



Continuação

12/09/1998

Neste caso, a liberdade de expressão, prevista na Primeira Emenda da Constituição Americana, prevaleceu sobre a restrição do acesso por crianças a material considerado impróprio.

Com a derrubada desta lei, os Estados Unidos estão estudando soluções, baseadas na tecnologia, para afastar certos aspectos da Internet considerados “desagradáveis”, como por exemplo este problema da proteção infantil. Para isto, têm sido desenvolvidos *softwares* que permitem a seleção do material disponível na rede, permitindo às crianças o acesso a sites interessantes da rede, ao mesmo tempo que o *software* bloquearia os sites impróprios. Dessa forma, estariam protegidos tanto as crianças, quanto o direito de expressão dos adultos.

Outra solução, proposta por senadores americanos, é a criação de leis de incentivo para que os sites da Internet possuam classificação. Os *softwares* de filtragem dependem de uma classificação do material, semelhante àquelas utilizadas nos sistemas de seleção de filmes e de programas da televisão, que também constituem uma inovação no que se refere à passagem da censura das mãos dos órgãos oficiais para as mãos dos pais e responsáveis pela educação das crianças.

Há ainda o debate a respeito da responsabilidade dos servidores de informações, no que se refere ao conteúdo das mensagens e informações que circulam pela rede. Já houve casos em que os servidores da rede foram responsabilizados pelo material por eles veiculados. A maioria dos litígios referentes a material ofensivo veiculado pela Internet tem como alvo os serviços de acesso à rede, que são mais facilmente localizados pelo ofendido do que o próprio ofensor.

No entanto, normalmente o judiciário considera os provedores de acesso e os provedores de informação como não sendo responsáveis pelo material que veiculam, pois não é possível haver uma estrutura de fiscalização pelos provedores do referido material, para detectar a existência de temas impróprios ou ofensivos ao público.

De um modo geral, as tentativas de regulamentação e restrição do uso da Internet não têm sido recebidas com bons olhos pela comunidade em geral.

Mas os projetos de limitação à livre utilização da Internet não cessam de surgir. Tomando uma vez mais um exemplo ocorrido nos Estados Unidos, uma lei do Estado da Georgia visa proibir a prática do uso de pseudônimos nas relações *on-line*. Esta lei foi aprovada como uma medida anti-fraude, mas seus efeitos negativos podem ser maiores do que as vantagens que sua aplicação traria, pois restringiria mais uma vez a liberdade de comunicação de milhares de usuários da rede que utilizam pseudônimos em suas conversas *on-line*. O governo da Georgia, no entanto, aceitou não aplicar esta lei enquanto não for solucionada a questão de sua constitucionalidade.

O problema das tentativas de regulamentação da Internet é que esta nova tecnologia apresenta certos aspectos que são, até o momento, incompatíveis com o potencial regulamentador existente. Um dos motivos, já comentado, é a internacionalidade da Internet. Outro problema, relacionado diretamente à censura, é a distinção, que a maioria das legislações dos países hoje em dia faz, entre comunicação privada e particular. Assim, em uma conversa particular podem ser ditas coisas que jamais poderiam ser veiculadas pelos meios de comunicação tradicionais, como o rádio e a televisão. Como a Internet apresenta características de comunicação particular (pois só acessa a mensagem quem quer, e às vezes esta mensagem é direcionada a uma pessoa ou público em especial) e de comunicação pública (pois as informações estão à disposição de quem quer que acesse a rede), o mais aconselhável seria utilizar a legislação existente, para a solução de eventuais conflitos, e evitar a regulamentação da utilização da rede, até que suas características e potencialidades tenham sido melhor definidas.

3. O Comércio e a Prestação de Serviços via Internet

3.1. A Segurança nas Transações On-line

Existe uma grande expectativa referente ao desenvolvimento do comércio realizado via Internet. A grande maioria dos usuários da rede possui um padrão de vida elevado, com uma alta média de rendimento anual e considerável grau de cultura. O público-alvo do comércio a ser realizado via Internet constitui, portanto, um mercado promissor.



No entanto, apesar de ter havido crescimento considerável no que se refere à oferta de produtos e serviços pela rede, além da adoção das transações *on-line* por um número cada vez maior de bancos para a prestação de serviços, o que se tem verificado é que o que ocorre via Internet é, na verdade, a proposta de contratação e o oferecimento de produtos, e não a realização do negócio em si. Este fato se deve especialmente às dificuldades de realização e comprovação do pagamento, insegurança em relação às garantias oferecidas ao comprador, à qualidade dos produtos, etc.

Tais dificuldades serão superadas ou minimizadas com a aplicação e divulgação de novas tecnologias que oferecerão uma maior segurança no que se refere ao sigilo das operações e à segurança do pagamento pelo bem ou serviço adquiridos.

Uma das maneiras de se proteger o conteúdo das informações que são transmitidas via Internet é a criptografia, ou seja, a transformação de uma mensagem em uma forma ininteligível. Dessa forma, a mensagem é transmitida via rede, e será lida somente pelo destinatário, que possuirá a “chave” capaz de recompor a estrutura inicial da mensagem.

A codificação pode ser feita mediante a utilização de um só código, aplicado tanto para criptografar quanto para descriptografar o texto transmitido. Essa forma não oferece muita segurança, nem possibilita que se tenha certeza sobre quem é o destinatário e quem é o receptor da mensagem, pois sendo a chave de conhecimento tanto do remetente quanto do destinatário, o sigilo fica comprometido.

A forma mais segura é a utilização de duas chaves distintas, sendo uma utilizada para a transmissão de mensagens, de conhecimento exclusivo do remetente, e outra para a decodificação desta mensagem, de conhecimento exclusivo do destinatário. A característica mais importante deste sistema é que uma chave não pode ser deduzida de sua correspondente, ou seja, há uma grande dificuldade em se quebrar o sigilo destes códigos. Além disso, estas chaves, ou códigos, são desenvolvidas por cientistas mediante a aplicação de princípios matemáticos, o que certamente dificulta ou quase impossibilita a descoberta e “quebra” do segredo por pessoas não especializadas.

O sistema de utilização de chaves “públicas” e “privadas”, além de garantir o sigilo das transações ocorridas em rede, possibilita a identificação do remetente e do receptor, uma vez que é atribuída ao remetente uma chave privada, de conhecimento exclusivo deste, enquanto que o destinatário deverá saber a chave pública, correspondente à chave privada do remetente, que é a única capaz de decodificar a mensagem por ele enviada. A utilização da chave privada funciona, portanto, quase que como uma assinatura eletrônica.

A criptografia também é utilizada para codificar o número de cartões de crédito, para realizar pagamentos via Internet, e também para proteger operações com alto potencial de risco quando realizadas via Internet.

O desenvolvimento de *softwares* capazes de criar e aplicar sistemas de codificação semelhantes ao exemplo exposto acima é de fundamental importância para o futuro do comércio realizado na Internet, pois apesar da grande expectativa que o acesso a tamanho público consumidor cria, tanto comerciantes quanto consumidores estão receosos em investir neste tipo de negociação. Tanto é que algumas empresas, como a Mastercard, Visa e American Express estão desenvolvendo programas piloto para uniformizar a linguagem e sistemas utilizados para a criptografia de números de cartão de crédito e de *e-cash*, tanto para a realização de pagamento com segurança, quanto para a manutenção do sigilo necessário em operações de alto risco, que poderão ser realizadas via rede.

Já existem no mercado empresas especializadas em oferecer o acesso a esta tecnologia de segurança no que se refere ao pagamento de transações ocorridas *on-line*. Mediante o cadastramento do número do cartão de crédito do cliente, a empresa cria uma espécie de carteira de crédito para o cliente, e o coloca em contato com os comerciantes e empresas que oferecem produtos e serviços na Internet. Os valores correspondentes à compra de mercadoria serão debitados na conta do cliente (na verdade, de seu cartão de crédito), mediante a autorização deste. A segurança é garantida, pois o número do cartão de crédito não circula pela rede.

Este sistema, que é uma das formas de *e-cash* (que será explicado no item 3.2., abaixo) possibilita, por exemplo, a realização de pequenos pagamentos, em qualquer parte do mundo, e em qualquer moeda de pagamento. Dessa forma, a empresa fornecedora de tecnologia de segurança funciona como um intermediário entre os internautas e os comerciantes, viabilizando os meios de pagamento.

A utilização da criptografia tem sido reconhecida como ferramenta indispensável para a proteção da propriedade intelectual, da integridade e confiabilidade de informações financeiras, da integridade da segurança individual e pública, além da segurança nas operações do comércio eletrônico. A criptografia garante a confidencialidade, a autenticidade e a



integridade das mensagens transmitidas via rede, e a tendência mundial é buscar o desenvolvimento desta e de novas tecnologias para viabilizar o crescimento dos negócios realizados via Internet.

O destino do comércio via Internet ainda é uma incógnita. As opiniões passam da crença de que haverá uma explosão nos usos comerciais da rede, com a diminuição drástica das vendas “tradicionais” e o aumento do contato direto entre o consumidor e o fabricante, para a afirmação dos mais céticos de que a Internet nada mais é do que um meio de comunicação, alternativo ao telefone ou à presença física das partes, para realizar encomendas.

Para os que apostam no maior nível de desenvolvimento do comércio na rede, as vendas via Internet trariam inúmeros benefícios, como o fácil acesso a produtos e consumidores situados nas áreas mais remotas do globo, a redução dos preços, devido ao acirramento da concorrência e da facilidade de pesquisa de preços pelo cliente, dentre outras vantagens.

A realidade aponta para um crescimento neste tipo de comércio principalmente na área de venda de *softwares*, informativos, livros, CD-ROM, etc, que são mercadorias que podem efetivamente ser transmitidas ao computador do cliente via rede.

Mas o simples fato de existir uma alternativa para a compra de produtos de qualquer espécie, que possibilite que o consumidor, quer por motivo de dificuldade de acesso a esses produtos, quer por uma questão de urgência, satisfaça suas necessidades sem sair de casa ou do escritório, ou possibilite a realização da compra de qualquer parte do mundo onde o cliente estiver, constitui uma enorme inovação, uma nova porta de acesso ao mercado para comerciantes e consumidores.

3.2. *Novas Formas de Pagamento*

Com o grande interesse em desenvolver o mercado potencial oferecido pela Internet, estão surgindo novas alternativas para efetuar o pagamento das transações ocorridas em rede com segurança e sigilo. Uma das novas e polêmicas alternativas desenvolvidas, que também utiliza as técnicas de criptografia, é o dinheiro eletrônico ou *e-cash*. Polêmica, porque o desenvolvimento deste novo sistema de pagamento vem desafiar as estruturas que permitem a normatização e regulamentação das transações financeiras pelos órgãos de controle dos governos nacionais.

São chamados *e-cash* vários mecanismos de pagamento, que não as formas “físicas” tradicionais, desenvolvidos para proporcionar sigilo e segurança, e ao mesmo tempo rapidez, nas transações ocorridas em rede. Para este fim, são utilizados nas transações serviços de informação e manejo de dados, juntamente com os serviços de segurança (criptografia). A criptografia protege o teor das negociações e verifica a integridade da informação recebida, evitando desta forma a interceptação por terceiros.

Ao contrário das formas tradicionais de transferência de fundos, o valor monetário é diretamente transferido pelo computador do próprio usuário a qualquer instituição financeira, ou diretamente para o computador do credor da transação. O resultado é um sistema confidencial e extraterritorial, que foge a qualquer regulação estatal, de transferência de valores.

O *e-cash* pode ser classificado em duas categorias: o *e-cash* que utiliza os serviços bancários tradicionais para realizar as transferências de fundos e o *e-cash* que dispensa qualquer regulação ou intervenção das instituições financeiras tradicionais, pois os recursos (valores) ficam armazenados nos computadores dos próprios usuários.

Na primeira forma, apesar de existir sigilo nas transações, há a possibilidade de se fazer uma espécie de “rastreamento” das informações criptografadas, o que permite às instituições e ao governo um certo controle das transferências de valores. Esse é o modelo mais utilizado hoje em dia pela maioria dos bancos e empresas de cartão de crédito.

A segunda categoria implica na utilização do dinheiro digital, ou seja, os recursos financeiros ficam armazenados no computador do usuário em forma de dados digitais. Um exemplo deste tipo de *e-cash* é um sistema aplicado na Holanda, mediante o qual o usuário utiliza moeda corrente holandesa para comprar “dinheiro digital” de um banco, que fica armazenado no computador do usuário. O usuário pode pagar por suas negociações com este dinheiro digital, mediante o envio de seqüências numéricas, representativas do *e-cash*, ao computador do credor da negociação. Este, por sua vez, pode transmitir as seqüências numéricas ao seu banco, que efetua o depósito em sua conta bancária.

Não é possível rastrear a seqüência numérica representativa do dinheiro eletrônico, pois a criptografia impede que os bancos envolvidos na operação detectem os autores das transferências de valores de uma conta para outra. Só é possível



ao banco verificar se a seqüência numérica é válida ou não, proporcionando o mais absoluto sigilo nas transações. É claro que este tipo de serviço ainda se encontra em fase de teste e desenvolvimento, e provavelmente levará mais tempo para ter a aceitação no mercado.

O interesse no desenvolvimento de novas formas de pagamento eletrônico tem unido empresas anteriormente competidoras entre si em alianças para o aperfeiçoamento desses recursos e aquisição de uma posição predominante no mercado. Um exemplo disso foi a união da VISA, MasterCard, GTE, IBM, Microsoft e outras entidades para desenvolver o Sistema de Segurança nas Transações Eletrônicas (*Secure Eletronic Transaction -SET*), que também envolve a utilização de chaves públicas e privadas de criptografia, e procura uniformizar os métodos de sua aplicação, favorecendo, dessa forma, a rapidez e a liquidez do dinheiro eletrônico.

Uma das conseqüências sérias trazidas por este tipo de movimentação financeira é a impossibilidade de controle das remessas de dinheiro, tanto dentro dos países como internacionalmente, pelos organismos de controle tradicionais. Até o momento, tanto os governos nacionais quanto as demais entidades responsáveis pela regulamentação financeira não intervieram no processo de criação desses sistemas. Mas sem dúvida será motivo de preocupação para os órgãos reguladores tradicionais quando a utilização desses novos sistemas passarem a permitir, com facilidade nunca vista anteriormente, a remessa e o ingresso de recursos entre os países. Com certeza, a regulamentação neste sentido virá assim que a utilização dos sistemas de *e-cash* passarem a representar movimentação expressiva de recursos, com maior aceitação do mercado.

Continua em *Artigos*

Fonte: <https://conjur.jumps.com.br/1998-set-12/continuacao-3-2/>