Aspectos legais da Perícia Forense Computacional em um cenário de Cloud Computing

Caio César Carvalho Lima

***Resumo*—O presente artigo pretende abordar a noviça questão que diz respeito aos aspectos legais da Perícia Forense Computacional, em um cenário de Computação em Nuvem. Consoante se observará, cumpre sejam realizadas alterações na legislação hodiernamente em vigor, tendo-se em conta a modificação por que a sociedade passou, a qual não foi acompanhada pari passu pelos diplomas normativos. E isso necessita ser feito com relativa urgência, uma vez que os temas aqui examinados não são parte de um futuro incerto, mas já estão presentes no quotidiano de inúmeras pessoas. Dessarte, acaso esses pontos não sejam examinados com a devida cautela, danosas consequências podem ser infligidas à população, de um modo geral, o que, decerto, não é o que se espera.**

Palavras-chaves: Digital; Computação Forense; Computação em Nuvem; Investigação Digital.

Abstract—This article seeks to address the novice question related to the legal aspects of Computer Forensics in a Cloud Computing scenery. As it will be shown, changes in legislation are needed, taking into account society changes which were not accompanied by law pari passu. It needs to be done with relative urgency, since the issues discussed here are not part of an uncertain future, but are already present in the everyday lives of countless people. Thus, if these aspects are not verified, harmful consequences can be inflicted to the general population, which certainly is not expected.

***Keywords*—Computer Law; Computer Forensics; Cloud Computing; Digital Investigation.**

1. Introdução

Certo é que, ultimamente, a utilização de recursos da Tecnologia da Informação vem crescendo de forma bastante expressiva. Dados de 30 de junho de 2010 dão conta de que foi superada a marca de 1,96 bilhão de usuários na Internet no mundo [1], número que, atualmente, deve estar em algo próximo de 2 bilhões. Com isso, é autorizada a conclusão de que é esse o principal recurso pelo qual se tem manifestado essa crescente utilização de mecanismos tecnológicos.

Isso foi o resultado, consoante se observa na obra de Manuel Castells, das confluências "de uma mistura única de estratégia militar, grande cooperação científica, empreendedorismo tecnológico e inovação contracultural" [2]. Está-se no que se convencionou chamar de Sociedade da Informação Convergente.

E nesse contexto forjou-se a novel questão da Computação em Nuvem, que, em apertada suma, representa a possibilidade de que, com a utilização da Internet, tenha-se o acesso a dados, informações, *softwares*, dentre outros, sem que eles sequer estejam armazenados no computador que realiza a comunicação com a Rede das Redes. Observe-se que a ideia não é puramente noviça, podendo-se recuperar resquícios de seu uso, desde a década de 90 do século passado [3].

A máxima expressão desse mecanismo representa a desnecessidade de que sejam utilizados discos rígidos para armazenar arquivos nos computadores. Possibilidade há de que nem mesmo o Sistema Operacional precise estar gravado no disco das máquinas.

Atualmente, seguindo a tendência do forte crescimento do uso de mecanismos de tecnologia da informação, cumpre observar que o número de transações bancárias realizadas *online* superou aquelas ultimadas em ambiente físico, tendo-se constatado que quase 50 milhões de brasileiros se utilizaram desses serviços no ano de 2009 [4]. Ocorre que, à medida que aumentou a utilização da Rede Mundial de Computadores, os criminosos também passaram a cometer suas infrações nesse meio virtual.

A fim de verificar a consumação de um delito em meio eletrônico, utiliza-se da Perícia Forense Computacional, que serve à investigação minuciosa de quaisquer dados gravados nas máquinas *sub examine*, não havendo, frise-se, sua restrição à averiguação de crimes. Em se tratando da Computação em Nuvem, entretanto, esse procedimento não mais terá grande índice de sucesso, caso continue a ser realizado nos moldes hoje processados, consoante se examinará adiante.

Desse modo, necessário se faz que seja estudado como se fará para proceder à Perícia Forense de uma máquina, cujo usuário, utilizando-se da *Cloud Computing*, concentre todos os seus dados em *data centers*, os quais, geralmente, são localizados fora do âmbito de atuação direta da jurisdição brasileira.

Surge, pois, também, implicação para os legisladores, juízes e operadores do Direito, que devem estar atentos a essa nova demanda, sob pena de deixar-se um flanco aberto à prática criminosa, por não conseguir, a produção legislativa, acompanhar *pari passu* a evolução da tecnologia da informação.

Acaso se efetive a utilização dos mecanismos de Computação em Nuvem, de pouca utilidade será a apreensão

de um computador, como hodiernamente ocorre na grande maioria dos casos envolvendo investigação digital, já que as informações buscadas não estarão armazenadas diretamente no interior da máquina apreendida.

Esse fator representará mais um desafio aos diversos profissionais responsáveis pela análise e pelo combate de crimes cibernéticos, que precisarão se qualificar ainda mais, a fim de que passem a dominar, também, essas novas técnicas.

Melhor investigação prévia será necessária para que se consiga traçar, de forma exata, o meio utilizado pelo possível criminoso para armazenar seus dados. Acaso possível e necessário, ter-se-á que conseguir até mesmo autorização do poder Judiciário do local de guarda dessas informações ou da respectiva autoridade responsável, para que essas informações sensíveis sejam liberadas, possibilitando que se obtenha sucesso na investigação, como mais à frente será analisado.

Passa-se a fazer análise rápida da Computação em Nuvem e da Perícia Forense Computacional, examinando-se, ao final do trabalho, o que diz respeito aos aspectos legais que envolvem o estudo em conjunto desses mecanismos aqui referenciados.

2. Perícia Forense Computacional: Abordagem Analítica e Técnica

Antes de adentrar, especificamente o foco do presente estudo, necessário se faz que os aspectos basilares do instituto da Perícia Forense Computacional sejam trazidos, a fim de que melhor possa ser compreendida a temática, tornando mais inteligível a efetivação das considerações a que se pretende chegar.

2.1. Aspectos Basilares da Perícia Forense Computacional

Iniciando a abordagem recorrendo-se ao conceito de perícia, em abordagem mais abrangente, tem-se que ela é a averiguação minuciosa, de caráter técnico, feita por profissional com informações específicas sobre o objeto estudado, para suprir a insuficiência de conhecimentos da parte que requereu o exame. Apresenta, como meio de prova, valor relativo, podendo o juiz desconsiderar as conclusões do perito.

Assim, a Perícia Forense Computacional abrange desde a colheita até o exame técnico de dados obtidos em quaisquer computadores, e que servem como meio de prova em certo processo judicial. Em outras palavras, considerada em sentido *lato*, "(...) perícia forense é a aquisição, preservação, análise e apresentação de evidências relacionadas à Informática" [5].

Interessante observar que, com a noviça questão da Computação em Nuvem, termo que adiante será melhor explicitado, em breve, não se precisará gravar as informações necessárias na própria máquina em que se está, podendo elas estar na "nuvem", possibilitando-se que essas informações sejam acessadas de qualquer ponto do universo – ou até mesmo fora do Planeta Terra, levando-se em consideração a tecnologia desenvolvida pela Agência Espacial Norte-Americana (NASA), que permite o acesso de dados em espaçonaves –, por meio de computadores, de celulares ou de aparelhos de televisão com conexão à Internet.

Em certos casos, pois, a fim de efetivar-se a colheita dos elementos para uma investigação pericial, far-se-á necessário não a simples apreensão da máquina buscada, mas sim que se realizem estudos cautelosos com o fito de confirmar em qual central de dados estão sendo armazenadas as informações daquele terminal averiguado, devendo-se nela ser efetuada a colheita do material que será objeto da investigação.

Decerto que, com essas alterações, exsurge a necessidade de que os métodos de análise hoje em prática sejam repensados, a fim de que a repressão à prática criminosa continue, sob pena de se verificar elevação no número de condutas delituosas perpetuadas por meio da Rede.

2.2. Importância Crescente da Perícia Forense Computacional em Razão da Elevação da Quantidade de Dados Eletrônicos Gerados

Com o transcurso do tempo, tem-se observado elevação contínua da dependência da população mundial em relação às inovações da Tecnologia da Informação e da Comunicação (TIC). O quotidiano já se encontra permeado de tantos aparelhos tecnológicos que muitos não conseguem imaginar suas vidas sem essas novidades. Aí se incluem Internet móvel, smartphones, computadores pessoais, leitores digitais, televisão digital interativa, dentre outros. Daí porque se diz que hodiernamente se vive em uma "Sociedade Digital" ou em uma "Sociedade da Informação" [6].

Depara-se com uma comunidade em que a aquisição, o registro e a replicação daquilo com que se tem contato – quer seja uma simples conversa com amigos ou até mesmo dados mais sensíveis, como transferências bancárias, consultas médicas ou a lista de medicamentos a serem prescritos para um paciente internado em uma Unidade de Terapia Intensiva (UTI) –, são feitos através de mecanismos que se utilizam da tecnologia.

Com esse modelo, elevou-se à categoria de bem de valor mais importante o conhecimento, o qual é intangível, daí derivando o conceito de Capital Intelectual [7]. Desse modo, surge clara diferenciação entre o que antes se observava durante as Revoluções Agrícola e Industrial, em que a força física do homem era que apresentava maior valoração, cabendo ao Estado o controle dos meios de produção.

Decerto, hoje o processamento se dá de maneira diversa. Fator marcante dessa nova sociedade é a velocidade com que as alterações ocorrem, exsurgindo grande necessidade de sempre se estar atento a elas, sob pena de impossibilidade no acompanhamento dessa evolução. É nesse ambiente de rápidas modificações que se insere a questão aqui enfocada.

Assim, com o crescimento vertiginoso dos mecanismos virtuais, observa-se, também, maior necessidade de que a segurança daquilo que se realiza nesse meio seja garantida, fazendo-se mister o avanço das técnicas de forense computacional.

Apenas exemplificando um dos fatores dessas importantes inovações relatadas, observe-se que já há certo tempo que as técnicas investigativas se encontram sobremaneira evoluídas, já havendo a possibilidade da extração de provas digitais em computadores queimados e em aparelhos encontrados no fundo de um lago, por exemplo [8]. Isso apenas traz a constatação de que as pesquisas estão sendo realizadas de maneira proveitosa.

Dessarte, levando-se em conta a crescente importância desse instituto, a seguir faz-se análise mais aprofundada de suas balizas principais, não sendo, entretanto, o escopo do presente trabalho descer a todos os detalhes sobre a temática, recomendando-se para tanto a leitura de obras específicas.

2.3. Da Validade Jurídica de Documentos Produzidos em Meio Eletrônico

Especificamente tratando da Perícia Computacional, tem-se que ela corresponde à coleta e à posterior análise dos arquivos objeto da investigação. Ato contínuo, de posse do material a ser peritado, utilizando-se de ferramentas apropriadas, o expert faz o estudo da evidência coletada e, empós, apresenta seu laudo, que mostra, para o magistrado, se houve, ou não, alguma modificação do arquivo sub judice.

Convém observar que, em se tratando de documentos eletrônicos que serão utilizados como meio de prova em processo judicial, é de fundamental necessidade a juntada aos autos da fonte em que se originou o objeto a ser periciado.

Assim, se impugnado um e-mail, verbi gratia, pouco valerá, em razão da ampla chance de adulteração, anexar ao processo cópia daquele documento eletrônico, devendo-se possibilitar a realização da perícia no disco rígido em que o mesmo foi gravado.

Observe-se que há possibilidade de que se faça necessário o estudo nos servidores por meio dos quais a mensagem trafegou, desde o seu envio até o seu recebimento, caso não estejam esses dados registrados no disco do computador, o que se torna cada vez mais comum com a utilização dos mecanismos da Computação em Nuvem.

Em geral, quando bem efetivados os procedimentos periciais, os índices de sucesso são bastante elevados, especialmente quando realizado em computadores, pois eles guardam bem mais informações do que se pensa, sendo, efetivamente, bastante difícil a remoção completa de um dado nele gravado [9].

Minuciosa metodologia deve, pois, empreender o profissional com o mister de assegurar que a evidência não seja alterada ou até mesmo perdida. Diferentes necessidades implicam diversos métodos de estudo dessas provas coletadas, dependendo da habilidade do perito a melhor solução para o caso.

A regra de ouro desse procedimento, independentemente da opção do profissional, é a preservação das evidências de tal forma que não se opere qualquer dúvida acerca da sua veracidade. Para que seja garantido tal intento, fundamental o cumprimento de alguns requisitos básicos trazidos pela doutrina especializada, incluindo, mas não se limitando a:

> a) se possível, criar imagens dos discos investigados, também conhecido como duplicação parcial [consiste em criar uma imagem, cópia perfeita, de um sistema], para que as evidências digitais possam ser depois analisadas;
>
> b) se o caso necessitar de análise ao vivo [perícia realizada no equipamento investigado ainda em funcionamento], salvar as evidências em discos e bloqueá-los contra regravação; e
>
> c) lacrar em sacos com etiquetas todas as evidências [10].

Observa-se, pois, que, nas orientações anteriormente relatadas, sobressalta a necessidade da máxima proteção dos dados originais, que devem permanecer em estado puro, realizando-se, sempre que possível, a perícia apenas na cópia dessas informações, reduzindo ao mínimo possível a possibilidade de apagar ou de danificar o arquivo-matriz. Desse modo, observa-se que é possível a verificação de modificações efetivadas em documentos eletrônicos, acaso sejam eles resguardados em seu estado puro.

Verifica-se, assim, que não há razões para, com a tecnologia hoje disponível, ainda haver desconfiança relativa à documentação digital, como outrora existia. Apenas ratificando esse entendimento, fundamental observar que o Anteprojeto do novo Código de Processo Civil pátrio, tornado público em junho do ano de 2010, já traz uma seção que trata especificamente da questão da documentação eletrônica, a ela atribuindo plena eficácia [11].

Por fim, fundamental observar os Enunciados 297 e 298, produzidos na III Jornada de Direito Civil, promovida pelo Centro de Estudos Judiciários do Conselho da Justiça Federal, no ano de 2007:

> Enunciado 297 – III Jornada de Direito Civil
>
> Art. 212 [do Código Civil]: O documento eletrônico tem valor probante, desde que seja apto a conservar a integridade de seu conteúdo e idôneo a apontar sua autoria, independentemente da tecnologia empregada.
>
> Enunciado 298 – III Jornada de Direito Civil
>
> Arts. 212 e 225 [do Código Civil]: Os arquivos eletrônicos incluem-se no conceito de "reproduções eletrônicas de fatos ou de coisas" do art. 225 do Código Civil, aos quais deve ser aplicado o regime jurídico da prova documental.

Acredita-se serem essas as principais características que precisam ser dominadas sobre a questão suso referida,

a fim de que se consiga compreender o tema adiante examinado.

3. Computação em Nuvem: Análise dos Aspectos Básicos

A seguir, passa-se a realizar análise perfunctória dos aspectos básicos da Computação em Nuvem, a fim de que, ao se estudar as influências desse instituto na Perícia Forense, não haja maiores dificuldades no entendimento. Almejando traçar um conceito inicial sobre o tema, fundamental trazer à colação o escólio de Taurion:

> (...) Computação em Nuvem é um termo para descrever um ambiente de computação baseado em uma imensa rede de servidores, sejam estes virtuais ou físicos. Uma definição simples pode então ser "um conjunto de recursos como capacidade de processamento, armazenamento, conectividade, plataformas, aplicações e serviços disponibilizados na Internet". O resultado é que a nuvem pode ser vista como o estágio mais evoluído do conceito de virtualização, a virtualização do próprio *data center*. [12]

Isto é, como acima já referido, não se precisará gravar os dados e informações comumente consultados na máquina utilizada, já que eles estarão na "nuvem", podendo ser acessados, de qualquer lugar do mundo, através de um computador, celular ou televisão com conexão à Internet. Essas informações estarão armazenadas em *datas centers*, poderosas centrais de processamento de dados, estando pouco ou quase nada no equipamento.

A máxima evolução desse mecanismo é alcançada quando tudo está na "nuvem", até mesmo o *software* principal do computador, o chamado Sistema Operacional, como o *Windows* ou o *Linux*, por exemplo.

A utilização da *Cloud Computing* está crescendo expressivamente a cada dia. Confirmando a importância do assunto tratado, em 2008, o valor gasto no mundo com Computação em Nuvem foi da ordem de 16 bilhões de dólares. Em 2012, espera-se que essa cifra atinja cerca de 42 bilhões de dólares, o que representa aumento de 27% na utilização dessa tecnologia, em apenas quatro anos [13].

Importante observar que dentre as características dessa nova aplicação, destacam-se a elasticidade, a escalabilidade e o pagamento por utilização.

Por elasticidade, entende-se a possibilidade de utilização dos recursos na exata medida em que eles forem necessários, podendo ser aumentada ou diminuída a capacidade, de forma dinâmica. Quanto à escalabilidade, grosso modo, pode-se entendê-la como sendo a capacidade para alocar recursos de processamento, disco, memória ou banda individualmente e sob demanda. Em relação a esses serviços, o pagamento ocorre de forma variável, conforme a utilização efetiva deles.

Observa-se, pois, que um dos pontos-chave do instituto em apreço diz respeito à possibilidade de pagamento consoante a utilização. Isto é, o uso dos recursos, por parte dos computadores em nuvem, flutua conforme a demanda efetivamente requisitada, sendo o adimplemento dos valores proporcional à parcela efetivamente consumida.

E essa "nuvem" apresenta diversos tipos de serviços, dentre os quais se inclui o SaaS (*Software-as-a-Service* - Programa de Computador como Serviço), que pode ser entendido basicamente como a capacidade de ter um programa de computador implementado como serviço hospedado em um *data center*, sendo acessível pela Internet, trazendo grande economia relativamente à infraestrutura. Como exemplos, pode-se referir ao *Zoho* e *ao Google Docs*.

Frise-se que isso não é algo distante, havendo pesquisas no sentido de que, neste ano de 2010, aproximadamente "65% das empresas norte-americanas terão pelo menos uma aplicação rodando no SaaS" [14].

Passa-se a pagar o *software* como se um serviço prestado ele fosse, não havendo mais que se falar em licenciamento para o terceiro adquirente – isto é, a licença se dá entre o provedor de serviços e a empresa que elaborou o logiciário. Em verdade, vendem-se os serviços de um sistema para um terceiro, sem que o programa de computador em si seja repassado – tal mecanismo, convém destacar, não condiz com os atuais mecanismos de licenciamento permitidos pela Lei de *Softwares* (Lei Nº 9.609/1998) e pelo Código Civil, fugindo a análise dessa questão do foco do presente trabalho. Nesse sentido, segue Taurion:

> SaaS está relacionado com a funcionalidade da aplicação, entregue via modelo de subscrição pela Internet. O cliente não precisa ter a "propriedade" do *software*. (...) No SaaS, ele não "possui" o *software* e adicionalmente não precisa se preocupar com a tecnologia em que o *software* vai operar. (...) *Software-as-a-service* é um modelo disruptivo. Sua proposição de valor é a funcionalidade oferecida e não a "propriedade do produto". (...) O cliente não adquire licença de uso, mas paga uma taxa mensal baseada no número de funcionários que acessem o serviço. SaaS, por ser um modelo disruptivo, vai afetar toda a estrutura da indústria de *software* [15].

Assim, os programas comerciados pelos provedores dos serviços são a eles licenciados, e não à terceira parte que os utilizará. Diante desse licenciamento, os detentores negociam os direitos que possuem sobre o *software* a terceiros, adquirentes dos serviços da Computação em Nuvem.

Nessa transação, várias são as formas de efetivação, sendo certo, no entanto, que do cliente será cobrado tão somente o serviço efetivamente usado, quer seja relativamente ao número de acesso, tempo de uso, número de estações, dentre outros. Há, também, a possibilidade de entabular-se acordo de utilização mediante um valor fixo mensal, bimestral, semestral, podendo ser estipulado uso ilimitado nesse

período, enfim. As partes livremente formam o negócio da maneira que melhor lhes aprouver.

Outro aspecto dessa inovação diz respeito à PaaS (*Plataform-as-a-Service* – Plataforma como Serviço), a qual está representada pela disponibilização de um ambiente no qual os desenvolvedores de programas têm espaço destinado à elaboração de aplicações destinadas a operar sob o modelo de *Cloud Computing*. Atualmente, esses serviços estão acessíveis no *Windows Azure, Google, Sales Force*, dentre outros.

Há, também, o IaaS (*Infrastructure-as-a-Service* – Infraestrutura como Serviço), o qual consiste na disponibilização de *hardware*, via *web* aos usuários. Uma das formas mais utilizadas desse serviço está presente na utilização de máquinas para armazenamento de informações. Grandes empresas, como a *Amazon*, a IBM, e a *Sun Microsystems* já fornecem esse tipo de utilidade. Seu grande diferencial está no fato de que, com o pagamento de pequena quantia, tem-se acesso às mais modernas tecnologias disponíveis.

Existem ainda outras modalidades, tais como DaaS (*Database-as-a-Service* – Banco de Dados como Serviço) e BaaS (*Backup-as-a-Service*, Cópia de Segurança como Serviço), cuja análise extrapola os objetivos do presente estudo.

4. Aspectos da Forense Computacional em Um Cenário de Cloud Computing

Pelo que acima se trouxe, percebe-se que quando se têm, simultaneamente, os aspectos referentes à Perícia Forense em um cenário de *Cloud Computing*, ambos os polos envolvidos nessa relação encontram-se com questionamentos difíceis de serem solucionados.

Tanto os peritos quanto os aplicadores do Direito carecem de melhor regramento para especificação das atitudes que devem tomar quando se depararem com situações como as aqui enfrentadas.

4.1. A Privacidade Contratual e a Realização de Cópias de Segurança

Em primeiro lugar, cumpre analisar o que diz respeito à possibilidade de acesso a dados sigilosos guardados na "nuvem", por parte de malfeitores.

Certo é que, a despeito de previsões contratuais acerca do sigilo das informações, inúmeros são os incidentes relatados acerca de "vazamentos" na Internet que se operam de modo ilegal, em razão do ingresso não autorizado em diretórios privados, protegidos contra a entrada livre de terceiros. Por esse motivo, grande parte das críticas dirigidas às ferramentas de Computação nas Nuvens diz respeito exatamente à segurança das informações [16]

Tendo-se em conta a grande dificuldade existente para conseguir comprovar a origem do acesso, aliado ao fato de que o próprio sistema de Computação em Nuvem pode ser utilizado pelo contraventor para propagar as informações a que teve acesso, mais uma vez, esbarra-se em situação que foi dificultada, em razão das inovações da Cloud Computing, não estando as técnicas de Forense suficientemente desenvolvidas para, em curto lapso temporal, solucionar o caso posto a apreciação.

Desse modo, um dos bens intangíveis protegidos pela Carta Máxima da República, a honra, pode ser aviltada sem que se consiga rastrear a origem desse crime.

Importante observar, de igual modo, que, até mesmo a cópia de segurança que precisa ser realizada pelos peritos forenses computacionais, a fim de iniciar o estudo sobre os dados coletados será mais difícil. Isso decorre do fato de que, como se sabe, necessária se faz a efetivação do procedimento hash sobre o conteúdo antes e depois de efetuada a duplicação dos discos que serão examinados.

A função hash consiste em um método matemático utilizado, exemplificativamente, com a intenção de possibilitar a confirmação da integridade das partes de uma mensagem transferida, isto é, visa-se confirmar que não foram alterados os dados durante a sua transmissão.

Uma característica marcante do hash é que ele é unidirecional, não havendo possibilidade de retornar ao arquivo original, a partir do código hash. Isso ocorre, pois o hash é tão somente um resumo do documento, apresentando, via de regra, o mesmo tamanho independentemente do volume do arquivo em que ele é aplicado.

Fazendo-se uma analogia, pode-se dizer que o hash funciona como os dígitos verificadores, que têm a função de confirmar que nenhum erro de digitação foi cometido na transcrição de certo número – no presente caso, almeja-se confirmar não ter havido sequer mínima alteração no conteúdo da mensagem.

Impende ainda informar que o hash gerado deve ser sempre único, isto é, ímpar, não havendo igualdade para outro arquivo, ainda que a diferença entre eles seja de apenas um espaço em branco, por exemplo.

Assim, partindo-se do pressuposto de que a Internet é um ambiente dinâmico, em que atualizações podem ser feitas a qualquer momento, existe possibilidade de que, caso seja necessário grande tempo para duplicar todas as informações que serão estudadas, o indivíduo altere, nesse interregno, algum conteúdo daquela pasta virtual que está sendo transferida, terminando por haver a invalidação da aplicação do hash de conferência, tornando facilmente anuláveis as conclusões às quais o perito chegar, já que não se conseguirá comprovar a integridade da cópia de segurança efetivada.

Acresça-se a isso o fato de que instabilidades no servidor, tanto no de origem, quanto no de destino, podem causar ruídos que terminem por alterar, de algum modo, as informações dos arquivos copiados, provocando, mais uma vez, a invalidação do seu conteúdo.

Ademais, a realização de uma Cadeia de Custódia também estará comprometida, já que será difícil se garantir que apenas os peritos tiveram acesso àquela informação. Por meio da Cadeia de Custódia se "prova onde as evidências estavam em um determinado momento e quem era o responsável por elas durante o curso da perícia" [17].

Está-se, desse modo, diante de diversos empecilhos que terão de ser enfrentados pelo perito que trabalhará com uma evidência em um cenário de Computação em Nuvem.

4.2. Tempo e Local dos Cibercrimes: Necessidade de Cooperação Internacional

Têm-se questionamentos acerca de dois aspectos que precisam ser bem analisados, relativamente a quaisquer delitos, quais sejam, o local e o tempo dos crimes. Em se estando diante de crimes cibernéticos a atenção quanto a esses quesitos precisa ser ainda maior. O Código Penal trata da temática em seus arts. 4º e 6º:

> Art. 4º - Considera-se praticado o crime no momento da ação ou omissão, ainda que outro seja o momento do resultado.
>
> Art. 6º - 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.

Sobre o tempo do crime, três são as teorias existentes. O Brasil se filiou à Teoria da Atividade, que considera como tempo do crime o momento da ação ou da omissão, ainda que em outra oportunidade seja efetivado o resultado.

Há, ainda, a Teoria do Resultado (ou do efeito), que tem como tempo do crime o momento de sua consumação, independentemente de quando tenha se dado a ação ou omissão que carrearam ao resultado; bem como a Teoria Mista, que considera como tempo do crime tanto o momento da conduta, quanto o do resultado.

Entende-se que, em se tratando de Direito Eletrônico, razão não há para que sejam feitas modificações nesse entendimento já consolidado sobre o tempo do crime, devendo-se dar continuidade àquilo já praticado.

Grande diferença reside no que pertine ao local em que o crime foi praticado. Existem, também, três teorias sobre o tema. A aplicada atualmente no ordenamento brasileiro, Teoria da Ubiquidade, posiciona-se no sentido de que o lugar da conduta criminosa pode ser tanto aquele em que ocorreu a ação ou omissão, como aquele em que o resultado foi produzido. Com esse entendimento, possibilita-se que, mesmo naqueles crimes em que a conduta ocorre no Brasil e o resultado se dá em outro país, ou vice-versa, seja a justiça pátria competente para julgá-los.

Há ainda a Teoria da Atividade, que considera como local do crime aquele em que houve a ação ou omissão, ainda que o resultado ocorra em outro espaço; bem como a Teoria do Resultado, que, de outra banda, como seu nomen juris expressa, tem como local do crime, onde houve a consumação do resultado.

Convém observar que os cibercrimes rompem com esse tradicionalismo metódico, na medida em que existe possibilidade de que sejam praticados, simultaneamente, em diversos países, podendo em cada um deles serem efetivadas condutas diversas, sendo viável que o autor dos delitos esteja localizado em nação diferente de todas aquelas em que suas atitudes tomam efeito.

Ademais, acresçam-se algumas diferenças que podem ser constatadas, quando se faz o cotejo entre os crimes praticados em ambiente físico e em meio virtual, atentando-se para: "a velocidade com a qual o crime é praticado; o volume de dados e/ou a quantia de dinheiro envolvidos; e a distância a partir da qual ele pode ser cometido" [18].

Com isso, exsurge a necessidade de redefinição no que diz respeito à busca e apreensão de máquinas, aliada à questão da competência das polícias e dos juízes. Explica-se: atualmente, com a possibilidade de alocação de grande quantidade de informações na Internet, a simples apreensão do computador pode ser infrutífera para os fins de ultimar-se investigação pericial, como anteriormente já se aludiu.

Como os dados estarão em ambiente virtual, necessário se faz que se tenha acesso às informações que serão objeto da perícia em seu estado puro. Com isso, surge o conceito de busca e apreensão online. Há a possibilidade, pois, que o cumprimento de mandados passe a se dar sem que seja necessário sair dos ambientes de trabalho, bastando para tanto uma máquina com conexão à Internet.

Ocorre que esse procedimento não pode ser efetivado sem que as mínimas garantias constitucionais sejam preservadas, sob pena de as provas obtidas serem ilícitas, fragilizando, ou às vezes, impossibilitando, a condenação do indivíduo investigado.

Imagine-se, verbi gratia, a situação da autoridade policial que, sabedora da prática de ilícitos com a utilização da Internet para guarda dos dados que poderiam comprovar o crime, resolva, sponte propria, adquirir essas informações na Grande Rede.

Acaso essa tentativa de coleta de dados se dê em relação a informações cujo armazenamento esteja sendo feito em servidores fora do Brasil, algumas situações-problema podem ser evidenciadas e precisam ser melhor analisadas, a fim de que sejam evitados ulteriores questionamentos quanto à validade das provas obtidas.

Caso se consiga ter acesso ao próprio computador do criminoso, por meio de uma perícia *online* ao vivo – situação possível quando se consegue pegar o criminoso no momento em que ele tenta obter as informações na Rede das Redes, estando ainda com a máquina que intermedeia esse acesso ligada, com todos os *logins* e senhas necessários à verificação do conteúdo das pastas em que as informações estão armazenadas na "nuvem" já digitadas – ou se alcance, por meio do computador pessoal do Perito,

as informações desejadas, certamente a prova obtida violará as regras constitucionalmente trazidas no art. 5º da Magna Carta, ainda que com prévia autorização judicial, já que a autoridade que proferiu a decisão será territorialmente incompetente.

Entende-se que a única maneira de ser tida como válida uma prova assim obtida dá-se quando a autoridade investigadora, contando com permissivo emitido por Magistrado pátrio, não tem ciência de que a informação acessada está localizada em servidor fora da jurisdição nacional, o que, na maioria dos casos, não ocorre, já que a investigação prévia conduz a um completo estudo sobre a cena do crime, sendo essa questão, geralmente, levantada logo no início dos estudos.

Isso, contudo, não representa entendimento uníssono, já que vozes há que se insurgem em sentido contrário, consubstanciadas nos artigos 70 e 88 do Código de Processo Penal, que abordam, em síntese, a questão da competência para o julgamento de crimes realizados fora do âmbito do território brasileiro [19].

Diante disso, é clara a necessidade de que a cooperação internacional exista, a exemplo do que já se vem tentando com a Convenção de Budapeste, sob pena de proliferação dos crimes eletrônicos, já que haverá consolidação do existente pensamento no sentido da "inexistência de leis" no âmbito da Internet.

4.3. Das Dificuldades Decorrentes da Ausência de Legislação Internacional

Outro grande questionamento que vem à mente, diz respeito ao fato de que, em razão da crescente utilização da Computação em Nuvem, em pouco tempo, não só os dados, como a infraestrutura, os softwares, os bancos de dados e diversos outros aspectos passarão a ficar hospedados na nuvem.

Diante desse novo cenário, a simples apreensão de uma máquina seguida da investigação do seu conteúdo pode pouco, ou até mesmo nada, resolver para a solução de certo caso estudado, consoante anteriormente já analisado.

Ora, se o computador será basicamente um entreposto entre o usuário e a "nuvem" em que todos os seus dados estão salvos, certamente, quase nenhum rastro ficará disponível nessa máquina.

Com isso, surgirá como de fundamental importância a realização de uma prévia e robusta investigação levada a efeito pelos entes policiais, a fim de que se consiga traçar as rotas utilizadas pelo investigado para ter acesso ao material cujo conteúdo está sub examine.

Eis então que surge outro grande desafio: na maior parte dos casos, as informações estão armazenadas em servidores que não se encontram no local em que o criminoso está fisicamente. Isto é, utilizando-se como exemplo um infrator sito no Brasil, grande será a possibilidade de que ele esteja se utilizando dos serviços de armazenamento de empresas localizadas em países diversos.

Surgirá, então, a necessidade de que, antes mesmo da efetiva apreensão do suspeito, seja expedida ordem para que o Juiz da jurisdição em que está havendo a gravação das informações determine à empresa de hospedagem que as forneça.

A Internet tem apresentado grande crescimento, já sendo, como se disse ab initio, quase 2 bilhões o número de usuários conectados. Em razão dessa magnitude, os criminosos visualizaram grande espaço para diversificar seu campo de atuação, passando a agir ativamente na Grande Rede.

Abriu-se novo flanco para a atuação criminosa, passando-se a cometer aquilo que antes era feito no mundo físico no "mundo virtual" [20]. A sociedade, pois, está exposta a inúmeras ameaças que levam a um comprometimento da segurança das informações, dos dados, de dinheiro e até mesmo da vida, tendo-se em conta que, hodiernamente, hospitais há em que o controle dos medicamentos do pacientes é feito à distância, nos termos anteriormente já traçados.

Em razão disso, observa-se vertiginosa elevação do gasto das empresas com a segurança dessas informações, com o fito de mantê-las protegidas contra terceiros mal intencionados. Isso, contudo, não é suficiente, esbarrando-se em fatores limitativos, como a ausência de dispositivos legais que tracem a regulamentação básica para os crimes na Internet.

Isso não significa, contudo, que o Direito Penal deve ser totalmente reformulado. Pelo contrário. É de amplo conhecimento que esse ramo da ciência do Direito representa a ultima ratio. Isto é, só se deve a ele recorrer empós o esgotamento de todos os outros modos de solucionar a questão.

Essa característica presente no ramo do Direito antes referido é decorrência do Princípio da Intervenção Mínima ou da Subsidiariedade. Não se está pregando, frise-se, que não devem ser regradas as condutas criminosas efetivadas no ambiente da Internet. Ao reverso, defende-se que a sistemática Penal deve ser utilizada, mas tão somente quando o Direito Civil e o Direito Administrativo não conseguirem estancar as decorrências danosas levadas a efeito pelos cibercriminosos.

Assim, tendo-se em conta a grande mudança de paradigma evidenciada com a Sociedade da Informação, exsurge a necessidade de que alguns tipos penais sejam repensados, a fim de que prevejam as novas formas por meio das quais crimes antigos podem ser efetivados.

Não se pode olvidar, outrossim, da eventual necessidade de criação de novos tipos penais, na medida em que condutas antes não pensadas pelo legislador, ou tidas até então como irrelevantes penais, precisam ser contidas, sob pena de preocupantes consequências serem infligidas à população. Convém frisar, contudo, que estatísticas há no sentido de que cerca de 95% (noventa e cinco por cento) dos crimes digitais ultimados conseguem ser apenados com a legislação penal hoje em vigor.

Isso se torna ainda mais importante, principalmente se considerando, também, o Princípio da Legalidade, por meio do qual resta proibida a utilização da analogia in malam partem no Direito Penal, podendo ser essa técnica aplicada nas situações em que haja benefício ao acusado.

Não restam dúvidas, pois, de que é necessário ter cautela relativamente a essa nova Sociedade. Fundamental, para melhor entendimento da temática, observar as palavras de Alvin Toffler:

> Esta nova civilização, ao desafiar a antiga, derrubará burocracias, reduzirá o papel do estado-nação e gerará economias semiautônomas em um mundo pós-imperialista. Isso exigirá governos que sejam mais simples, mais eficazes e, também, mais democráticos do que os que hoje são conhecidos. É uma civilização com sua própria e característica perspectiva mundial, suas próprias formas de entender o tempo, o espaço a lógica e a causalidade. Acima de tudo (...) a civilização da Terceira Onda começará a fechar a brecha histórica aberta entre produtor e consumidor, originando a economia do "prossumidor" de amanhã. Por essa razão, entre muitas outras, poderia resultar – com um pouco de ajuda inteligente de nossa parte – a primeira civilização verdadeiramente humana, de toda a História. [21]

Nesse sentido, então, as previsões da Convenção de Budapeste, que objetiva traçar uma padronização da legislação sobre crimes da Internet, têm forte valor, pois servirão ao mister de reduzir a grande dificuldade ainda hoje existente em combater, de forma efetiva, os crimes efetivados em ambiente web.

O ajuste de Budapeste foi assinado aos 23 de novembro de 2001, na Hungria, pelo Conselho da Europa, contando, à época, com diversos países europeus, bem como com Estados Unidos, Canadá e Japão. Hodiernamente, outras nações não europeias já aderiram ao Acordo, incluindo algumas da América Latina, como Chile, Costa Rica, México e República Dominicana [22].

Com a padronização das legislações internacionais objetivada com a Convenção, tornar-se-á mais fácil a cooperação entre as polícias mundiais, o que, sem dúvidas, facilitará a detenção dos infratores.

Isso se torna ainda mais relevante na medida em que se constata a crescente utilização das ferramentas de Computação em Nuvem, havendo, como consequência, todos aqueles fatos antes já examinados.

Outrossim, convém deixar a reflexão de que tramita no Brasil o Substitutivo ao Projeto de Lei da Câmara Nº 89/2003, conhecido como Projeto de Lei do Senador Eduardo Azeredo, o qual tem previsões bastante semelhantes às trazidas pela Convenção de Budapeste. A leitura comparativa de ambos os diplomas deixa clara essa constatação, havendo, inclusive diversos dispositivos com profunda identidade.

Esclareça-se que nada obsta a que o Brasil seja signatário da Convenção de Budapeste e aprove o Projeto de Lei do Senador Azeredo, não havendo qualquer restrição a que isso se dê, sendo crescente, inclusive, o movimento daqueles que entendem ser necessário tomar essa medida.

Acaso não sejam implementados modernos mecanismos de cooperação internacional entre justiças, esses procedimentos poderão demandar grande tempo, já que, a se continuar seguindo o procedimento atual, faz-se necessária a elaboração de uma Carta Rogatória, a qual é encaminhada ao Ministro da Justiça, a fim de que seja feito o pedido do seu cumprimento, por via diplomática, às autoridades estrangeiras competentes, a teor do que dispõe o art. 783 do Código de Processo Penal.

Frise-se o grande sigilo que deve envolver essa complexa troca de informações, já que, a depender do contrato que o indivíduo mantenha com a empresa prestadora de serviços de Computação em Nuvem, mediante um simples comando, pode ser determinada a remoção de todo o conteúdo até então armazenado.

Surge, então, como de fundamental necessidade para a melhor solução de demandas de perícia forense em um cenário de *Cloud Computing* a necessidade de uma legislação internacional que preveja a cooperação entre as diversas nações signatárias do Tratado que vier a ser elaborado. Entende-se que, somente dessa maneira, ter-se-á possibilidade de êxito em uma operação que envolva os casos aqui analisados.

De modo contrário, as operações da Polícia Federal, que até então têm apresentado grande sucesso, esbarrarão na dificuldade de acessar as informações dos investigados, o que pode, na maioria dos casos, inviabilizar a persecução criminal, deixando livre, por falta de provas, perigosos malfeitores.

5. Considerações Finais

Como se teve oportunidade de observar, as questões que envolvem a Perícia Forense Computacional em um cenário de *Cloud Computing* são novas, tanto para os operadores do Direito, quanto para os profissionais peritos, que farão as investigações nessas cenas.

Como se frisou, no entanto, principalmente por parte dos legisladores, faz-se mister a aprovação de legislação que vise ao combate dos crimes efetivados em meio eletrônico, sob pena de perpetuação da já existente ideia de que a "Internet é uma terra sem lei", o que tem permitido uma grande elevação dos casos de condutas maléficas levadas a efeito na Grande Rede.

Tendo-se em conta que, geralmente, as informações na Internet circulam em diversos países do globo, simultaneamente, surge a necessidade de cooperação internacional, a fim de que se consiga, de modo mais efetivo, barrar a ação dos cibercriminosos.

Encontra-se em trâmite no Brasil um Projeto de Lei sobre Crimes Eletrônicos, que, mesmo não atendendo, satisfatoriamente, todas as questões que precisam ser solucionadas, já representa certo avanço na área. Esse projeto

apresenta ponto positivo, no que pertine à semelhança que apresenta com a Convenção de Budapeste, o que poderia facilitar essa interoperabilidade entre os diversos organismos internacionais.

Como se abordou, atualmente, caso seja necessária a busca de informações armazenadas na "nuvem", em se verificando que os servidores em que elas estão guardadas não se localizam no Brasil, ficam bastante restritas as possibilidades de atuação dos órgãos policiais e jurisdicionais pátrios, devendo-se ter bastante atenção nas ações empreendidas, sob pena de violação de lídimos direitos constitucionais dos investigados.

E isso porque, caso se faça a colheita de provas violando essas garantias, estar-se-á diante de prova ilícita, podendo haver a contaminação de todas as outras evidências dela derivadas, inutilizando-as – teoria do fruto da árvore envenenada – o que pode, em última análise, levar a que o acusado seja solto por ausência de provas.

Em sendo assim, necessário se faz que seja feito esforço conjunto da sociedade, dos operadores do Direito, do Legislativo e das diversas polícias, a fim de que sejam aprovadas normatizações que tratem de perto da questão da Perícia Forense Computacional, em um cenário de *Cloud Computing*, com o objetivo de que essas novidades não sejam utilizadas com o mister de elevar a prática criminosa.

Referências

[1] Internet Usage World Stats - Internet and Population Statistics. Disponível em: <http://www.internetworldstats.com/>. Acesso em: 11 ago. 2010.

[2] CASTELLS, Manuel. **Information age: economy, society, and culture**. 2. ed. Oxford: John Wiley and Sons, 2010, p. 45.

[3] KAUFMAN, Lori M. *et al.* Data security in the world of Cloud Computing**. IEEE Security and Privacy**, vol. 7, no. 4, pp. 61-64, July/Aug. 2009.

[4] CUCOLO, Eduardo. Internet lidera as transações bancárias. Caderno Mercado. **Folha de São Paulo**, São Paulo, B8, 06 de julho de 2010.

[5] VACCA, John R. **Computer Forensics**: computer crime scene investigation. 2. ed. Hingham: Cengage Learning, 2005, p. 4.

[6] LÉVY, Pierre**. Cibercultura**. Tradução de Carlos Irineu Costa. São Paulo: Editora 34, 1999, *passim*.

[7] BERNARDEZ, Mariano L. **Capital intelectual**: creación de valor en la sociedad del conocimiento. Bloomington: AuthorHouse, 2008, *passim*.

[8] BRASSANINI, David; MORENO-TAXMAN, Karine. **Guia de campo sobre prova digital.** Federal Bureau of Investigation, p.2.

[9] VACCA, John R. **Computer Forensics**: computer crime scene investigation. 2. ed. Hingham: Cengage Learning, 2005, *passim*.

[10] FREITAS, Andrey Rodrigues de. **Perícia forense aplicada à Informática**. Rio de Janeiro: Brasport, 2006, *passim*.

[11] LIMA, Caio César Carvalho. **Análise da validade dos documentos eletrônicos na sistemática Processual Civil Constitucional brasileira**: evolução do sistema probatório e a sociedade da informação. Fortaleza: UFC, 2010. 180 p. Monografia (Graduação em Direito), Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2010.

[12] TAURION, Cezar. **Cloud Computing**: computação em nuvem – transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009, p. 2.

[13] MATHER, Tim; KUMARASWAMY, Subra; e LATIF, Shahed. **Cloud Security and Privacy** – an enterprise perspective on risks and compliance. O'Reilly Media Inc.:Sebastopol, 2009, p. 10.

[14] TAURION, Cezar. **Cloud Computing**: computação em nuvem – transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009, p. 103.

[15] TAURION, Cezar. **Cloud Computing**: computação em nuvem – transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009, p. 102.

[16] LILLARD, V. Terrence *et al*. **Digital forensics for network, Internet, and cloud computing**: a forensic evidence guide for moving targets and data. Elsevier: Burlington, 2010.

[17] FREITAS, Andrey Rodrigues de. **Perícia forense aplicada à Informática**. Rio de Janeiro: Brasport, 2006, p.5.

[18] ALBUQUERQUE, Roberto Chacon de. **A criminalidade informática**. São Paulo: Juarez de Oliveira, 2006, p.64.

[19] ALBUQUERQUE, Roberto Chacon de. **A criminalidade informática**. São Paulo: Juarez de Oliveira, 2006, *passim*.

[20] LÉVY, Pierre**. Cibercultura**. Tradução de Carlos Irineu Costa. São Paulo: Editora 34, 1999, *passim*.

[21] TOFFLER, Alvin. **La tercera ola**. Bogotá: Ediciones Nacionales, 1981, p. 18-19.

[22] Conventions on Cybercrime. Disponível em: <http://conventions.coe.int/Treaty/Commun/ChercheSig. asp?NT=185&CM=8&DF=02/06/2010&CL=ENG>. Acesso em: 08 jul. 2010.

Agradecimentos

Aproveita-se a oportunidade para agradecer ao incentivo à pesquisa levado a efeito: pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq); pela Faculdade de Direito da Universidade Federal do Ceará (UFC), especialmente à Pró-Reitoria de Assuntos Estudantis; bem como por todos da Comissão de Informática Jurídica da Ordem dos Advogados do Brasil – Seccional Ceará (OAB/CE).

Caio César Carvalho Lima Universidade Federal do Ceará (UFC), ccesar@gmail.com, Fortaleza (CE)