro, esperam o momento certo para o ataque e tentam esconder-se para não serem exterminados.
>
> Os vírus de computador podem anexar-se a quase todos os tipos de arquivo e espalhar-se com arquivos copiados e enviados de usuário para usuário. Uma simples rotina, ou comando, pode disparar o gatilho do vírus, que pode mostrar apenas mensagens ou imagens (sem danificar aquivos da máquina infectada), ou destruir arquivos e reformatar o disco rígido. Se o vírus não contém uma rotina de danos, ele pode consumir capacidade de armazenamento e de memória ou diminuir o desempenho do PC infectado. (SEGURANÇA UOL, 2014)

Diversos vírus famosos surgiram durante este lapso temporal. Nomes ameaçadores e engraçados como Madona, Sexta Feira 13, Chernobyl, I Love you. Cada um com seu poder de destruição e alguns que serviam apenas para atrapalhar e tomar tempo dos usuários e corporações. (TEC MUNDO, 2013)

Um dos tipos de vírus mais famosos é o Cavalo de Tróia ou Trojan Horse, que segundo a mitologia, foi um grande cavalo de madeira que os troianos pensavam ter conquistado durante a guerra e mal sabiam que em seu interior os gregos haviam deixado soldados escondidos para atacarem apenas depois que já estivessem dentro dos muros da cidade fortificada e em se tratando de crimes digitais, o princípio da invasão é o mesmo.

> [...] bastante interessante é o uso de programas semelhantes a vírus denominados Trojan Horses ou Cavalos de Tróia. Em lugar de destruir programas ou arquivos os trojan monitoram a digitação do login e da senha da vítima e os gravam num pequeno arquivo que fica oculto no sistema. Quando o usuário se conecta à rede o trojan envia um email para seu criador com o arquivo que contém o login e a senha do usuário (VIANA, 2003, p.4)

Várias ameaças virais como Phishing, que é a "pesca" de dados bancários e senhas através do envio de e-mails com pedidos de atualização e tipos diversos de invasão devastaram o mundo digital desde então e, com isso, houve urgência na criação de setores preocupados com a segurança virtual que exige uma atenção especial para identificação e punição dos responsáveis.

4.2 CONCEITO DE PROVAS NO CRIME DIGITAL

Quando se fala em direito digital não se deve pensar em um ramo novo do direito, mas sim na forma de aplicar os diversos ramos existentes do direito para a solução de conflitos nos contratos, negociações e etc. efetivadas tendo como escritório a plataforma virtual.

Assim também é com o crime digital. Os crimes cometidos por meio digital são tratados pelo código penal. Como alguns deles são exclusivamente cometidos através desta plataforma, leis como as já citadas anteriormente, foram criadas para suprir esta lacuna e adicionadas ao Código Penal Brasileiro. Mas o que diferencia o crime digital dos crimes comuns cometidos fora do âmbito virtual?

Essa é justamente a discussão proposta por este trabalho, a materialidade e autoria dos referidos crimes digital. Como a fase processual trata hoje os delitos cometidos virtualmente se, em sua grande maioria, a dificuldade está em se chegar a fonte criminosa.

Já foram abordadas, em capitulo anterior, algumas definições de crime segundo doutrinadores através do tempo. Temos também três teorias que tratam sobre o crime:

- Teoria bipartite - Elementos do Crime = fato típico, antijurídico.
- Teoria tripartite - Elementos do Crime = fato típico, antijurídico, culpável.
- Teoria quatripartida - Elementos do Crime = fato típico, antijurídico, culpável e punível.

E apesar de as três teorias contarem com a presença de dois elementos fundamentais que são o fato típico e antijurídico, a adotada pelo nosso Código Penal é a Teoria tripartite, embora grande número de criminalistas já defenda a aplicação da Teoria bipartite.

Partindo deste princípio, não se pode falar em crime sem que estejam presentes todos os elementos do crime e na ausência de um destes, não há crime. Todo crime parte do pressuposto da presença indispensável da conduta humana, no crime digital não é diferente. A máquina, embora hoje se encontre altos níveis de I.A. (Inteligência Artificial), não efetua nada sozinha. Esse conceito não foi abandonado, pois exige-se a presença humana que desenvolva a ferramenta que será usada como artifício no cometimento do delito virtual, e o desenvolvimento de tais meios está cada dia mais popular entre os criminosos do *cyber espaço,* e por isso o número de crimes catalogados tendo o mundo digital como ambiente fático tem aumentado a cada minuto, e provar a autoria delituosa tem se tornado uma tarefa árdua e ás vezes quase impossível.

O roubo das fotos íntimas de Carolina Dieckmann, caso que gerou a lei nº 12.737, de 30 de novembro de 2012 e que dispõe sobre a tipificação criminal de delitos informáticos e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) e dá outras providências, só pôde ser elucidado com tal velocidade devido à tentativa de extorsão por parte de um dos integrantes do grupos de *hackers* que invadiu o email da atriz que a policia conseguiu desencadear a chamada engenharia reversa e rastrear para onde os arquivos foram enviados.

Mas isso, quando se trata de crime digital, é trabalho considerado amador. Exemplo disso esta no grupo *Anonymous* que executou diversas incursões nas redes virtuais, invadindo sites governamentais de vários países, incluindo o Brasil, paralisando empresas de cartão de crédito (SOARES, 2013).

Nestes e em outros ataques contra dispositivos informáticos não resta dúvida sobre a materialidade do fato, porém deixa um dos quesitos indispensáveis em torná-lo culpável: a "autoria".

Com autor desconhecido mantemos o fato típico, antijurídico e culpável, mas quem é o culpado?

Somente depois de demonstrada a materialidade, comprovando a existência do delito, e a autoria, que se refere à pessoa sobre a qual recairá a sanção penal prevista em lei, é que o magistrado poderá prolatar sua decisão. Em caso de dúvidas será aplicado o famoso "*in dúbio pro reo*", e o investigado ou denunciado deverá ser absolvido, sob a alegação de que o conjunto de provas juntadas aos autos foi insuficiente para ter-se certeza dos fatos reais.

Diante do exposto, temos como vilã do processo de autoria em crime digital: as provas.

Existem hoje, à disponibilidade das mentes criminosas, centenas de ferramentas que possibilitam despistar a origem do crime como desviadores de IP, túneis virtuais, acessos remotos, programas de Proxy entre muitos outros.

Essas ferramentas possibilitam o que a maioria dos criminosos deseja: o anonimato.

> Tor (anteriormente um acrônimo para "The Onion Router" ou o Roteador Cebola, fazendo menção à navegação em camadas) é um software livre e de código aberto para proteger o anonimato pessoal ao navegar a *Internet* e atividades online, protegendo contra a censura e protegendo a privacidade pessoal. A maioria das distribuições GNU/Linux disponibilizam pacotes do Tor, embora haja versões para diferentes sistemas operacionais, tais como Windows e Mac OS. A rede Tor é uma rede de túneis http (com tls) sobrejacente à *Internet*, onde os roteadores da rede são computadores de usuários comuns rodando um programa e com acesso web (apenas). O objetivo principal do projeto é garantir o anonimato do usuário que está acessando a web.
> A partir daí, o Tor vai rotear todo o tráfego do computador através de túneis http da rede Tor até o destino, na rede "convencional". Se o usuário entrar em site do tipo http://myip.is e http://meuip.com.br, vai ver que o seu endereço vai aparecer diferente do seu endereço real (anonimato). O endereço que vai aparecer é o endereço do nó Tor por onde ele saiu da rede Tor para a rede "convencional". O tráfego é roteado por vários nós Tor, o que pode deixar o acesso bem lento, às vezes.
> Ou seja, para o servidor acessado você terá o endereço IP de um do nó de saída, como a rede Tor tem uma topologia caótica (aleatória), não se pode escolher o IP final ou de qual região da rede será. Por exemplo, usando a rede Tor você não pode escolher ter um IP de uma máquina localizada em um país ou região específica.
> Ainda é possível aumentar a rede, abrindo seu computador para uso de outros usuários do Tor4. (TOR, REDE DE ANONIMATO, 2014 – grifo meu).

Esses crimes geralmente são cometidos através da *DEEP WEB* ou "*Internet Profunda*", que segundo o site da Anonynous Brasil tem a seguinte definição:

> O que chamamos de "rede profunda" são redes de proxies, conectadas a vários computadores, formando outra rede da *Internet*. Pode ser facilmente comparada a VPN (Virtual Private Network ou Rede Virtual Privada) utilizada por algumas empresas comuns como segurança dos funcionários (ANONYMOUSBRASIL.COM, 2013).

Muito embora a *DEEP WEB* não fora concebida com o intuito unicamente voltado para o crime, ela se tornou uma faca de dois gumes. Nesta camada da web são encontrados tanto sites preocupados apenas com o anonimato de seus visitantes e colaboradores quanto àqueles com informações e conteúdos mais variados, diversos e porque não, macabros.

> Nessa porção da *Internet* inacessível aos navegadores comuns é possível encontrar livros raros, artigos científicos e fóruns de discussões específicas que tiram proveito da liberdade de expressão. Mas é lá também onde estão os sites do submundo, dedicados a atividades ilegais - que vão desde a venda de drogas ilícitas até a oferta de serviços de matadores de aluguel, passando ainda por conteúdo macabro e ultrajante, geralmente envolvendo a prática de crimes. Esse lado sombrio da rede é chamado de "dark web".
> [...] o pesquisador Sergey Lozhkin, especialista da companhia de segurança Kaspersky Lab, revelou dados de seu estudo sobre os recursos da deep web através da rede Tor no qual constata a existência de cerca de 900 serviços à disposição dos cibercriminosos. Entre eles estão a hospedagem para infraestrutura de funcionamento de programas maliciosos (malware), lavagem de dinheiro, venda de informação para prática de fraude financeira ou de kits de vírus para golpes na *Internet*.
> Todos esses serviços se aproveitam da capacidade da rede Tor de tornar difícil a identificação e a eliminação das ameaças. Outro item necessário para existência desse mercado negro é a "bitcoin", a moeda virtual que também garante que as transações sejam feitas no anonimato (DIÁRIO DO NORDESTE, 2014).

A "*Internet profunda*" é considerada hoje o "*underground*" dos crimes cometidos tendo a tecnologia como meio de execução ou apenas como ferramenta auxiliar no cometimento destes. Redes de pedofilia, facções criminosas, entre outras, se utilizam deste subterfúgio para obter êxito em suas ações delituosas. Isto tem gerado problemas além do que se poderia imaginar em épocas remotas quando o assunto era associação ao crime, devido justamente as distâncias físicas, que hoje se tornaram ínfimas, tendo em vista a velocidade com que a informação pode trafegar combinada com áudio e vídeo.

> *Deep Web* – Sites criptografados, onde você só consegue ter acesso com programas específicos.
> Existe um bom motivo para esses sites serem criptografados e acessados apenas via proxy (mecanismos que dificultam o rastreamento do seu IP). E qual é esse motivo? Simples, a *Deep Web* esconde o que de mais perverso o ser humano pode produzir. Pedofilia pesada, tráfico de armas, drogas, órgãos, assassinos de aluguel, seitas macabras, *hackers,* tudo isso são figurinhas carimbadas escondidas pelo anonimato da *Deep Web* (DEEP WEB, 2014).

Esse é um dos maiores desafios em se provar a autoria do delito, já que a materialidade quase não é discutida em função de, na maioria das vezes, estar aos olhos dos usuários da rede.

Certamente que o Instituto das Provas passa por um momento de transição em seus padrões no sentido da valoração das provas que possuam um maior grau de certeza e confiabilidade.

O mundo virtual tem sido, senão o principal, um dos principais protagonistas nesta transição de valores pela qual passam as provas processuais na busca deste grau de certeza e confiabilidade. Avanços ocorreram na produção de provas com confiabilidade técnica, mas ainda há muita divergência quanto a aceitação da prova eletrônica.

5 MEIOS DE PROVAS ADMITIDAS NO CRIME DIGITAL

Quando se fala em prova no direito processual penal, surgem algumas singularidades deste ramo do Direito. Neste quesito, a prova terá força para produzir no magistrado, pelo menos a certeza do que alega a parte que produziu o conteúdo probatório, seja autor ou réu, pois não basta apenas alegar os fatos, mas deve-se comprová-los, e o instituto utilizado para esse convencimento é o da prova.

Humberto Theodoro Junior (2009) classifica as provas no direito processual da seguinte maneira:

> a) um objetivo, isto é, como o instrumento ou o meio hábil, para demonstrar a existência de um fato (os documentos, as testemunhas, a perícia etc.);
> b) e outro subjetivo, que é a certeza (estado psíquico) originada quanto ao fato, em virtude da produção do instrumento probatório. Aparece a prova, assim, como convicção formada no espírito do julgador em torno do fato demonstrado (THEODORO JÚNIOR, 2009, p. 411).

Desta maneira, pode-se dizer que prova é a junção entre os documentos inseridos no processo com o estado psíquico gerado no julgador (magistrado) criando a certeza da veracidade do que foi alegado.

Em processual penal, existem, basicamente, três sistemas de avaliação e valoração das provas: o sistema tarifado, o sistema de livre convencimento, e o sistema de livre convencimento motivado (ou persuasão racional). O Brasil adota o sistema de livre convencimento motivado, pois nele, a autoridade judicial está livre para decidir e apreciar as provas que lhe são submetidas, desde que o faça de forma fundamentada, seguindo os termos prescritos no art. 93, IX da Constituição Federal, com a redação dada pela Emenda Constitucional nº 45, de 2004.

O art. 155 do Código de Processo Penal, alterado pela reforma de 1988, preceitua:

> Art. 155. O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas (BRASIL, 1941)

E, apesar da relevância da classificação supra citada, o que efetivamente interessa no ponto é o fato de que, no processo penal, nenhuma prova terá valor absoluto, sequer a confissão ou os exames periciais.

Sendo assim, esse é o fundamento do princípio da busca da verdade real, próprio da seara processual penal, em contrapartida à busca da verdade formal, inerente processo civil, porquanto naquele, diferentemente deste, está presente, de forma impositiva e prevalente sobre qualquer outro, o inafastável interesse público.

Se a prova, sob um aspecto objetivo, representa todos os meios utilizados para a comprovação dos fatos que se alegam, e de maneira subjetiva prova é a valoração que julgador dá ao que foi demonstrado no processo, de forma racional e motivada, o grande celeuma causado pela prova no crime digital é sua valoração.

A Constituição Federal de 1988 traz em seu art. 5º, os princípios constitucionais que regem a Teoria Geral das Provas, que são: devido processo legal – art. 5º, LIV, CF; ampla defesa e contraditório – artigo 5º, LV, CF; e proibição da prova obtida por meios ilícitos – artigo 5º, inciso LVI.

Como visto no capítulo anterior, as provas passam por um momento de transição, assim meios de provas utilizados no crime digital, as provas eletrônicas, por várias vezes ferem o inciso LVI do art. 5 º, CF/88, pois se utilizam dos mesmos meios ilícitos praticados pelos criminosos virtuais, muitos deles meios de invasão e obtenção de dados citados em capítulos anteriores.

Como valorar provas que podem facilmente, mediante conhecimentos simples da área, serem alteradas ou contaminadas.

Segundo o Juiz Demócrito Reinaldo Filho:

> A produção em juízo da prova eletrônica tem amparo legal em razão da regra adotada pelo nosso Código de Processo Civil, no seu artigo 332, que admite "todos os meios legais, bem como os moralmente legítimos" para a prova da verdade de fatos. Vigora, pois, no processo civil brasileiro, a regra da atipicidade dos meios de prova, significando que os fatos podem ser provados por qualquer meio, ainda que não os típicos (depoimento pessoal, confissão, exibição de documento ou coisa, testemunha, perícia ou inspeção judicial). Ademais disso, o documento eletrônico produzido de acordo com as regras da Medida Provisória 2.200-2/01, cuja autenticidade possa ser certificada por órgão competente vinculado à estrutura da ICP-Brasil, pelo sistema de chaves pública e privada, tem caráter de documento público ou particular (art. 10), presumindo-se verdadeiro quanto ao signatário (par. 1º.) (REINALDO FILHO, 2006)

Neste sentido o art. 13 da Lei 12.965/14 (Marco Civil da *Internet* no Brasil) procurou sanar uma deficiência legislativa no tocante à preservação dos dados de acesso, pois sérios são os prejuízos para uma das partes decorrentes da perda de informações potencialmente importantes se não fossem adotadas medidas para a sua preservação.

5.1 A CYBER PROVA

A criminalidade se aprimora pelo uso cada vez maior de hardwares avançados e de tecnologia da informação, resultando em crimes digitais e trazendo a tona o debate sobre a prova extraída dos meios digitais, a cyber prova.

O mundo do direito esta lidando com uma informação totalmente diferente de tudo o que, durante muito tempo, foi produzida em papel ou qualquer outro meio tangível. Imaginar o volume de informações que podem armazenadas em um HD (Hard Disk) de 1TB (Tera Byte) é o mesmo que se deparar com 500 milhões de paginas A4 de texto impresso. Empresas simples de nossa época costumam possuir servidores com dois até quatros HDs destes em uma única máquina, as vezes trabalhando espelhados como backup ou simplesmente para armazenamento de dados somados. Discos portáteis menores que muitos aparelhos celulares atuais e que tem a capacidade de armazenamento de 1bilhão de páginas de texto impresso, ou seja, 2TBs (Tera Bytes) sendo transportados em bolsos de camisas por exemplo, tornam a mobilidade destes dados, mais uma problemática para os peritos digitais, pois o *rastro* da informação pode estar presente em uma máquina, mas tal informação pode não ser encontrada, impossibilitando a finalização da perícia. E por se tratarem de informações eletrônicas voláteis, o simples ato de ligar e desligar o dispositivo pode alterar a informação armazenada.

> Os computadores quando em funcionamento reescrevem e deletam informação, quase sempre sem o conhecimento específico do operador. Uma terceira e importante característica é que a informação armazenada eletronicamente, ao contrário de textos escritos em papel, pode se tornar incompreensível quando separada do sistema que a criou (REINALDO FILHO 2006).

Tais complexidades tornam a apresentação das provas eletrônicas em juízo um caminho longo e dispendioso quando comparado a uma simples juntada de um documento/prova que fora produzido originalmente em papel. Mas como devem ser apresentadas as provas eletrônicas diante do juízo? Os magistrados possuem conhecimento para valorar as provas eletrônicas? Os peritos judiciais atualmente

possuem tal conhecimento para auxiliarem os magistrados? Uma simples intimação para apresentação de um arquivo eletrônico sem tratamento (nativo) será suficiente para que as partes e seus advogados compreendam o que nele consta, sendo que como citou Reinaldo Filho (2006), algumas informações eletrônicas são incompreensíveis quando separadas do sistema que as gerou?

O receio de se gerar insegurança jurídica quanto a prova no meio digital, ou prova extraída do mundo virtual trouxe uma maior cautela na apreciação destas, pois "em meio às especificidades da era digital a segurança da informação passa a ser aspecto fundamental para se conferir validade às provas, no que passa a merecer a atenção e o estudo por parte dos operadores do direito" (TULIO SILVA, 2012).

E como toda inovação no mundo jurídico, a falta de conhecimento técnico/específico do operador do direito sobre a área inovante, acaba por delimitar sua trajetória de aceitação.

Segundo padrões internacionais de normatização expressos na norma ABNT NBR ISO/IEC 27002, as provas colhidas em ambiente digital devem conter os seguintes atributos básicos (ABNT, 2013):

- Confidencialidade - propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.
- Integridade - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento,manutenção e destruição).
- Disponibilidade - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.
- Irretratabilidade - propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita.

Esses atributos visam garantir a segurança da informação, ou seja, proteger as informações consideradas importantes para a continuidade e manutenção dos objetivos de negócio da organização.

Ate o exposto sobre provas na fase processual, pode-se afirmar que os meios de produção de prova continuam admitindo amplas fontes de origem, porém no crime digital ganha relevância o meio de prova pericial ou computação forense, pois dele depende em boa parte a segurança da informação, então ponto crucial no combate ao crime digital.

5.2 O DIREITO PROCESSUAL PENAL E A COMPUTAÇÃO FORENSE

Questionamentos como os citados no capítulo anterior tem fortalecido a cada dia um ramo de perícia técnica, em sua grande maioria particular, conhecida como "computação forense" ou "perícia digital" ou "forense digital", uma área de pesquisas que busca investigar soluções para problemas relacionados à coleta, organização, classificação e análise de evidências digitais e que tem por principal função reconstruir o passado, constatar a materialidade e apurar a autoria de incidentes cometidos com o requinte dos bits.

> Portanto a Computação Forense tem como objetivo principal determinar a dinâmica, a materialidade e autoria de ilícitos ligados à área de informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais de crime, por meio de métodos técnico-científicos, conferindo-lhes validade probatória em juízo (ELEUTÉRIO, 2013, p.16)

A disciplina envolve técnicas e princípios para recuperar dados, utilizando diretrizes e práticas destinadas a criar uma trilha de auditoria legal. A computação forense busca, então, colher e preservar os dados obtidos, extrair informações e analisar as informações extraídas para que essas possam se tornar evidências digitais constantes do material examinado. Para isso deve respeitar alguns fundamentos necessários à validação da prova obtida, como, por exemplo, a cadeia de custódia, que é o processo de garantia de proteção da prova, cujo objetivo é assegurar sua idoneidade, a fim de evitar questionamentos quanto a sua origem ou seu estado inicial. Por isso, devem ser registrados todos os caminhos percorridos pela prova durante a persecução penal.

A Perícia digital também considera a distinção entre crime que utiliza equipamentos computacionais como ferramentas de apoio ao cometimento do delito e os crimes que usam como meio para o cometimento. São considerados crimes que utilizam equipamentos informáticos como auxilio os chamados crimes convencionais, ou seja, aqueles que existiriam mesmo sem a utilização dos equipamentos informáticos. Já os crimes que utilizam os equipamentos informáticos como meio para o cometimento dos delitos, não seriam possíveis se tais equipamentos não existissem. (ELEUTÉRIO, 2013, p.18)

Sendo o dispositivo utilizado como ferramenta ou como meio, os dados utilizados podem ser apagados pelo usuário. O tempo é um fator primordial para a recuperação de tais informações, pois as áreas que forram utilizadas para o armazenamento das informações da prática delituosa poderão ser sobrescritas

por novos dados que nada tem a ver com o crime, diminuindo, assim, a chance de recuperação da prova do crime digital.

Tudo isto corrobora para a necessidade urgente da atenção do mundo jurídico à criação de um juizado que cuide de crimes digitais, pois a influencia do tempo nestes afasta a cada minuto a possibilidade da identificação da materialidade, em alguns casos, e autoria, fazendo com que o caso concreto alcance seu objetivo de julgamento justo e imparcial.

> Em um tribunal, a autoridade irá exigir que as provas estejam sujeitas às exigências habituais para servirem de provas. O juiz pode solicitar informações de que as provas foram obtidas de forma confiável e admissível. Em alguns países existem diretrizes especificas e algumas práticas para colher provas e recuperar evidências. Na Inglaterra, por exemplo, os peritos seguem as diretrizes dos delegados de polícia que ajudam a garantir a autenticidade e a integridade das provas. O Brasil não foge a esta regra. Desta forma antes de coletar as provas você deve criar imagens do sistema investigado, guardá-los em mídias imunes a alteração, etiquetar e datar todas as provas que serão levadas sob custódia. Se você estiver investigando apenas HDs, estes devem ser armazenados em sacos antiestáticos além de tomar cuidados com calor, umidade, sujeira, etc... (GOMES ROSAS, 2012).

Embora frequentemente associada a investigação de crimes cometidos tendo o mundo digital como meio ou auxiliar, a computação forense também é utilizada em processos civis. Indenização por danos morais decorrentes de ofensas via rede social, por exemplo, são casos comuns de ações ajuizadas no Juizado Cível. Neste caso uma simples impressão ou salvamento da pagina onde as ofensas foram publicadas, cumuladas ou não de testemunhas que também tiveram acesso às referidas publicação, podem ser provas suficientes ao livre convencimento motivado do julgador da causa.

> Não há um dever de provar, nem à parte contrária assiste o direito de exigir a prova do adversário. Há um simples ônus, de modo que o litigante assume o risco de perder a causa se não provar os fatos alegados dos quais depende a existência do direito subjetivo que pretende resguardar através da tutela jurisdicional. Isto porque, segundo máxima antiga, fato alegado e não provado é o mesmo que fato inexistente (THEODORO JÚNIOR, 2009, p. 420).

Porém a causa pode ser revertida contra quem a propôs caso a prova seja critério considerado pelo juiz como afirma Theodoro Junior no primeiro volume de sua obra Curso de Direito Processual Civil:

> Inexistindo obrigação ou dever de provar para a parte, o ônus da prova se torna, em última análise, um critério de julgamento para o juiz: sempre que ao tempo da sentença se deparar com falta ou insuficiência de prova para retratar a verdade dos fatos controvertidos, o juiz decidirá a causa contra aquele a quem o sistema legal

> atribuir o ônus da prova, ou seja, contra o autor, se foi o fato constitutivo de seu direito o não provado, ou contra o réu, se o que faltou foi a prova do fato extintivo, impeditivo ou modificativo invocado na defesa (THEODORO JÚNIOR, 2009, p. 420).

Sabendo-se que tais provas, pelo exposto neste trabalho, podem ser contestadas em juízo alegando-se uma série de falhas na obtenção das mesmas, mais uma vez recorre-se à computação forense como sendo a única realmente habilitada à validação das provas que foram colocadas como duvidosas em sua produção ou conservação.

> O que percebemos no judiciário é que há uma enxurrada de laudos periciais sendo contestados por bons advogados que, com a ajuda de verdadeiros assistentes de perito e formados em tecnologia, conseguem neutralizar um trabalho investigatório em favor do seu cliente utilizando meramente os conhecimentos de tecnologia para respaldar os argumentos que derrubam um laudo pericial.
> Os peritos nomeados pelo juízo, nesses laudos periciais contestados e muitos até anulados, são pessoas de "confiança" do juízo mas sem o preparo técnico para tal. São administradores de empresas, engenheiros civis e outros profissionais de diversas áreas que só participaram no processo como perito, pois fizeram em algum momento de suas vidas uma especialização em tecnologia que, a princípio, daria um respaldo técnico (MÉDICE, 2013).

Não havendo dever de provar no processo civil, caso a contestação da prova seja relevante, cabe á parte que assumiu o risco do ônus da prova custear a validação e veracidade desta.

> Art. 33. Cada parte pagará a remuneração do assistente técnico que houver indicado; a do perito será paga pela parte que houver requerido o exame, ou pelo autor, quando requerido por ambas as partes ou determinado de ofício pelo juiz.
> Parágrafo único. O juiz poderá determinar que a parte responsável pelo pagamento dos honorários do perito deposite em juízo o valor correspondente a essa remuneração. O numerário, recolhido em depósito bancário à ordem do juízo e com correção monetária, será entregue ao perito após a apresentação do laudo, facultada a sua liberação parcial, quando necessária. (Incluído pela Lei nº 8.952, de 13.12.1994) (BRASIL, 1973).

Esta remuneração por conta do responsável pelo ônus da prova no processo civil, na maioria das vezes, impossibilita a validação da prova primeiro pela escassez da mão de obra especializada, estando esta não disponível em todas as localidades e como sugere o blog Computação Forense:

> O Magistrado, membros do Ministério Público, empresas ou pessoas físicas, nunca devem recorrer a perito que não seja habilitado em computação forense. O profissional não certificado carece dos requisitos técnicos e teóricos para a preservação da prova durante os exames, o que tornaria inválido todo o trabalho pericial (COMPUTAÇÃO FORENSE, 2010).

Segundo pelo seu custo, justamente devido a especificidade do trabalho pericial, havendo, assim, muitas desistências quando há a necessidade de se contratar perito onde o juiz se vale do parágrafo único do artigo 33 do Código de Processo Civil.

O que deve estar claro à mente do leitor deste trabalho, é que mesmo sendo a computação forense a mais indicada e confiável à vista do judiciário, mesmo ela seguindo passos citados no inicio deste capítulo e ainda outros ainda mais técnicos, específicos e complexos os quais merecem a dedicação de um trabalho exclusivo explorando sua efetiva aplicação mas que no entanto não se encaixaria na graduação aqui proposta, é que não há infalividade na obtenção das provas periciais no mundo digital.

6 CONSIDERAÇÕES FINAIS

O objetivo inicial deste ensaio científico foi o elaborar um estudo sobre a demora na resolução de crimes no ambiente virtual, os chamados crimes digitais, apoiando-se nas barreiras processuais que atravancam o prosseguimento das diversas fases dos processos relacionados a estes crimes.

Porém com o desenrolar do estudo, pode-se notar que a maior problemática encontrada neste é, durante a fase probatória, a comprovação da materialidade de alguns e a autoria da grande maioria dos casos concretos, pois a falta de mão de obra técnico/especializada dentro do poder judiciário aliada ao constante surgimento de ferramentas utilizadas para o cometimento dos delitos visando o anonimato cria tal situação.

No capitulo primeiro, pode-se notar que a globalização teve como grande aliada a *Internet* que colaborou encurtando distâncias e oferecendo serviços diversos que ajudaram a impulsionar esta realidade. Também ficou evidente a necessidade do judiciário em atentar para a falta de legislações eficientes no combate aos delitos virtuais.

Citou-se, também, o advento da Lei 12.965/14, o *MARCO CIVIL DA INTERNET*, que, ao que tudo indica, será um grande aliado do judiciário na lacuna existente mundialmente quando se fala em legislação envolvendo a rede mundial de computadores, mas que ainda não se tem doutrinas tratando deste assunto específico, por se tratar de lei muito recente, onde sua aplicabilidade ainda não pôde ser analisada com instância.

O mundo jurídico foi um dos mais relutantes na adesão a era digital, muito embora quase todo o processo fosse elaborado utilizando-se o meio digital, inclusive

a sentença, o trânsito do processo ainda era feito pela via tradicional de papeis datilografados ou impressos. Mas, não sem tempo, o judiciário acabou sucumbindo ao mundo digital, utilizados-se das ferramentas oferecidas pela rede mundial ao iniciar a migração dos processos em papel para processos digitais, aumentando a agilidade na protocolização, citação, manejo e outros que necessitassem da movimentação física dos processos, processos esses que necessitavam de espaços físicos astronômicos para seu arquivamento e que se tratando de ambiente virtual, foram reduzidos a apenas alguns metros quadrados onde os servidores do judiciário são acondicionados, inclusive com sistemas antichamas, sistemas TTF (tolerância e tratamento de falhas), backups e espelhamentos entre outras normas de segurança exigidas a um DataCenter.

O capitulo segundo trás alguns conceitos clássicos de crime na visão de alguns doutrinadores contemporâneos, apenas com o intuito de embasar as demais colocações feitas no discorrer deste trabalho.

O terceiro capítulo descreve um breve histórico do surgimento da rede mundial de computadores, seu ingresso no segmento comercial e o crescimento do número de usuários desta referida rede, a *Internet,* e a importância e força que ela ganhou e ainda vem ganhando em nosso dia-a-dia. Não é somente um acesso para consultas a sites de notícias e trocas de e-mails. Hoje se criou uma dependência lógica e física dos serviços oferecidos pela *Internet*.

Basicamente não há necessidade de se sair de casa ou local de trabalho para praticamente nada. Pode-se pagar contas, fazer empréstimos pré-aprovados, comprar desde suprimentos básicos para consumo diário, como gêneros de primeira necessidade até os mais sofisticados, roupas, calçados, pacotes de viagem, eletrodomésticos e eletroeletrônicos, veículos e assessórios, além de uma infinidade de outros serviços oferecidos. Estes avanços vem implementando em nossa rotina diária a falsa impressão de otimização do tempo que seria gasto para se realizar os mesmos trabalhos sem a utilização da *Internet*. Segundo o que foi pesquisado, o tempo de conexão do brasileiro é sete horas acima da média mundial, ou seja, outros serviços como redes sociais, salas de bate-papo, jogos online, grupos de conversação extrafunção e ofertas que aparecem como spam em páginas e e-mails acabam tomando o tempo que seria economizado com as facilidades oferecidas. O apetite voraz das empresas instiga o usuário a clicar nesse ou naquele anúncio que levam a outros sites que apresentam mais anúncios, notícias ou fofocas de última hora e assim segue a vida do nosso usuário conectado. Com 68 milhões de usuários únicos, o Brasil hoje é um país promissor e pouco explorado pelas empresas de

tecnologia, o que nos tornam alvos para a maioria delas que a cada minuto oferecem novos serviços angariando novos usuários. Mais usuários significam mais vítimas potenciais de crimes digitais que muitas vezes não se preocupam em proteger seus dispositivos informáticos.

O crime digital evolui a mesma velocidade que avança a tecnologia. Novas brechas são detectadas constantemente nos mais diversos sistemas utilizados diariamente pelos usuários da *Internet*. Exemplo disso foi o recente vazamento de fotos retiradas do sistema de backup da *Apple,* o *icloud*, onde houve o vazamento de fotos e vídeos de várias celebridades mundiais. O sistema da *Apple,* que era considerado um dos mais seguros do mundo até então, foi atacado há mais de 6 meses e só agora o resultado deste ataque foi publicado.

Este é justamente o assunto abordado pelo capítulo quarto, que analisa a evolução do crime no tempo e como o direito tem se comportado perante essa evolução.

O crime digital é parte desta evolução, que vem ganhando notoriedade com os constantes escândalos gerados através deste meio. Várias são as ferramentas utilizadas para se obter sucesso nos delitos digitais como vírus, e-mails falsos entre outros, e pode-se notar que a criatividade do criminoso vai muito além do que se imagina, surgindo novas formas delituosas a cada instante.

O problema que envolve a questão está abordado no capítulo quinto. O quesito provas no crime digital acaba por ser a vilã da história. Dificuldade na produção destas, questionamento sobre a autenticidade e possíveis posicionamentos em locais fictícios gerados por tuneis virtuais e redirecionamento de IPs tornam a prova de um crime digital a parte mais controversa da fase processual quando o delito é cometido por profissionais e não um simples comentário em rede social ou pornografia de vingança.

Outro fato relevante encontrado durante os estudos é a falta da capacidade de se dimensionar o dano gerado pelo crime digital, pois em se tratando de um ambiente virtual de alcance mundial, os danos podem ser incomensuráveis, tendo em vista a capacidade de transmissão cada vez mais veloz e a de armazenamento cada vez maior com dimensões super-reduzidas, onde se transportam milhões de informações em um chip de memória com menos de 1 cm^2.

Tudo isso conduz ao mundo da ficção não tão distante da realidade, mais diretamente para o seriado de televisão *CSI – Crime Scene Investigation* – onde a solução para estas possíveis divergências nas provas esta nos métodos, conhecimentos e técnicas dos peritos forenses que, quase sempre, encontram o caminho para a

produção de uma prova incontroversa que liga o acontecimento ao autor. Fato que já ocorre pelos crimes digitais ocorridos no Brasil, onde a maioria das provas válidas é produzida pela computação forense. Uma notícia do conceituado jornal *The New York Times* trouxe a seguinte manchete: "O Brasil está se tornando um laboratório para crimes de informática porque prolifera o crime organizado no país e as leis para prevenir crimes digitais são poucas e ineficazes", o que só vem a corroborar que o país precisa mais do que apenas tipificação delituosa. As estatísticas mostram que a criminalidade digital no Brasil bate todos os recordes comparada a outros delitos. Em 2012, 54 delitos digitais eram cometidos a cada minuto, totalizando 2.332.800 crimes digitais diários no país segundo a empresa de segurança Symantec. (JUSBRASIL, 2014).

Há a necessidade de urgente investimento na aquisição de tecnologia e preparo de policiais, especialmente no que tange ao rastreamento e coleta de provas nos crimes digitais e assim também deve ser preparado todo o poder judiciário, que hoje ainda trata os crimes digitais com a mesma burocracia dos crimes comuns.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. *ABNT NBR ISO/IEC 27002* – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. ABNT, 2013.

ANONYMOUSBRASIL.COM. *Deep Web:* o que você procura? In: Anonimous Brasil.com. Disponível em: <http://www.anonymousbrasil.com/tecnologia/deep-web-o-que-voce-procura/>. Acesso em outubro 2014

ARPANET. In: *WIKIPÉDIA*, a enciclopédia livre. Flórida: Wikimedia Foundation, 2014. Disponível em: <http://pt.wikipedia.org/w/index.php?title=ARPANET&oldid=39125362>. Acesso em: março 2014.

BRASIL. *Lei 5.869, de 11 de janeiro de 1973*.

_____. *Lei 12.965, de 23 de abril de 2014*.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. In: *Âmbito Jurídico*, Rio Grande, XV, n. 99, abr 2012. Disponível em: <http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_ artigos_leitura&artigo_id=11529&revista_caderno=17>. Acesso em ago 2014.

COMPUTAÇÃO FORENSE. Computação Forense - Cuidados com a Evidência Digital. In: *Computação Forense*. Disponível em: < http://adscomputacaoforense.blogspot.com.br/2010/09/computacao-forense-cuidados-com_8654.html >. Acesso em outubro 2014.

DIÁRIO DO NORDESTE. Rede TOR é faca de dois gumes. In: *Verdes Mares* – Diário do Nordeste. Disponível em < http://diariodonordeste.verdesmares.com.br/suplementos/tecno/materia-1.846528>. Acesso em outubro 2014.

E-COMMERCE NEWS. Brasil é quinto em ranking dos países com maior número de internautas. In: *E-commerce News*, absolutamente tudo sobre e-commerce. Disponível em <http://ecommercenews.com.br/noticias/pesquisas-noticias/audiencia-digital-do-brasil-e-maior-que-a-populacao-da-franca>. Acesso em Agosto 2014.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Márcio Pereira. *Desenvolvendo a Computação Forense*. 3ª reimpressão, Novatec Editora, 2013.

ENIAC. In: *WIKIPÉDIA*, a enciclopédia livre. Flórida: Wikimedia Foundation, 2014. Disponível em: <http://pt.wikipedia.org/w/index.php?title=ENIAC&oldid=39795960>. Acesso em: março 2014.

FARIA OLIVEIRA, Paulo Vitor. A definição de Crime. In: *Paulo Vitor Faria Oliviera*. Disponível em: <http://paulovitorf.no.comunidades.net/index.php?pagina=1855462080>. Acesso em maio 2014.

FIGUEIREDO, Elisa Junqueira. Marco Civil da *Internet* – controvérsias instantâneas. In: *Fernandes Figueiredo Advogados*. Disponível em: < http://fernandesfigueiredo.com.br/marco-civil-da-*Internet*-controversias-instantaneas/ >. Acesso em agosto 2014.

GOMES ROSAS, Dalilo Sérgio. Computação Forense. In: *Boogaloo*, 2012. Disponível em <http://serggom.blogspot.com.br/2012/01/computacao-forense.html> . Acesso em Outubro 2014.

GUILHERME, Paulo. Os 7 mais famosos vírus de computador da história. In: *TecMundo*, Julho 2013. Disponível em <http://www.tecmundo.com.br/virus/41664-os-7-mais-famosos-virus-de-computador-da-historia.htm>. Acesso em Julho 2014.

JUSBRASIL. Pornografia por Vingança. In: *Jusbrasil.com.br*. Disponível em: http://www. jusbrasil.com.br/topicos/27170452/pornografia-por-vinganca. Acesso em 05 de Outubro de 2013.

JUSBRASIL. *Brasil registra 54 crimes virtuais por minuto*. Disponível em: http://amp-mg.jusbrasil.com.br/noticias/3125198/brasil-registra-54-crimes-virtuais-por-

minuto. Acesso em 25 de Setembro de 2014.
KLEINA, Nilton. A história da *Internet*: pré-década de 60 até anos 80 [infográfico]. In: *TecMundo*, abril 2011. Disponível em < http://www.tecmundo. com.br/infografico/9847-a-historia-da-*Internet*-pre-decada-de-60-ate-anos-80-infografico-.htm >. Acesso em março 2014.

MÉDICE, Roney. Perito judicial: os obstáculos para se fazer da computação forense uma profissão. In: *Profissionais TI*, pra quem respira informação. Disponível em: < http://www.profissionaisti.com.br/2013/08/perito-judicial-os-obstaculos-para-se-fazer-da-computacao-forense-uma-profissao/>. Acesso em Outubro 2014.

MILAGRE, José Antonio. *Guerra Eleitoral na Internet*. 1ª ed. São Paulo: Edpro/ Legaltech, 2012.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. *Manual de Direito Penal I*, São Paulo: Atlas, 2012.

MORAES, Paulo Francisco Cardoso de. A vedação constitucional do anonimato aplicada à *Internet*. O papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores. In: *Âmbito Jurídico*, Rio Grande, XIV, n. 91, ago 2011. Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=9964&revista_caderno=17>. Acesso em Março 2014.

MULLER, Nícolas. O começo da *Internet* no Brasil. In: *Oficina da Net*, maio 2013. Disponível em: < http://www.oficinadanet.com.br/artigo/904/o_comeco_da_*Internet*_ no_brasil >. Acesso em outubro 2013.

PINHEIRO, Patricia Peck. *Direito Digital*. 4ª ed. São Paulo: Saraiva, 2011.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. In: *Jus Navigandi*, Teresina, ano 7, n. 58, 1 ago. 2002. Disponível em: <http://jus.com.br/artigos/3186>. Acesso em: março 2014.

REINALDO FILHO, Demócrito. A exibição da prova eletrônica em juízo: necessidade de alteração das regras do processo civil?. In: *Jus Navigandi*, Teresina, ano 11, n. 1190, 4 out. 2006. Disponível em: <http://jus.com.br/artigos/9003>. Acesso em: set. 2014.

SAFERNET. Será que a culpa é da *Internet*? In: *Crimes pela Internet*, setembro 2013. Disponível em: <http://www.crimespela*Internet*.com.br/sera-que-a-culpa-e-da-*Internet*/>. Acesso em: outubro de 2013.

SEGURANÇA UOL. O que são vírus de computador? In: *UOL segurança online*. Disponível em: < http://seguranca.uol.com.br/antivirus/duvidas/o-que-sao-virus-de-computador.html#rmcl>. Acesso em março 2014.

SOARES, Luis. Grupo Anonymous: *Quem são e como se organizam?* Disponível em: <http://www.pragmatismopolitico.com.br/2013/06/grupo-anonymous-quem-sao-e-como-se-organizam.html>, acesso em agosto 2014.

THEODORO JÚNIOR, Humberto. *Curso de direito processual civil*. Vol. I. Rio de Janeiro: Forense, 2009.

TOR (REDE DE ANONIMATO). In: *WIKIPÉDIA*, a enciclopédia livre. Flórida: Wikimedia Foundation, 2014. Disponível em: <http://pt.wikipedia.org/w/index.php?title=Tor_(rede_de_anonimato)&oldid=39738428>. Acesso em: set. 2014.

TÚLIO SILVA, Marco. Ciberprova: O processo penal na era dos crimes digitais. In: *Webartigos*, maio 2012. Disponível em: <http://www.webartigos.com/artigos /ciberprova-o-processo-penal-na-era-dos-crimes-digitais/89599/#ixzz3EcN7xkFd>. Acesso em Setembro 2014.

VIANA, Túlio Lima. Dos crimes por computador. In: *Mundo jurídico*, abril 2003. Disponível em: < www.mundojuridico.adv.br/cgi-bin/upload/texto259.rtf>. Acesso em Julho 2014.