A ADOÇÃO DE PROTOCOLO DE AUTENTICIDADE PARA A PROMOÇÃO DA SEGURANÇA JURÍDICA NA CONTRATAÇÃO VIA INTERNET

João Fábio de Oliveira[*]

Cinthia O. de A. Freitas[**]

Antônio Carlos Efing[***]

Cláudia Maria Barbosa[****]

RESUMO

Este trabalho discute os problemas de segurança nas transações de contratação via Internet, determinando um protocolo de autenticidade que irá manter diversos registros das atividades realizadas, durante todo o processo de contratação, em arquivos armazenados digitalmente, tanto do lado do fornecedor quanto do lado do consumidor. Entende-se que é obrigação legal do fornecedor garantir o registro e a integridade das operações realizadas na Internet, uma vez que em situações de litígio pode ocorrer a inversão do ônus da prova, conforme definido no art. 6º, inciso VIII, da Lei 8.078/90 – Código de Defesa do Consumidor. Deste modo, o protocolo de autenticidade proposto garantirá a confiança na transação realizada, registrando informações relevantes que ajudarão na identificação das partes, utilizando-se para tal um *software* adicional (*Plug-in*) instalado no servidor do fornecedor e na máquina do consumidor, executado no ambiente *Web* (meio que permite as contratações de consumo na Internet). Portanto, acredita-se que a segurança na contratação via Internet é fator imprescindível, pois permite ao consumidor uma garantia da celebração contratual, já que mantém a integridade do documento, bem como serve ao Poder Judiciário como prova ao dirimir situações de litígio, satisfazendo as premissas da aceitação legal de um documento digital.

[*] Mestrando do Programa de Pós-Graduação em Informática (PPGIa) da PUCPR. joao.fabio@gvt.com.br.

[**] Doutora em Informática, Professora Titular da Pontifícia Universidade Católica do Paraná para os Cursos de Ciência da Computação, Engenharia da Computação e Direito. Professora dos Programas de Pós-Graduação em Direito (PPGD) e em Informática (PPGIa) da PUCPR. cinthia.freitas@pucpr.br.

[***] Doutor em Direito pela Pontifícia Universidade Católica de São Paulo – PUCSP, Professor Titular de Direito do Consumidor e Professor do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná – PUCPR, efing@mber.com.br.

[****] Doutora em Direito, Professora Titular de Direito Constitucional e Professora do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná – PUCPR. claudia.barbosa@pucpr.br.

PALAVRAS- CHAVE: DIREITO E INTERNET; DIREITO DO CONSUMIDOR; AUTENTICIDADE.

ABSTRACT

This paper discusses the security problems on the contracts hired by Internet and describes an authenticity protocol that will keep log files from the activities during the web hiring, throughout the process of recruitment. These log files will be stored digitally, either on the side of the supplier as of the consumer. It is understood that it is legal obligation of the supplier to register and ensure the integrity of the operations on the Internet, because in situations of dispute can occur a reversal of the burden of proof, as defined in art. 6, section VIII, of the Law 8.078/90 - Brazilian Consumer Code. Thus, the authenticity protocol will ensure confidence on the Internet contracts, registering relevant information that will help in the identification of the parties, using a Plug-in software installed on the supplier server and in the consumer machine, executable in the Web. Moreover, it is important to remind that security in hiring by Internet is an essential feature because it allows the consumer a guarantee of contract award, since it maintains the integrity of the document, and also can be presented as an evidence to the Judiciary, helping in litigation and satisfying the premises of the legal acceptance of a digital document.

KEYWORDS: LAW AND INTERNET; CONSUMER PROTECTION; AUTHENTICITY.

INTRODUÇÃO

O crescimento do uso da Internet na rotina diária das pessoas já se concretizou como ferramenta básica e essencial para solução de diversos problemas característicos do dia-a-dia da sociedade, tais como: pagamento de contas bancárias, consulta a catálogos telefônicos e mapas, relacionamento entre pessoas, mensagens eletrônicas e, ainda, aquisição de objetos e serviços de consumo.

Segundo o Centro de Estudos sobre as Tecnologias da Informação e da Comunicação[2], cerca de 14,49% dos domicílios brasileiros já possuem acesso à Internet,

[2] Comitê Gestor da Internet Brasil, Centro de Estudos sobre Tecnologias da Informação e da Comunicação, disponível em: http://www.cetic.br/, acesso em 11 de março de 2008.

contabilizados na última pesquisa em 2006[3], o que representa um crescimento de 1,56% sobre os 12,93% do ano de 2005[4]. Este universo crescente de usuários e potenciais consumidores de produtos e serviços por meio da Internet representa uma grande preocupação do ponto de vista técnico e jurídico, pois potencializa a cada ano o volume de problemas a serem tratados no âmbito de cada ciência relacionada.

Como meio de acesso digital, a Internet traz algumas preocupações de segurança da informação, uma vez que os registros não são mais feitos em meio físico, como papel, e sim arquivados eletronicamente em meios digitais, como o disco rígido dos computadores. Ao mesmo tempo em que simplifica as operações comerciais realizadas no meio digital, insere um fator restritivo e aponta para um universo de estudo sobre os aspectos da segurança, confiabilidade, autenticidade. Sem esquecer, ainda, da legalidade dessas operações frente a fatos duvidosos e questionados por qualquer parte envolvida na transação, conforme apresentado por Mattos (2007).

As principais situações inconvenientes existentes na Internet[5], como mensagens eletrônicas indesejadas, invasão de sites, vírus em computadores, tem crescido nos acessos à Internet, porém o esforço em busca de soluções técnicas para a segurança da informação trafegada permite propor mecanismos mais seguros para o tráfego e o armazenamento das informações, principalmente para torná-las confiáveis do ponto de vista da veracidade do conteúdo registrado. Neste sentido, os métodos de criptografia e assinatura digital têm contribuído para a segurança de transações via Internet (Behrens, 2005) (Garfinkel, 1997).

1. PROBLEMAS DE SEGURANÇA NA *WEB*

A base de transporte das informações na Internet é o protocolo TCP/*IP (Transmission Control Protocol/Internet Protocol*) e este, em sua versão 4, é o

[3] Pesquisa disponível em: http://www.cetic.br/usuarios/tic/2006/rel-geral-05.htm, acesso em 11 de março de 2008.

[4] Pesquisa disponível em: http://www.cetic.br/usuarios/tic/2005/rel-int-01.htm, acesso em 18 de novembro de 2007.

[5] Segundo o Centro de Tratamento de Incidentes de Segurança da Rede Nacional de Pesquisa, disponível em: http://www.rnp.br/cais/alertas/2007/cais-res-20071106.html, "*No terceiro trimestre de 2007 a equipe do CAIS tratou 8.080 incidentes de segurança na sua totalidade. Destes, 49,12% referem-se ao envio de spam em grande escala, 18,57% a tentativas de invasão de sistemas e 13,89% a propagação de vírus e worms através de botnets (computadores infectados e controlados à distância por atacantes). Também foram tratados 225 casos de troca de páginas, em que o atacante substitui o conteúdo original de uma página web ou inclui conteúdo não autorizado na página atacada, e ainda 88 casos de phishing, ataques que têm por objetivo básico obter dados confidenciais de usuários.*", acesso em 18 de novembro de 2007.

consolidado para uso na Internet (Comer, 1991). Este protocolo não prevê mecanismos de segurança quanto ao transporte das informações, deixando, para as aplicações que são desenvolvidas para interação com os usuários finais, o papel da preocupação com critérios relativos à proteção do conteúdo trafegado. Isto significa que o transporte das informações entre dois pontos na Internet, independente de sua localização física, poderá ser capturado por um analisador de protocolo[6], tornando-se conhecidas as informações ali capturadas.

Na especificação do protocolo TCP/IP existe a divisão conceitual de cinco camadas ou níveis, conforme mostrado na Tabela 1 (Comer, 1991). As camadas mais baixas (1 a 4) preocupam-se em fazer com que a informação saia da origem e chegue ao destino através da rede, seja ela Internet pública ou mesmo uma rede privada[7]. A camada 5, também chamada de aplicação, especifica e implementa softwares aplicativos que interagem com os usuários finais. É justamente neste nível que todas as preocupações relativas à segurança da informação deverão ser implementadas, ou seja, as aplicações no nível do usuário devem ter mecanismos de tratamento que sejam considerados seguros o suficiente para, de um lado dar a percepção ao usuário final que sua transação na rede está segura, sem riscos de adulterações de conteúdo, e por outro lado promover condições técnicas comprovadas de mecanismos considerados seguros, como o uso de algoritmos criptográficos no nível da aplicação (Schneier, 1996).

Tabela 1 – Modelo em Níveis do TCP/IP

Camada	**Protocolo**
5 – Aplicação	HTTP, DNS, SMTP,...
4 – Transporte	TCP, UDP
3 – Rede	IP, IGMP
2 – Enlace	Ethernet, 802.11 Wifi, FR,...
1 – Física	Modem, RS232, USB,...

[6] O analisador de protocolo Wireshark é o mais popular conhecido e distribuído livremente na Internet, disponível em: http://www.wireshark.org/, acesso em 18 de novembro de 2007. Outros aplicativos disponíveis são o CommView e Norton Ghost, ambos com licença através de pagamento.

[7] Redes Privadas são que usam endereçamentos IPs reservados e distintos dos usados na Internet pública, conforme definição disponível em: http://pt.wikipedia.org/wiki/Rede_privada, acesso em 18 de novembro de 2007.

O tráfego na Internet conhecido como WWW (*World Wide Web*), ou simplesmente *Web*, é uma aplicação de software, modelo cliente-servidor[8], que é executada como interface direta com o usuário através do ambiente conhecido como navegador ou *browser*[9]. Neste ambiente diversas aplicações são escritas no formato do protocolo de nível de aplicação do TCP/IP conhecido como http (*hypertext transfer protocol*)[10] (Garfinkel, 1997). Em não havendo mecanismos definidos no próprio protocolo TCP/IP, cabe então as aplicações definirem e implementarem seus algoritmos adicionais de segurança para minimizar os impactos das vulnerabilidades existentes na rede.

Os problemas de segurança na *Web* consistem em três grandes categorias (Garfinkel, 1997):

- Segurança no servidor *Web* e nos dados que estão ativos e arquivados nele: o usuário deve ter garantias de que suas informações estão confiáveis e seguras, e que não foram modificadas ou distribuídas sem sua autorização;
- Segurança da informação que viaja entre o servidor e o cliente pela rede de computadores: o usuário deve ter garantias de que a transmissão das informações entre o servidor e seu navegador *Web* tem um nível de proteção baseado em critérios tidos como confiáveis, tal qual a criptografia ou a assinatura digital (Behrens, 2005);
- Segurança da informação na própria máquina do usuário: o usuário deve ter garantias de que seu computador está o mais protegido possível através do uso de ferramentas associadas ao seu ambiente operacional[11]. Neste ponto, a avaliação do quanto a máquina do usuário está protegida fica comprometida pela própria autoridade do usuário sobre seu ambiente, pois, no nível de autonomia sobre gestão de sua máquina, o usuário pode autorizar, indevidamente, a instalação de softwares maliciosos que irão atuar em contravenção ao seu uso. Estes aspectos dependem do conhecimento e esclarecimento do usuário sobre

[8] Modelo computacional que separa o servidor de informações do cliente através de uma rede de computadores, conforme definição disponível em: http://pt.wikipedia.org/wiki/Cliente-servidor, acesso em 18 de novembro de 2007.
[9] Software cliente do protocolo http que é executado na máquina do usuário, conforme definição disponível em: http://pt.wikipedia.org/wiki/Browser, acesso em 18 de novembro de 2007.
[10] Aplicação de nível 5 na estrutura TCP/IP que define um protocolo de transporte hypermídia, conforme definição disponível em: http://pt.wikipedia.org/wiki/HTTP, acesso em 18 de novembro de 2007.
[11] Cartilha sobre segurança para Internet recomenda uso e configurações adequadas para o usuário final, disponível em: http://cartilha.cert.br/, acesso em 18 de novembro de 2007.

segurança, sendo que na prática o usuário tem pouco, ou quase, nenhum domínio sobre este assunto.

Transpondo as definições dos protocolos envolvidos na Internet e suas características de fragilidade vistas anteriormente, sobre as contratações realizadas na Internet, o paradigma da confiança do contrato de consumo eletrônico, apresentado em Mattos (2007), levanta aspectos jurídicos de despersonalização extrema baseado em massificação contratual instrumentalizado comumente por adesão e com cláusulas gerais, em que há pluralidade de consumidores e fornecedores organizados em cadeia, dificultando as identificações dos fornecedores e a relação de responsabilidades sobre o contrato. Isto se agrava quando a tecnologia usada oferece riscos de alterações de conteúdo, quebra de autoridade, plágio ou mesmo acessos indevidos e mau uso do conteúdo para fins ilícitos[12].

Desta forma, considerando os problemas de segurança existentes na Internet, passa-se a analisar estas vulnerabilidades sob a ótica de contratos realizados via Internet, considerando para tais aspectos relevantes da área de segurança da informação.

2. SEGURANÇA DA INFORMAÇÃO

Para Sêmola (2003) segurança da informação pode ser definida como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

Pode-se também considerar a segurança da informação como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos de segurança: confidencialidade, integridade e disponibilidade da informação. Define, portanto, as regras de incidência sobre todos os momentos do ciclo de vida da informação: manuseio, armazenamento, transporte e descarte, levando à identificação e ao controle de ameaças e vulnerabilidades. Assim sendo, tem-se:

- Confidencialidade: toda a informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação do seu acesso e uso apenas às pessoas para quem elas são destinadas;

[12] De 1999 até 2007, o número de incidentes de segurança registrado no Brasil tem crescido anualmente, conforme demonstrado em: http://www.cert.br/stats/incidentes/, acesso em 18 de novembro de 2007.

- Integridade: toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais;
- Disponibilidade: toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade.

Sêmola (2003) ainda define alguns elementos de impacto na prática da segurança da informação que refletem a importância da visão estruturada sobre as vulnerabilidades e pontos críticos na administração dos conteúdos trafegados na Internet que possam gerar fraudes e adulterações, as quais podem comprometer a legalidade juridicamente as relações contratuais realizadas neste ambiente. Esses elementos são:

- Autenticação: processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica que permite o acesso à informação e aos seus ativos por meio de controles de identificação desses elementos;
- Legalidade: característica das informações que possuem valor legal dentro de um processo de comunicação, no qual todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes;
- Autorização: concessão de uma permissão para o acesso às informações e às funcionalidades das aplicações aos participantes de um processo de troca de informações (usuário ou máquina);
- Autenticidade: garantia de que as entidades (informação, máquinas, usuários) identificadas em um processo de comunicação como remetentes ou autores sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação.

Em toda operação de contratação em ambiente virtual, realizada na Internet, os elementos apresentados anteriormente compõem a parte essencial da análise de integridade para autenticidade do processo realizado, ou seja, a garantia e a veracidade da contratação realizada.

3. CONTRATAÇÃO VIA INTERNET

Para Boiago Júnior (2005) os contratos provêm dos negócios jurídicos que são realizados em virtude de acordos de vontade bilateral ou plurilateral, e a diferenciação está caracterizada na convergência de dois ou mais consentimentos para que sejam produzidos efeitos jurídicos. Assim, se uma pessoa por meio de e-mail se compromete a realizar determinada obrigação para com outras duas pessoas que aceitam a execução da obrigação, certamente ocorreu um negócio jurídico, pois houve a convergência de três vontades para a consecução de um determinado negócio jurídico, por conseqüência a realização de um contrato.

Ademais, sabe-se que o consumo em sites virtuais por meio do comércio eletrônico tem crescido a taxas na ordem de 35% ao ano[13], o que escala um nível na mesma proporção de problemas a serem tratados, desde aspectos técnicos quanto aos aspectos jurídicos da própria contratação.

Em pesquisa realizada pelo Procon-SP no período de junho a julho de 2007 sobre uma amostragem de 3 mil usuários de computadores, 59,11% destes usuários praticaram comércio eletrônico, ou seja, geram aceitação sobre os contratos virtuais. Nesta mesma pesquisa, 35,46% apontam para a falta de confidencialidade e segurança nos contratos virtuais, e 36,42% apontam para a falta de segurança no processo de contratação, destacando este fator como restritivo ao maior crescimento e confiabilidade em todo o processo de contratação pela Internet[14].

Em sua essência, o contrato eletrônico não se descaracteriza em qualquer aspecto que componha a idéia de contrato como principal fonte do direito das obrigações, apenas sua forma é diversa, e é necessária a análise de sua natureza para se determinar os elementos formativos em face do novo ambiente em que ele se realiza sem perder de vista os interesses que devem estar presentes em qualquer abordagem jurídica (Relvas, 2005).

Na composição dos elementos contratuais no ambiente virtual, podem-se relacionar os itens fundamentais em sua estrutura (Relvas, 2005):

---

[13] Segundo a FOLHAOnline, disponível em http://www1.folha.uol.com.br/folha/dinheiro/ult91u359556.shtml, temos: "O número de consumidores que compraram pela internet deve crescer 35% em 2007. Junto com o aumento das vendas, as reclamações de consumidores insatisfeitos com o serviço também subiram. Somente em dezembro, o Procon de São Paulo recebeu em seu site quase o mesmo número de queixas que o total do ano em todos os canais de reclamação". Acesso realizado em 14 de janeiro de 2008.

[14] Pesquisa realizada pelo Procon-SP, disponível em http://www.procon.sp.gov.br/pdf/comercio_eletronico.pdf, acesso realizado em 14 de janeiro de 2008.

- Usuário-consumidor: diz respeito à pessoa física ou jurídica que adquire ou utiliza produto ou serviço, pela via eletrônica, como destinatário final;
- Fornecedor: é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços (Código de Defesa do Consumidor, art. 3º.);
- Contratos eletrônicos: são contratos formais ou informais, expressos ou tácitos, individuais ou por adesão, realizados através da rede mundial de computadores (Internet);
- Local do contrato: é o local de residência habitual do contratante, que deve ser considerado para efeitos jurídicos.

O princípio fundamental da autonomia da vontade destaca particularidades na contratação eletrônica, a saber (Relvas, 2005):

a) faculdade de contratar ou não contratar, ou seja, liberdade de escolha do contratante em aceitar ou não o contrato;
b) liberdade de escolha do contratante em relação ao contratado, ou seja, no mundo virtualizado da Internet, ter a liberdade de escolha de quem contratar;
c) liberdade de fixar e/ou negociar o conteúdo dos contratos, a exceção dos contratos por adesão[15].

Sendo assim, a assinatura de um contrato tradicional é a confirmação explícita da vontade entre as partes. Já nos contratos virtuais, o problema da assinatura eletrônica torna-se cada vez mais imprescindível para a validade e para a legalidade do contrato (Behrens, 2005).

A grande parte das contratações em ambiente virtual não considera o uso de mecanismos de assinatura digital, porém estes mecanismos estão disponíveis

[15] A respeito dos contratos de adesão: “Os contratos de adesão são os contratos já escritos, preparados e impressos com anterioridade pelo fornecedor, nos quais só resta preencher os espaços referentes à identificação do comprador e do bem ou serviços, objeto do contrato. As cláusulas são preestabelecidas pelo parceiro contratual economicamente mais forte, sem que o outro parceiro possa discutir ou modificar substancialmente o conteúdo do contrato escrito. É evidente que esses tipos de contrato trazem vantagens as empresas, mas ninguém duvida de seus perigos para os contratantes hipossuficientes ou consumidores. Estes aderem sem conhecer as cláusulas, confiando nas empresas que as pré-elaboraram e na proteção que, esperam, lhes seja dada por um Direito mais social.”. Scaravaglioni, Eduardo. O Código de Defesa do Consumidor e os contratos de adesão. Disponível em:

publicamente na Internet e garantem o mesmo valor jurídico de uma assinatura convencional[16], conforme Medida Provisória 2.200-2/2001, que estabelece: "*"Art. 1º: Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.*".

Isto significa que, toda a contratação realizada em ambiente virtual, se confirmada com uma assinatura digital, possui o valor jurídico necessário para confirmar a vontade das partes.

E, ainda, deve-se ressaltar que, o documento eletrônico, por possuir os elementos da autoria, conteúdo e meio, configura-se perfeitamente como documento para fins de prova no processo civil (Dias, 2004).

Deste modo, o presente trabalho apresenta a proposta de um protocolo de autenticidade para o relacionamento entre o fornecedor e o consumidor, sendo que tal protocolo define parâmetros técnicos e rastreáveis da operação realizada, e disponibiliza informações seguras[17], tanto no servidor do fornecedor, quanto na máquina do consumidor. Assim, um *software* vem sendo desenvolvido e será disponibilizado para ambas as partes envolvidas em contratações via Internet. Este *software* deve ser usado juntamente com o servidor *Web* do fornecedor e com o navegador *Web* do consumidor, e seguirá o conceito de *Plug-in Web*[18].

4. PROTOCOLO DE AUTENTICIDADE

As contratações realizadas no âmbito da Internet contemplam desde uma simples aceitação de um acordo estipulado em e-mail, até os mais complexos contratos postados em sites *Web* com aceitação por adesão por parte do contratante (Boiago Júnior, 2005).

---

http://www.procon.go.gov.br/procon/detalhe.php?textoId=000808 acesso realizado em 13 de março de 2008.

[16] Conforme definição e disponibilização em http://www.contratosdigitais.com/oque/valorLegal.html: "As assinaturas eletrônicas têm o mesmo valor jurídico da assinatura convencional, desde que sejam realizadas por meio de um processo que assegura todos os elementos de prova jurídica em conformidade com a legislação vigente.". Acesso em 14 de janeiro de 2008.

[17] Estão sendo considerados como "seguras" as informações armazenadas em arquivo criptografado [Schneier, 1996], depositado no servidor *Web* do contratado e também na máquina do contratante.

[18] Conforme definição disponível em: http://pt.wikipedia.org/wiki/Plugin, "*Na informática, um **plugin** ou **plug-in** é um (geralmente pequeno e leve) programa de computador que serve normalmente para adicionar funções a outros programas maiores, provendo alguma funcionalidade especial ou muito específica.*", acesso em 18 de Novembro de 2007.

Isto aponta para que, especificamente no contexto do tráfego Web, o nível de segurança das informações trafegadas por meio do protocolo *http* na rede Internet garanta um mínimo de segurança através de mecanismo de criptografia. De fato, o uso do protocolo SSL[19] *(Secure Sockets Layer*) nas aplicações *Web* aplica criptografia entre o nível do protocolo TCP/IP e a camada de aplicação do usuário, evitando que as informações sejam trafegadas na rede Internet de forma aberta, (Garfinkel, 1997).

Nos diversos níveis do protocolo TCP/IP, há características que podem ser exploradas de forma maliciosa por *hackers* ou outros usuários mal intencionados (Atkins, 1997). A exemplo do nível 2 – Enlace (Tabela 1) da camada do protocolo TCP/IP, o endereço da placa de rede de um computador em rede local pode ser adulterado por um outro usuário com intenções de redirecionar o tráfego para outra máquina naquela mesma rede local, gerando fraude para os usuários envolvidos neste problema. No nível 3 – Rede (Tabela 1) da camada do protocolo TCP/IP, o endereçamento IP também pode ser adulterado de forma maliciosa, desviando o tráfego agora não no contexto da rede local, mas sim ultrapassando as barreiras do ambiente do usuário e envolvendo o tráfego na rede Internet (Atkins, 1997).

As aplicações desenvolvidas para o ambiente da Internet, seguindo o modelo cliente-servidor, utilizam-se da infra-estrutura padronizada do protocolo TCP/IP, estando, todavia, vulneráveis aos diversos problemas característicos deste ambiente. Especificamente no tráfego *Web* na Internet, quando a comunicação entre o servidor do contratado e o navegador do contratante usar o protocolo SSL para criptografia dos dados trafegados na rede, o risco de fraudes no conteúdo trafegado estará reduzido pela criptografia utilizada (Garfinkel, 1997).

Nas contratações via Internet, a exemplo de compras de bens de consumo em *sites* eletrônicos de vendas[20], o consumidor estará utilizando-se de toda a infra-estrutura de comunicação definida na rede Internet, ou seja, desde seu computador com o seu navegador Web, linhas de comunicação, provedor do serviço Internet, seguindo a comunicação até o servidor do fornecedor. Quando o consumidor realiza uma operação

[19] O protocolo SSL foi desenvolvido pela Netscape para uso com seu navegador *Web*. O IETF (Internet Engineering Task Force) o utiliza como protocolo de criptografia básica em sua especificação TLS (Transport Layer Security), que é a recomendação de uso para o TCP/IP, conforme apresentado em [Garfinkel, 1997] e http://en.wikipedia.org/wiki/Transport_Layer_Security, acesso em 13 de janeiro de 2008.

[20] Como exemplo de site de comércio eletrônico pode-se citar o http://www.submarino.com.br, entre outros de mesma natureza. Acesso em 13 de janeiro de 2008.

de compra sobre o servidor do fornecedor por meio do seu navegador *Web*, ele está desprovido de mecanismos que comprovem a evidência da operação em sua relação contratual no nível técnico da operação realizada, ou seja, não há registros efetivos em seu computador que armazene e recupere o histórico realizado entre consumidor e fornecedor. Assim, o protocolo de autenticidade proposto, considerando o contexto do desenvolvimento de software (*Plug-in*) para coleta e tratamento das informações relativas à contratação via Internet, está dividido em duas partes:

a) Servidor: ficará instalado junto ao servidor *Web* do fornecedor e segue os padrões do protocolo *http* e linguagem *Java* para suporte a extensões de software nas aplicações *Web*, sendo configurado como uma extensão dos serviços do servidor e oferecido ao consumidor como *Plug-in* de *software* para o navegador do fornecedor. O contexto deste servidor considera o ambiente operacional Linux como suporte ao servidor *Web* do fornecedor e que o mesmo permita disponibilização de extensões de software ao usuário remoto, a exemplo do servidor *Web* Apache[21], disponível na maioria dos sistemas operacionais Linux;
b) Cliente: ficará instalado no computador do consumidor e segue o procedimento próprio para a instalação inicial do *Plug-in*, sendo considerada a anuência do consumidor para aceitar a instalação deste software em seu computador. Este *Plug-in* vem sendo desenvolvido em linguagem Java e estará disponível para o navegador Internet Explorer da Microsoft no sistema operacional Windows nas versões mais recentes e popularmente utilizadas, como Windows 2000, 2003, XP e Vista. A linguagem de programação Java foi definida por ter a flexibilidade de tratamento das informações no ambiente de navegação Internet.

Pode-se, então, apresentar o cenário geral do protocolo de autenticidade, no qual o consumidor possui em sua máquina o registro das transações efetuadas sobre o site *Web* do fornecedor, de forma a poder extrair um relatório com as informações pertinentes a estes acessos. Do lado do fornecedor, o protocolo permite que o mesmo

[21] O servidor Apache é um dos mais populares servidores HTTP para *Web* disponível na Internet para diversos sistemas operacionais. Maiores detalhes disponível em http://www.apache.org/, acesso em 19 de fevereiro de 2008.

conteúdo seja armazenado e resgatado por meio de relatório, de forma a confrontar as informações trafegadas entre as partes, tal qual mostrado na Figura 1.

Por sua vez, a Figura 2 detalha o modelo de captura realizado pelo *Plug-in* instalado nas máquinas do fornecedor e do consumidor. O tráfego entre o navegador do fornecedor e o servidor Web do consumidor é baseado no protocolo http e o *Plug-in* realiza a captura dos pacotes neste nível do protocolo e outras informações técnicas no nível do TCP/IP para registro nos arquivos de log.

Assim o protocolo proposto define que o consumidor, ao acessar o site *Web* do fornecedor por meio de seu navegador, tenha a sua disposição um ícone com informativo sobre o protocolo de autenticidade disponível para que o mesmo possa, com sua autorização e vontade explicitada, fazer o *download* em seu computador e, a partir desta aceitação, constar registrado todas as informações previstas pelo protocolo.

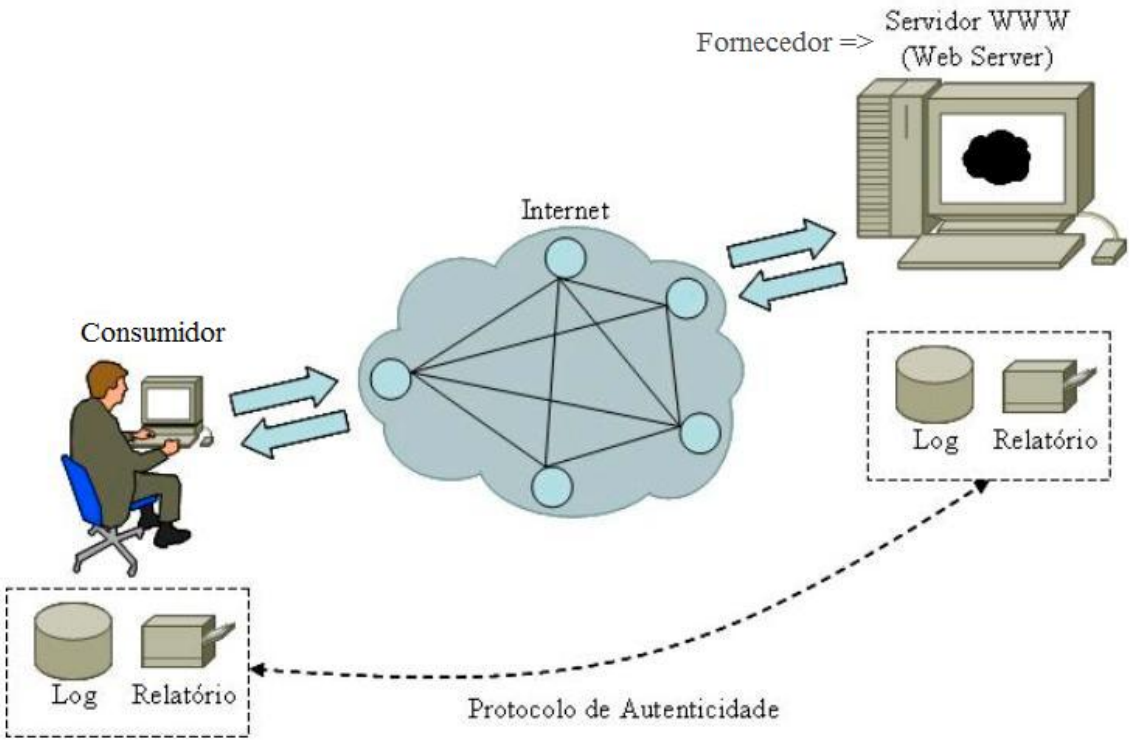

Figura 1 - Ambiente e Protocolo de Autenticidade

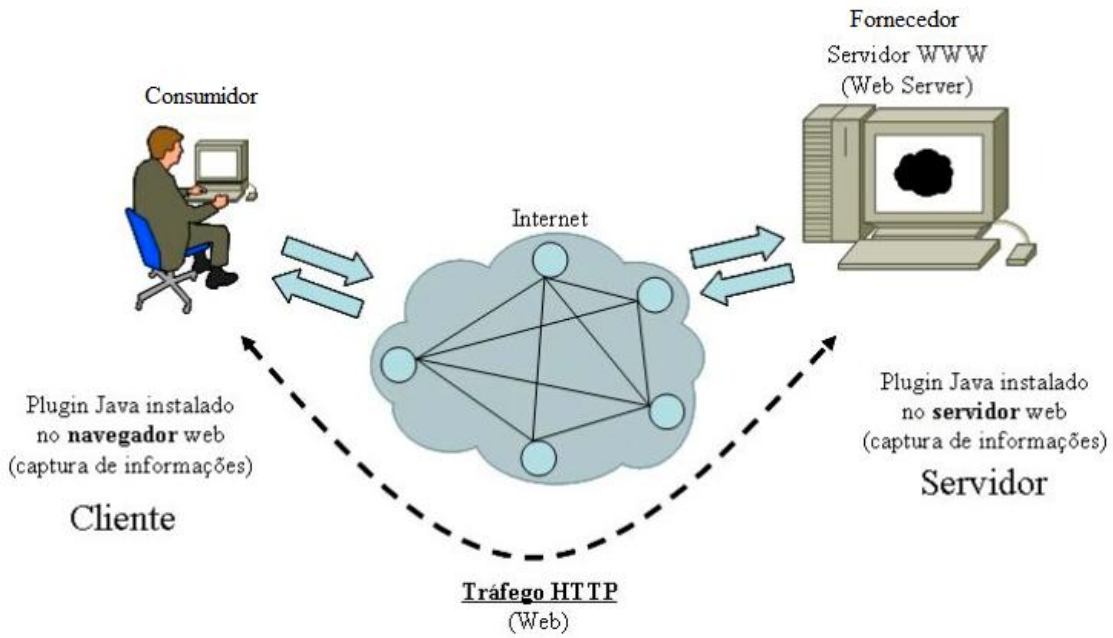

Figura 2 - Servidor e Cliente de Captura

Este processo inicial de navegação no site do fornecedor prevê uma verificação na qual, não havendo o aceite do consumidor, o mesmo será avisado textualmente em janela *Web* sobre a continuidade dos acessos, porém sem a autenticidade garantida pelo protocolo.

O algoritmo a ser desenvolvido, define a captura de informações do consumidor, realizado pelo processo inicial de interação com o mesmo na primeira vez que ele aceita a instalação e o uso do protocolo de autenticidade, e também a captura de informações técnicas referente aos acessos diretamente no site *Web* do fornecedor. Ou seja, na primeira interação do consumidor, há um questionário a ser respondido por ele que define um cadastro inicial com seus dados próprios[22], como definido na Tabela 2.

[22] Dados principais do Contratante para registro nos arquivos de captura, que serão informados uma única vez no processo inicial de instalação do *Plug-in*. Estes dados são a base de identificação legal do Contratante.

Tabela 2 – Informações do Consumidor - Cadastro Inicial

Informações do Contratante no Cadastramento Inicial	
Campo	**Descrição**
nome_contr	nome do contratante
endereco_contr	endereço completo do contratante
telefone_res_contr	telefone residencial do contratante
telefone_cel_contr	telefone celulcar do contratente
identidade_contr	identificação legal do contratante, considerando um tipo válido no Brasil como identificação do indivíduo
tipo_identidade_contr	RG, CNH, Passaporte, Carteira de Trabalho
cpf_contr	número do CPF do contratante

Após este processo inicial de cadastro o algoritmo prevê a verificação do *Plug-in* instalado na máquina do fornecedor, instalando-o nesta máquina quando da não existência do mesmo.

A partir deste ponto, as operações realizadas pelo consumidor no site *Web* do fornecedor terão suas informações armazenadas em um arquivo de *log*[23], o qual será gravado tanto no servidor do fornecedor quanto na máquina do consumidor. A Tabela 3 mostra as informações complementares que serão armazenadas em cada interação do consumidor no site do fornecedor.

O arquivo de *log* será encriptado utilizando-se DES (Data Encryption Standard), que é um algoritmo aprovado e aceito pelo *American National Standards Institute* (ANSI), que referencia os padrões de diversos protocolos utilizados mundialmente na Internet (Schneier, 1996). Este protocolo de criptografia trabalha com blocos de 64 bits, sendo um algoritmo simétrico[24]. Assim, ao ser simétrico, a chave usada para encriptação e decriptação do arquivo é a mesma, possuindo tamanho de 56 bits, tornando o algoritmo de rápido processamento considerando o arquivo de *log* a ser processado e garantido o acesso às informações.

[23] Conforme definição disponível em: http://pt.wikipedia.org/wiki/Log_de_dados, "*Em computação,* ***Log de dados*** *é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional*", acesso realizado em 12 de Dezembro de 2007.

[24] Há diversas técnicas de encriptação propostas em [Scheneier, 1996], como Lúcifer, Madryga, NewDES, IDEA, entre outras, que trabalham com conceitos próprios de chaves privadas ou públicas, aplicando técnicas simétricas ou assimétricas para encriptação dos respectivos arquivos.

Tabela 3 – Informações da Operação do Contratante

Informações da Operação do Contratante	
Campo	**Descrição**
IP_contratante	número IP do contratante (usuário)
IP_contratado	número IP do contratado (servidor)
data_acesso	data no formato DD/MM/AAAA
hora_acesso	hora no formato HH:MM:SS
protocolo_acesso	tipo de protocolo da pilha TCP/IP (TCP, UDP)
porta_contratante_acesso	número que especifica a porta do TCP ou UDP (usuário)
porta_contratado_acesso	número que especifica a porta do TCP ou UDP (servidor)
URL_contratado	endereço *Web* (URL - Uniform Resource Locator) acessado pelo contratante no site do contratado
observacoes	conteúdo capturado no pacote analisado

Desta forma, o consumidor terá condições de gerar seu relatório diretamente a partir de sua máquina sem depender de outras informações do fornecedor, a exemplo de utilização de outros critérios de encriptação com uso de chaves assimétricas (dependência da troca de chaves públicas e privadas entre as partes).

Este processo irá garantir que as informações armazenadas nas respectivas máquinas, fornecedor e consumidor, estejam com o nível básico de segurança garantida pela criptografia aplicada no arquivo, o que impede que qualquer pessoa possa tomar posse do conteúdo das informações armazenadas.

No *Plug-in* instalado na máquina do consumidor, haverá uma facilidade de visualização do arquivo de *log* armazenado, de forma a ser possível extrair as informações das operações realizadas em um relatório impresso para comprovação das diversas interações *Web* realizado no site do fornecedor.

No âmbito jurídico, o relatório impresso sobre as operações realizadas pelo consumidor permitirá ao mesmo comprovar o fato através do instrumento Ata Notarial (Rezende, 1999). Neste instrumento jurídico, o tabelião relata aquilo que vê, ouve, verifica e conclui, com seus próprios sentidos e própria opinião. É o testemunho oficial de fatos narrados pelos notários no exercício de sua competência em razão de seu ofício. Neste momento, há a confirmação jurídica do protocolo de autenticidade que registrou e relatou as operações de transação no âmbito da contratação via Internet, em que o relatório validado juridicamente será tratado como prova irrefutável das operações do contratante sobre o sítio *Web* do contratado.

O processo de captura das informações utiliza as facilidades disponíveis na estrutura da linguagem Java, integrando as bibliotecas de interface com o nível do protocolo TCP/IP, os quais constituem recursos de software que disponibilizam informações do tráfego de rede, contemplando todas as camadas definidas por este protocolo. Isto permite a captura e visualização das informações técnicas definidas no protocolo de autenticidade de forma aberta, possibilitando o armazenamento conforme definição do arquivo de *log*.

Os dados capturados seguem a estrutura definida na Tabela 4, que é um exemplo de captura de dados utilizando-se o software Wireshark[25], mantendo-se a referência ao modelo didático do protocolo TCP/IP. As informações necessárias para atender aos campos definidos no protocolo de autenticidade estão disponíveis no conjunto de dados capturados no *frame* Ethernet[26], conforme mostrado na Figura 3. As informações extraídas desta captura serão armazenadas no arquivo de *log* de forma seqüencial e logicamente estruturado em arquivo de dados no formato texto, sendo posteriormente encriptado para proteção dos dados ali armazenados.

A técnica para captura de pacotes baseia-se no uso da biblioteca libpcap/winpcap[27], que são bibliotecas de software de baixo nível disponível para desenvolvimento de código de programação, onde provêem informações do tráfego de rede de acordo com a interface utilizada, a exemplo para este trabalho, redes baseadas em protocolo Ethernet e Wireless WIFI.

Esta biblioteca fornece funções que capturam pacotes no formato básico de rede, onde temos o cabeçalho e os dados separados de forma distinta. Dentro do protocolo TCP/IP, em sua classificação didática, é possível separar os diversos níveis de informações, separando os níveis do protocolo e as informações do usuário, possibilitando a gravação destas informações em arquivo de *log* (Comer, 1991). A Tabela 4 mostra o formato do pacote capturado na interface de rede, que é disponibilizado pelas funções da biblioteca libpcap/winpcap para a aplicação do

[25] Disponível em http://www.wireshark.org, acesso em 12 de janeiro de 2008.
[26] O Frame Ethernet é a composição lógica de transmissão do pacote de dados em uma rede local usando o padrão IEEE 802.3 (http://www.ieee.org), onde os computadores do contratado e contratante estão conectados. Nesta rede local, em cada um das respectivas máquinas, são capturados os pacotes de dados para análise e armazenamento do protocolo de autenticidade.
[27] As bibliotecas Winpcap e Libpcap estão disponíveis para desenvolvimento de código de captura de pacotes em suas diversas interfaces de rede, conforme disponível em http://www.winpcap.org/ e http://www.tcpdump.org/, acesso em 19 de fevereiro de 2008.

protocolo de autenticidade, o qual irá separar os dados em seus níveis de informações técnicas, conforme definição do protocolo, e gravá-las em arquivo de *log*.

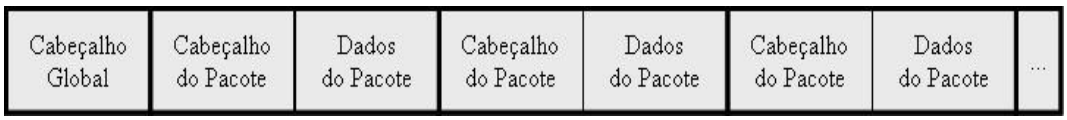

Figura 3 - Formato do Pacote Capturado

Tabela 4 – Captura do Pacote de Dados

```
⊟ Frame 306 (524 bytes on wire, 524 bytes captured)
    Arrival Time: Jan 12, 2008 22:23:48.079604000
    [Time delta from previous packet: 0.000094000 seconds]
    [Time since reference or first frame: 761.884003000 seconds]
    Frame Number: 306
    Packet Length: 524 bytes
    Capture Length: 524 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80]
⊞ Ethernet II, Src: HonHaiPr_c6:74:e2 (00:19:7d:c6:74:e2), Dst: IntelCor_95:11:82 (00:13:20:95:11:82)
⊞ Internet Protocol, Src: 192.168.10.203 (192.168.10.203), Dst: 10.1.1.1 (10.1.1.1)
⊞ Transmission Control Protocol, Src Port: 1164 (1164), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 470
⊟ Hypertext Transfer Protocol
  ⊞ GET /hag/pages/home.ssi HTTP/1.1\r\n
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms
    Accept-Language: pt-br\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)\r\n
    Host: 10.1.1.1\r\n
    Connection: Keep-Alive\r\n
  ⊞ Authorization: Basic YWRtaW46cGlwb2NA\r\n
    Cookie: userCookie=YWRtaW46cGlwb2NA\r\n
    \r\n
```

5 CONSIDERAÇÕES FINAIS

Em situações de litígio envolvendo contratações via Internet a maior dificuldade encontra-se na comprovação do contrato realizado, bem como, nos detalhes envolvidos nesta contratação. Esta dificuldade surge do fato das relações contratuais não serem mais obrigatoriamente presenciais, necessitando, portanto, de mecanismos auxiliares para efetivação destas contratações e, ainda, se necessário de ferramentas computacionais que permitam registrar e demonstrar que o contrato foi realizado.

Assim, o protocolo de autenticidade proposto no presente trabalho, e que vem sendo desenvolvido, permitirá que ambos interessados, consumidor e fornecedor, mantenham registros (arquivos de *log*) contendo informações sobre o contrato realizado via Internet. Este registro será composto por diversas informações, destacando-se o registro dos IPs das máquinas envolvidas na transação. Deste modo, o consumidor poderá emitir relatório dos acessos ao site do fornecedor, bem como dos contratos realizados via Internet. O importante é o consumidor poder resgatar, a partir da sua

máquina, dados e informações sobre o site reclamado, ou seja, do fornecedor. Ou, ainda, o consumidor terá condições de validar as informações relatadas pelo fornecedor. Assim, com a utilização do protocolo de autenticidade estará, de fato, sendo mapeada por meio do arquivo de *log* a operação realizada via Internet, com o registro íntegro e seguro dos principais elementos da contratação redigida (parte, objeto, local da celebração, data, etc.).

AGRADECIMENTOS

Este trabalho vem sendo realizado com apoio financeiro do CNPq através do projeto de pesquisa: "Segurança Jurídica na Contratação via Internet" (Proc. No. 471627/2006-2 - Apoio a Projetos de Pesquisa / Edital MCT/CNPq 02/2006 - Universal).

REFERÊNCIAS

ATKINS, Derek; BUIS, Paul; HARE, Chris; KELLEY, Robert; NACHENBERG, Carey; NELSON, Anthony B.; PHILLIPS, Paul; RITCHEY, Tim; SHELDON, Tom; SNYDER, Joel. **Internet security professional reference**, Second Edition. New Riders Publishing, 1997.

BEHRENS, Fabiele. **A assinatura eletrônica como requisito de validade dos negócios jurídicos e a inclusão digital na sociedade brasileira**. Curitiba, 2005. 134 p., Dissertação de Mestrado, Centro de Ciências Jurídicas e Sociais, Pontifícia Universidade Católica do Paraná, 2005.

BOIAGO JUNIOR, José Wilson. **Contratação eletrônica: aspectos jurídicos**. Juruá Editora, Curitiba, 2005.

COMER, Douglas E., **Internetworking with TCP/IP: principles, protocols, and architecture**, Second Edition. Prentice-Hall International, Inc., Vol. 1, 1991.

DIAS, Jean Carlos. **Direito contratual no ambiente virtual**. Juruá Editora, 2ª. Edição. Curitiba, 2006.

GARFINKEL, Simson; SPAFFORD, Gene. **Web security & commerce**. O'Reilly & Associates, Inc., 1997.

MATTOS, Analice Castor de; EFING, Antônio Carlos, **Aspectos relevantes dos contratos de consumo eletrônicos**. Curitiba, 2007. 156 p. Dissertação de Mestrado – Programa de Pós-graduação em Direito Econômico e Social, Pontifícia Universidade Católica do Paraná.

REZENDE, Afonso Celso Furtado de. **Tabelionato de notas e o notário perfeito: direito de propriedade e atividade notarial**. Copola Livros, Campinas, 1997.

RELVAS, Marcos. **Comércio Eletrônico**. Juruá Editora, Curitiba, 2006.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: visão executiva da segurança da informação**. Elsevier, Rio de Janeiro, 2003.

SCHNEIER, Bruce, **Applied cryptography: protocols, algorithms , and source code in C**. John Wiley & Sons, Inc., Second Edition, 1996.