Questões legais do uso da certificação digital na proteção dos direitos de autor de programa de computador

Hélio Santiago Ramos Júnior

***Abstract*—**Este trabalho se propõe a discutir eventuais implicações legais relativas ao uso da certificação digital na proteção dos direitos de autor de programa de computador em virtude da possibilidade de adoção de um modelo de proteção de programa de computador por certificação digital proposto na Universidade Federal de Santa Catarina com o objetivo de coibir de forma mais eficaz a pirataria de programa de computador.

Palavras-chave—Programa de computador, certificação digital, direito do consumidor.

I. INTRODUÇÃO

No Brasil, a Lei 9.609, de 19 de fevereiro de 1998, conhecida como lei do software, dispõe sobre a propriedade intelectual do programa de computador bem como sua comercialização no país. Ela traz, em seu artigo primeiro, o conceito jurídico de programa de computador e, no seu art. 12, tipifica como crime específico a violação de direito de autor de programa de computador.

A doutrina faz distinção entre programa de computador e software, considerando que este último difere do programa de computador na medida em que o seu conceito é mais abrangente, podendo ser utilizado para se referir, além do programa de computador, também aos seus acessórios que inclui os materiais de apoio relacionados ao programa.

Neste sentido, "software abrange, além do programa de computador em si, que é a linguagem codificada, também a descrição detalhada do programa, as instruções codificadas para criar o programa, a documentação escrita auxiliar deste, bem como outros materiais de apoio relacionados"

(Wachowicz, 2004, p. 71)

Esta diferença é importante porque o programa de computador é protegido pela Lei 9.609/98 enquanto que os materiais de apoio relacionados ao programa, sendo considerado obras intelectuais, são tutelados pela Lei 9.610/98 (Lei de Direitos Autorais).

Em 2001, um modelo de proteção de programa de computador por certificação digital foi proposto por João Luiz

Francalacci Rocha em uma banca de mestrado no Centro de

Ciências da Computação da Universidade Federal de Santa Catarina com a finalidade de propor uma forma mais eficaz de combate à pirataria de programa de computador.

De modo geral, este modelo de proteção tem como principal característica o fato de vincular o registro da licença de uso do programa de computador ao certificado digital do usuário para impedir o uso não autorizado e a comercialização ilegal de cópia de programa de computador.

Naquela ocasião, o próprio autor reconheceu que ainda há muito que ser feito para viabilizar a proteção de programa de computador por certificação digital, neste sentido, salientou que "a questão jurídica que envolve o termo de contrato entre produtor e usuário também deve ser alvo de pesquisa no campo do direito, respeitando, claro, o lado do consumidor, mas provendo termos legais e eficazes que reforcem a aliança entre o usuário, software e certificados". (Rocha, 2001, p. 75).

De tal sorte, dada a importância do tema, o presente trabalho se propõe a examinar a compatibilidade do modelo de proteção de programa de computador proposto por Rocha com as normas do ordenamento jurídico brasileiro, principalmente no que concerne aos direitos do consumidor, refletindo sobre suas implicações legais e, ao final, propõe-se alternativas para solucionar os problemas identificados, visando a sua adequação à lei.

II. A CERTIFICAÇÃO DIGITAL E A ICP-BRASIL

Antes de comentar sobre o modelo de proteção de programa de computador por certificação digital, é fundamental aprofundar um pouco o estudo sobre a criptografia, o contrato eletrônico e a assinatura digital para um melhor esclarecimento sobre a certificação digital e como ela poderá contribuir para proteger os direitos de autor de programa de computador.

A. A criptografia

O Instituto Nacional de Tecnologia da Informação (ITI) define a criptografia como sendo "um ramo das ciências exatas que tem como objetivo escrever em cifras. Isso ocorre em função de um conjunto de operações matemáticas que transformam um texto claro em um texto cifrado".

A criptografia é utilizada para evitar a violação de uma informação constante em um documento, através da transmissão de um texto cifrado pelo emissor para o receptor o qual, ao receber o documento cifrado, decifra-o, tornando-o,

assim, legível o conteúdo do texto emitido.

Em 2000, Corrêa já havia observado a importância da criptografia, apontando, inclusive, dentre as diversas vantagens da sua utilização, por exemplo, a possibilidade de contribuir para a proteção da propriedade intelectual: "Por que precisamos da criptografia na grande rede? Por vários motivos; dentre eles poderíamos citar: tornar original uma mensagem enviada por correio eletrônico, mediante a utilização de assinaturas digitais; tornar documentos pessoais inacessíveis e, assim, privados; verificar a identidade de outra pessoa online, que esteja acessando a rede; verificar a fonte provedora de um arquivo que está sendo copiado, em outras palavras, tornar o download mais seguro; proteger transações financeiras; habilitar o fluxo de caixa digital na internet; proteger a propriedade intelectual; evitar opiniões ilegais e puni-las; proteger a identidade e a privacidade de todos" (p.82).

Embora a criptografia seja um método bem antigo de codificar mensagens, a tecnologia veio a utilizar suas técnicas para dar soluções a problemas hodiernos, passando a garantir não somente a privacidade e o sigilo de documentos, mas, também, adaptou-se no sentido de preservar a integridade e autenticidade do documento eletrônico.

Diante dos constantes avanços tecnológicos e do emprego cada vez maior das tecnologias da informação, pode-se dizer que existe uma grande possibilidade de se explorar e elaborar mecanismos que contribuam para impulsionar ainda mais o desenvolvimento da sociedade, no entanto, deve-se atentar para a proteção dos direitos fundamentais do cidadão em face das novas tecnologias.

Há dois tipos de criptografia que são a simétrica e a assimétrica.

A criptografia simétrica funciona com a utilização de duas chaves idênticas, ou seja, a chave para cifrar e a chave para decifrar um documento são a mesma de modo que o emissor assim como o receptor devem conhecer o segredo da chave.

Logo, para garantir a privacidade da informação transmitida, faz-se necessário que apenas ambos conheçam a chave. Portanto, na criptografia simétrica, por se tratar de uma mesma chave, qualquer receptor que tiver conhecimento da chave secreta poderá alterar o documento por ser esta chave correspondente a mesma tanto para sua cifração quanto para decifração.

Ao contrário da criptografia simétrica, a criptografia assimétrica, por sua vez, "utiliza um par de chaves diferentes entre si, que se relacionam matematicamente por meio de um algoritmo, de forma que o texto cifrado por uma chave, apenas seja decifrado pela outra do mesmo par" (ITI).

Na criptografia assimétrica, a chave que o emissor utilize para cifrar seu documento é denominada chave privada e deve ser de seu exclusivo conhecimento, enquanto que a chave pública é aquela que pode ser fornecida ao público, pois o conhecimento da chave pública apenas permite a leitura do documento e não a sua alteração.

Há algumas desvantagens que podem ser apontadas no que concerne ao uso da criptografia, como, por exemplo, a possibilidade de utilizá-la para a troca de mensagens entre criminosos com o objetivo de violar a lei.

Acontece que os agentes que utilizam a criptografia para a troca de mensagens não são obrigados a produzir prova contra si mesmos. Além disso, mesmo se houvesse uma determinação judicial autorizando a quebra do sigilo destas mensagens para o fim de investigação criminal ou instrução processual penal, isto seria uma tarefa muito difícil.

Esta dificuldade está consubstanciada no fato de que os programas de criptografia são potentes e a sua quebra demoraria alguns anos o que possivelmente levaria à prescrição dos supostos delitos que tenham sido cometidos, sendo que os infratores poderiam ainda ser inocentados com base no princípio de que, na dúvida, deve-se inocentar o réu, uma vez que não se teria conhecimento do conteúdo da mensagem privada.

A relevância deste assunto que envolve a segurança nacional em face do uso da criptografia por criminosos e terroristas foi o tema central de ficção científica na obra "Fortaleza Digital", onde o autor explica bem a noção de criptografia:

"A codificação por chave pública era um conceito ao mesmo tempo simples e brilhante. Consistia no uso de um programa simples, para computadores pessoais, que alterava as mensagens de e-mails de tal forma que estas se tornavam impossíveis de ler. Os usuários passaram a poder escrever suas mensagens e codificá-las usando um programa desse tipo. O texto resultante parecia um bloco de caracteres aleatórios e sem sentido: um código. Qualquer um que interceptasse a mensagem iria ver apenas lixo em sua tela. A única maneira de decifrar o código era digitar a senha do remetente - uma série secreta de caracteres que funcionava basicamente como a senha de um cartão de crédito. Geralmente, as senhas eram longas e complexas e transportavam as informações para transmitir ao algoritmo de decodificação as operações matemáticas necessárias para recriar a mensagem original. Os usuários desses programas voltaram a poder, então, enviar emails com total confiança. Mesmo se a transmissão fosse interceptada, apenas aqueles que tivessem a chave poderiam decifrá-la" (Brown, 2005, p. 27).

B. O contrato eletrônico

A ausência de leis nos países referentes ao comércio eletrônico fez surgir a Lei-Modelo da UNCITRAL sobre comércio eletrônico que estabeleceu princípios para auxiliar os países na criação de suas legislações internas sobre o tema.

Dentre estes princípios, destacam-se "o reconhecimento das informações e das mensagens de dados e a igualdade entre o documento eletrônico e os registrados em papel; o reconhecimento legal da assinatura digital; a notificação de recibo de documentos, tempo e lugar de despacho e de recibo das mensagens de dados". (Leite, 2003, p.226).

O desenvolvimento do comércio auxiliado principalmente pela crescente utilização da Internet como um meio de

comunicação trouxe como conseqüência a necessidade de celebração de contratos através do meio eletrônico.

O contrato eletrônico deve ser compreendido como sendo um negócio jurídico celebrado através de meios eletrônicos onde as partes manifestam a vontade de assumir um compromisso recíproco e honrar com as disposições acordadas.

Há muitos contratos eletrônicos que consistem em contratos de adesão, ou seja, contratos preestabelecidos unilateralmente cujas cláusulas não foram discutidas nem acordadas entre as partes. Em geral, estes contratos recebem a denominação de clickwrap tendo em vista que o usuário manifesta a aceitação das cláusulas contratuais com um simples click do mouse.

Os contratos eletrônicos de adesão consistem em negócios jurídicos celebrados através do meio eletrônico onde diversas empresas oferecem seus serviços ou produtos e apresentam um contrato com as cláusulas preestabelecidas.

Deste modo, em se tratando de contrato de adesão, o usuário contratante, caso queira utilizar os produtos ou serviços da empresa, não tem outra alternativa senão se submeter a aceitar as cláusulas que constam no contrato as quais não foram acordadas entre ambos mas sim imposta por uma das partes contratantes, cabendo a outra apenas aceitar o contrato na íntegra ou recusá-lo.

O usuário contratante deve estar atento às cláusulas contidas nos contratos eletrônicos de adesão, e, por estas cláusulas contratuais serem estabelecidas unilateralmente, "deve-se recusar validade àquelas que sejam abusivas, isto é, que causem manifesto desequilíbrio do contrato, por reduzirem unilateralmente as obrigações do predisponente (a parte mais forte), em prejuízo dos clientes, ou por agravarem as destes, de forma que seja socialmente sentida como ilegítima" (Noronha, 2004, p.34).

Em relação à forma de manifestação de vontade nos contratos eletrônicos de adesão, especialmente naquela onde se considera o aceite dos termos através do click do mouse, cabe a observação de que "este tipo de declaração, que em muitos casos implica, inclusive, em renúncia a direitos, não pode ser manifesto apenas por um simples click, como nos contratos clickwrap" (Ventura, 2001, p. 68).

Há questões relativas aos contratos eletrônicos que devem ser esclarecidas pelo direito para a perfeita caracterização e identificação da celebração de um contrato eletrônico. Por exemplo, em se tratando dos contratos eletrônicos celebrados através da troca de e-mails, entende-se que há, neste caso, contratação entre ausentes por ser similar a uma contratação por correspondência.

Assim, quando se trata dos contratos entre ausentes, "o ordenamento jurídico brasileiro adota a teoria da expedição, ou seja, o contrato oriundo da troca de e-mails estaria formado no momento em que o oblato expedisse sua resposta aceitando os termos da proposta (anteriormente encaminhada por email)" (Glitz, 2003, p.190).

Há diversas preocupações ao se realizar uma celebração de um contrato por meio eletrônico, dentre estas, destaca-se a questão de identificação das partes e da integridade do conteúdo dos documentos eletrônicos por não haver a possibilidade de confirmação do endereço físico, veracidade da identidade e capacidade jurídica dos contratantes.

A respeito da integridade do documento, aponta-se a possibilidade da alteração do documento eletrônico, da alegação de não recebimento, ou de recebimento com conteúdo diverso do enviado, e de se interceptar informações contidas remetidas eletronicamente.

Desta forma, "percebe-se a importância de conseguir garantir que estes não sofreram alterações posteriores a sua concepção. Busca-se então a certeza da integridade do documento, para que possa haver também a certeza de que o conteúdo permaneceu inalterado" (Hammes, 2004, p.43).

C. Os documentos eletrônicos e a assinatura digital

A atribuição de valor probatório aos documentos eletrônicos é um dos pressupostos para que se possa garantir uma segurança nas atividades desenvolvidas eletronicamente, pois, sendo o documento eletrônico considerado válido como meio de prova, ele poderá ser utilizado, por exemplo, para provar a existência de um negócio jurídico.

No art.212, inc. II do Novo Código Civil, tem-se que "salvo o negócio a que se impõe forma especial, o fato jurídico pode ser provado mediante: II - documento". Pode-se entender que este termo documento expresso no Código Civil brasileiro tenha um sentido amplo o que permitiria a utilização do documento eletrônico como meio de prova.

Há também o princípio da livre apreciação de provas pelo juiz, neste caso, se o juiz confiar na autenticidade do documento eletrônico, poderá considerá-lo como meio de prova válido.

Assim, conforme consta no art. 131 do Código de Processo Civil: "O juiz apreciará livremente a prova, atendendo aos fatos e circunstâncias constantes dos autos, ainda que não alegados pelas partes; mas deverá indicar, na sentença, os motivos que lhe formaram o convencimento".

Ainda, o Código de Processo Civil de 1973, no caput de seu art. 332, estabelece que "todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa".

Desta forma, o Código de Processo Civil permite a abrangência de outros meios de prova desde que sejam meios legais e moralmente legítimos, assim, ao se garantir a integridade e autenticidade dos documentos eletrônicos, eles passam a ser dignos de eficácia probatória.

A Medida Provisória n. 2.200/01 criou a Infra-Estrutura de Chaves Públicas (ICP-Brasil) e teve como objetivo dar validade aos documentos eletrônicos, e, em seu art.10, caput, considerou-os como documentos públicos ou particulares para todos os fins legais.

Estabeleceu ainda uma presunção de veracidade para os documentos eletrônicos que forem assinados digitalmente e que utilizassem os certificados da ICP-Brasil. Desta forma, os documentos eletrônicos passam a ter a mesma validade

jurídica dos documentos em papel.

De acordo com o ITI, a assinatura digital pode ser conceituada como "uma modalidade de assinatura eletrônica, resultado de uma operação matemática que utiliza algoritmos de criptografia assimétrica e permite aferir, com segurança, a origem e a integridade do documento".

Acerca deste assunto, comenta Blum (2002, p. 148) que:

"A Assinatura Digital, por chaves públicas, oferece um elevado nível de segurança, proporcionando uma presunção muito forte de que o documento onde se encontra foi criado pela pessoa que dela é titular e, assim, satisfaz o objetivo do legislador na exigência de assinatura para atribuição de valor probatório aos documentos escritos. (...) para que este processo se desenvolva é necessário que haja uma autoridade certificadora, que reunirá os dados necessários para identificar cada portador de chaves (pública e privada). O papel da autoridade certificadora é criar, ou possibilitar a criação de um par de chaves critográficas (a chave pública e a chave privada) para o usuário, além de atestar a identidade do mesmo (conferindo, minuciosamente, sua identidade física pelos meios tradicionais). A certificadora emite um "certificado" contendo a chave pública do usuário e esse certificado acompanhará os documentos eletrônicos assinados, conferindo as características essenciais da integridade e da autenticidade".

No que se refere ao nível de segurança em razão do uso da assinatura digital em documentos eletrônicos, salienta Volpi que "a assinatura digital, atualmente fundamentada na tecnologia de autenticação, possibilita uma real segurança ao seu usuário, desde que preze pela constante evolução dos algoritmos, a fim de evitar o aprimoramento pelos especialistas em decifragem, também conhecidos como criptoanalistas" (2002, p. 380-381).

Há diversas vantagens em se assinar digitalmente um documento eletrônico, dentre elas, pode-se destacar a garantia da integridade, isto é, que o documento não sofreu alterações, e também a garantia de que o documento é autêntico, ou seja, a certeza de que o documento foi elaborado pelo verdadeiro autor.

Trata-se de garantias que podem ser asseguradas com o uso da assinatura digital, pois, o documento eletrônico, na ausência desta ou de outro mecanismo similar qualquer que venha a ser elaborado, torna-se vulnerável a modificações indevidas.

Portanto, na sociedade atual, apresenta-se como fundamental o uso da assinatura digital para fornecer a garantia da integridade e autenticidade do documento em sua forma eletrônica.

Além da preocupação com a integridade e com a autenticidade do documento eletrônico, deve-se também direcionar a atenção para um outro elemento que também é de grande relevância quando se refere à segurança, trata-se da privacidade onde se deve buscar a preservação do sigilo do documento eletrônico.

A utilização da assinatura digital baseada na criptografia assimétrica protege o conteúdo dos documentos eletrônicos através da cifragem da mensagem com a chave pública do receptor, e, assim, com o uso de sua chave privada, ele poderá decifrar e ler a mensagem.

Deste modo, evita-se a falsificação e garante a autenticidade, uma vez que para realizar a assinatura é necessário ter o conhecimento da chave privada a qual por esta razão, deve ser de uso exclusivo de seu proprietário. Neste sentido, explica Peck que:

"No quesito segurança, o sistema de chaves 'públicas' e 'privadas', além de garantir o sigilo das transações ocorridas na rede, possibilita a identificação do remetente e do receptor, uma vez que é deverá saber a chave pública, correspondente à chave privada do remetente, que é a única capaz de decodificar a mensagem enviada. Sendo assim, a chave privada funciona como uma assinatura eletrônica" (2002, p. 74).

A adoção da assinatura digital com base na criptografia assimétrica, na medida em que fornece as garantias fundamentais para o estabelecimento de um ambiente seguro na celebração de negócios jurídicos em meio eletrônico, permite que diversas atividades venham a adotar o meio eletrônico por identificar nele uma alternativa para a prestação de um serviço com maior praticidade, celeridade e garantia de segurança.

A tecnologia, da mesma forma que cria novos paradigmas no âmbito do direito, também pode auxiliar a lei a solucionar os problemas decorrentes do avanço tecnológico e do desenvolvimento da sociedade, por exemplo, através da regulamentação e da utilização do certificado digital, o qual funciona como uma carteira de identidade eletrônica, permitindo assim que o cidadão seja reconhecido, podendo evitar fraudes no comércio eletrônico.

O certificado digital consiste em um documento eletrônico assinado digitalmente por uma autoridade certificadora, e que contém diversos dados sobre o emissor e o seu titular, e a sua função principal é vincular uma pessoa ou uma entidade a uma chave pública.

Desta forma, pode-se dizer que "a essência da certificação digital reside na possibilidade de garantir a autenticidade e a integridade do documento eletrônico, que é objeto caracterizador de uma transação virtual" (Kaminski, 2004, p.247).

Para adquirir um certificado digital, o cidadão interessado deve se dirigir a uma autoridade de registro, sendo identificado mediante a apresentação de documentos pessoais.

O certificado digital funciona analogicamente como uma carteira de identidade do indivíduo, desta forma, deve constar nele informações básicas, como a sua chave pública, dados pessoais, período de validade do certificado, nome da autoridade certificadora (AC) que emitiu o certificado, o número de série do certificado e a assinatura digital da AC.

III. O MODELO DE PROTEÇÃO DE PROGRAMA DE COMPUTADOR POR CERTIFICAÇÃO DIGITAL

O modelo de proteção de programa de computador por certificação digital proposto em 2001 no Centro de Ciências da Computação da Universidade Federal de Santa Catarina teve o objetivo de desenvolver uma alternativa eficaz para coibir o uso não autorizado e a distribuição ilegal de cópias de programa de computador.

Desta forma, buscou-se elaborar um modelo de proteção que tivesse propriedades capazes de quebrar o ciclo vicioso da pirataria de programa de computador, por exemplo, através da criação de mecanismos que pudessem auxiliar na tarefa de identificar o usuário infrator, responsabilizando-o pela violação aos direitos de autor de programa de computador.

A principal característica deste modelo de proteção é o fato de condicionar o registro do programa de computador ao certificado digital do usuário e assim fazer com que as cópias ilegais de programa de computador possam ser neutralizadas através da revogação do certificado de licença de uso do programa.

Para a sua viabilidade técnica, o autor do modelo de proteção adotou as providências necessárias: 1. a adoção de um padrão ASN-1 pré-definido e registrado pelo LabSEC, sob número: 1.3.6.1.4.1.7687.1.8.1. Este número representa a OID destinada ao Modelo de Proteção de Software por certificação Digital (...); 2. definição das extensões que conterão as restrições do uso destes certificados, como por exemplo, certificados destinados a licença de uso de determinado software de alguma empresa; 3. emissão de certificados digitais para teste do protótipo. Estes certificados são baseados na recomendação X.509v3 e contém as extensões necessárias para o uso do software (Rocha, 2001, p. 49).

No processo de licenciamento do programa de computador, o produtor ou a revenda funcionaria como uma autoridade de registro, ou seja, funcionaria como uma entidade responsável por verificar a veracidade dos dados informados pelo cliente, conferindo sua identidade e a autenticidade dos de seus dados.

Em seguida, há o processo de validação da licença de uso do programa de computador que é dividido em três fases.

A primeira fase tem início no momento que o usuário efetua a autenticação e aciona o programa de computador protegido, o qual verifica a existência de um certificado com extensão própria e chave privada correspondente sempre que o programa é inicializado. Em caso positivo, um desafio é gerado e depois assinado com a chave privada.

Na segunda fase, o programa de computador protegido solicita que a gerência de certificados aplique a chave pública contida no certificado para verificar a assinatura do resumo assinado na primeira parte do processo.

Na última fase do processo de validação, verifica-se se a validade do certificado não expirou; se a validade da lista de certificados revogados local não expirou; se o certificado não consta na lista de certificados revogados local ou remota.

Explica o autor que "o fato de ser o sistema operacional, através da gerência de certificados e não o software protegido, o encarregado de validar as operações ligadas ao certificado, dificulta a ação de usuários sofisticados que tentam 'quebrar' o código para retirar a proteção" (Rocha, 2001, p. 52).

Para a viabilidade do modelo de proteção, propõe o autor que seja firmado um contrato entre o usuário e a empresa de software, elegendo uma autoridade certificadora como válida entre as partes e estabelecendo ainda uma cláusula na qual os dados cadastrais do usuário serão transmitidos através da rede para confirmação das informações e averiguação de eventual existência de cópias piratas por meio do número da licença do programa de computador.

Dentre as vantagens da adoção deste modelo de proteção, além de desativar as cópias ilegais do programa de computador, desestimularia a pirataria do mesmo uma vez que seria possível identificar o usuário infrator através da sua ligação com o certificado de licença de uso do programa e, conseqüentemente, responsabilizá-lo pela violação dos direitos do autor de programa de computador.

A proteção de programa de computador por certificação digital desestimularia o usuário infrator a distribuir cópias do programa que comprou, pois "se este mesmo usuário quiser fazer uma cópia pirata e distribuí-la, necessitaria fornecer, junto com a cópia, o seu certificado e sua chave privada, o que poderia trazer inúmeras complicações para ele, pois o certificado digital está associado ao usuário através de um contrato e essa associação não pode ser negada" (Rocha, 2001, p. 37).

Por último, o modelo de proteção permitiria ainda determinar concessões de direito de uso do programa, previstas em contrato e estabelecidas pelo período de validade do certificado de licença de uso e proporcionar a personalização do programa de computador com base nas informações contidas no certificado de licença do programa.

IV. IMPLICAÇÕES LEGAIS DO MODELO DE PROTEÇÃO EM ANÁLISE

De início, uma questão que se impõe é saber se há legalidade na conduta da empresa de software que obriga o cliente a ter que adquirir um certificado digital para que possa obter a licença de uso do programa de computador.

O contrato de licença de uso de programa de computador, por se tratar de uma prestação de serviço que tem o usuário como destinatário final, caracteriza-se como uma relação de consumo, submetendo-se ao regime jurídico do Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990).

Este diploma legal assegura como um direito básico do consumidor, por exemplo, a proteção contra métodos comerciais coercitivos ou desleais, bem como práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços (art. 6º, inc. IV).

Na seção IV do Código de Defesa do Consumidor (CDC) que trata das práticas abusivas, tem-se o art. 39, caput e incisos I e V que, respectivamente, vedam ao fornecedor de produtos ou serviços, dentre outras práticas abusivas: condicionar o fornecimento de produto ou de serviço ao fornecimento de outro produto ou serviço, bem como, sem justa causa, a limites quantitativos; e exigir do consumidor vantagem manifestamente excessiva.

Desta forma, com fundamento na Lei nº 8.078/90, é possível argumentar que a empresa de software poderia estar cometendo uma prática abusiva ao obrigar o consumidor a ter que adquirir um certificado digital para que possa usufruir do serviço.

Acontece que, atualmente, há um custo para a aquisição do certificado digital do usuário junto a uma autoridade certificadora, o qual, de modo geral, é suportado pelo próprio usuário.

Trata-se de um ônus que a empresa de software criaria para o consumidor em virtude da adoção de um modelo de proteção por certificação digital o qual tem a finalidade específica de proteger a propriedade intelectual do programa de computador da empresa de software.

Assim, sob esta perspectiva, pode-se entender que, no caso em questão, há a incidência do art. 39, inc. V do Código de Defesa do Consumidor que considera como prática abusive a conduta de exigir do consumidor vantagem manifestamente excessiva.

Um segundo ponto importante é que, de modo geral, o contrato de licença de uso de programa de computador se caracteriza como um contrato de adesão, isto é, as cláusulas são estabelecidas unilateralmente pela empresa de software, restando ao consumidor a opção de aceitar ou recusar o contrato na íntegra.

Não se pode olvidar que o inciso IV do art. 51 da Lei nº 8.078/90 determina que são nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada, ou sejam incompatíveis com a boa-fé ou a eqüidade.

Nos termos do dispositivo legal mencionado, a conduta da empresa de software de obrigar o consumidor a ter que adquirir um certificado digital pode ser considerada uma obrigação iníqua na medida em que a empresa criou uma obrigação que antes não existia, além disso, ela poderia prestar o serviço de concessão de licença de uso de programa de computador ao usuário sem que tivesse que obrigá-lo a adquirir um certificado digital na hipótese de utilizar outro tipo de proteção.

Desta forma, para afastar eventual nulidade de cláusula contratual em razão de possível caracterização de venda casada, vantagem manifestamente excessiva ou obrigação iníqua no contrato de licença de uso do programa de computador, seria aconselhável estabelecer que eventuais encargos referentes ao uso da certificado digital sejam suportados pela empresa de software.

É oportuno salientar que o modelo de proteção do programa de computador por certificação digital não foi idealizado com a finalidade de prejudicar o consumidor, mas sim de desenvolver uma forma mais eficaz de proteção contra a pirataria de programas de computador. A questão consiste, portanto, em conciliar os interesses no sentido de tornar viável o modelo de proteção por certificação digital, assegurando-se os direitos do consumidor, protegendo os direitos de autor de programa de computador e ainda contribuindo para que o Estado possa garantir o desenvolvimento nacional.

Desta forma, o primeiro passo deve ser orientar o consumidor sobre todas as peculiaridades da proteção de programa de computador por certificação digital, pois o art. 6º, inc. III do Código de Defesa do Consumidor assegura como um direito básico do consumidor a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade e preço, bem como sobre os riscos que apresentem.

O contrato de licença de uso de programa de computador protegido por certificação digital, dada sua própria natureza e peculiaridade, caracteriza-se como um contrato de adesão, desta forma, com fundamento nos art. 51, inc. IV e §1º, inc. III do CDC, é aconselhável que a empresa de software estabeleça que o foro de eleição para dirimir controvérsias oriundas do contrato seja o domicílio do consumidor.

Além de estipular a eleição do foro em benefício do consumidor, o contrato de licença de uso de programa protegido por certificação digital precisa indicar também a escolha da autoridade certificadora que será responsável pela emissão dos certificados.

Pode-se optar por utilizar certificados emitidos pela ICPBrasil os quais são dotados de presunção de veracidade, como também é possível utilizar certificados não emitidos pela ICPBrasil desde que sejam admitidos pelas partes como válidos ou aceito pela pessoa a quem for oposto o documento, conforme previsão do art. 10, §§1º e 2º da MP 2.200/01.

Trata-se de uma cláusula muito importante haja vista que a existência de controvérsia em relação à autoridade certificadora pode comprometer o funcionamento do modelo de proteção de programa de computador por certificação digital, inviabilizando, conseqüentemente, a prestação do serviço.

Na atualidade, não existe nenhuma norma legal em vigência que assegure à empresa de software ou revenda o direito de atuar como uma autoridade de registro, responsável por identificar o cliente e fornecer os dados para a autoridade certificadora, a qual pode se recusar ou aceitá-la como uma autoridade de registro ou não sem que isso constitua um ato ilícito.

Acerca destas questões envolvendo a regulamentação legal, Peck comenta que “apesar de o Brasil ser bastante avançado na área tecnológica de criptografia (...), nossa legislação está bastante atrasada na regulamentação da assinatura e da certificação virtuais” (2002, p. 87-88).

De outra forma, a empresa de software não pode se eximir de sua responsabilidade civil pelos danos que causar em virtude da adoção do modelo de proteção por certificação digital, devendo sempre respeitar os direitos do consumidor.

Nos termos do art. 51, inc. I da Lei 8.078/90, são nulas as cláusulas contratuais relativas ao fornecimento de produtos ou serviços que impossibilitem, exonerem ou atenuem a

responsabilidade do fornecedor por vícios de qualquer natureza dos produtos e serviços ou impliquem renúncia ou disposição de direitos.

O art. 43, §2º do Código de Defesa do Consumidor determina que "a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele".

Em decorrência do disposto nesta norma, a empresa de software não pode incluir o certificado de licença de uso do programa de computador do usuário na lista de certificados revogados sem antes comunicar o consumidor por escrito, pois o certificado digital de licença de uso do programa nada mais é do que um documento eletrônico que contém dados pessoais do usuário.

A inclusão do certificado de licença de uso do programa de computador do usuário na lista de certificados revogados pode trazer transtornos para o consumidor, impedindo-o de ter acesso ao programa de computador, pois o programa, ao estar conectado à internet e realizar a consulta à lista de certifivados revogados, não mais funcionará, inviabilizando o acesso ao mesmo em razão da revogação do certificado.

Desta forma, é aconselhável que o contrato de licença de uso de programa de computador protegido por certificação digital estabeleça as hipóteses em que a empresa de software poderá incluir o certificado de licença na lista de certificados revogados, devendo, em todo o caso, avisar previamente o consumidor por escrito para evitar a sua responsabilização pelos danos morais decorrentes da inobservância aos preceitos legais.

Em razão da peculiaridade do contrato de licença e do modelo de proteção por certificação digital, o contrato celebrado entre as partes precisa observar o respeito às normas do Código de Defesa do Consumidor para que tenha viabilidade perante o ordenamento jurídico brasileiro.

Além de consagrar a defesa do consumidor como uma garantia fundamental do cidadão no art. 5º, inc. XXXII, a Constituição Federal também assegura o direito da propriedade intelectual do autor no art. 5º, inc. XXVII e ainda consagra o direito à privacidade no art. 5º, inc. X e XII.

A Carta Magna tem como um de seus objetivos fundamentais garantir o desenvolvimento nacional e esta finalidade se apresenta incompatível com a pirataria.

Entretanto, se, de um lado, existe o objetivo de proteger os direitos do autor de programa de computador e garantir o desenvolvimento nacional, por outro, existe o direito fundamental à privacidade.

A proteção da privacidade dos dados pessoais do cidadão transmitidos através da rede é fundamental para evitar, por exemplo, a ocorrência de danos devido ao conhecimento de informações as quais deveriam ser mantidas em sigilo.

Desta forma, para que o modelo de proteção proposto por Rocha esteja em harmonia com o direito à privacidade, deve-se assegurar ao usuário o direito de saber exatamente o conteúdo dos seus dados pessoais que estejam sendo enviados pela rede e a faculdade de interferir neste processo.

No modelo de proteção em análise, observa-se que algumas operações podem acontecer sem a interferência do usuário, de forma imperceptível e sem a sua anuência na transmissão de tais dados. Isto acontece, por exemplo, no processo de validação da licença de uso do programa de computador, ao verificar a validade do certificado digital.

Para evitar este problema, o modelo de proteção por certificação digital deve permitir que o usuário tenha conhecimento de todos os dados que serão transmitidos através da rede e que lhe seja assegurada a faculdade de interferir neste processo, possibilitando-o impedir, por exemplo, a verificação automática que consulta se o certificado não consta na lista de certificados revogados local.

Por conseqüência, para uma maior segurança juridical para as empresas de software, seria interessante uma cláusula contratual que estabeleça que na hipótese de o usuário se recusar a fornecer as informações essenciais para a validação do certificado digital, o processo de validação do programa será interrompido, de forma que o usuário não terá acesso ao programa, podendo implicar na rescisão do contrato de licença.

V. CONCLUSÃO

A tecnologia pode contribuir para proporcionar uma maior eficácia da lei, na medida em que cria mecanismos técnicos que podem auxiliar na tarefa de coibir a prática de comportamentos proibidos pela legislação vigente.

Para que seja viável o uso da certificação digital para proteger os direitos do autor de programa de computador, é necessário que o contrato firmado entre as partes observe o respeito aos direitos e garantias fundamentais do cidadão.

Desta forma, sugere-se que os encargos com a certificação digital sejam suportados pela empresa de software, pois, de outro modo, ela poderia estar cometendo uma prática abusiva ao obrigar o consumidor a ter que adquirir um certificado digital, junto a uma autoridade certificadora, para que possa usufruir do serviço.

É oportuno enfatizar que o consumidor tem direito à informação adequada e suficiente sobre os riscos que o negógico jurídico apresenta, portanto, a empresa de software tem a obrigação de esclarecê-lo sobre o funcionamento do programa de computador e das peculiaridades do modelo de proteção em todos os seus aspectos.

Além disso, por observância ao direito à privacidade do cidadão, o programa de computador protegido somente poderá transmitir as informações essenciais para o funcionamento do processo de validação da licença de software através da rede quando houver prévia concordância por parte do usuário, facultando-lhe a possibilidade de cancelar o envio das mesmas.

Muitos consumidores não lêem atentamente os contratos, principalmente em se tratando de contratos eletrônicos. Portanto, seria aconselhável criar uma interface junto ao modelo de proteção que permita ao consumidor tomar

conhecimento de todas e quaisquer informações e dados de seu computador que estejam sendo transmitidos através da rede, possibilitando ao mesmo interferir no envio de tais informações, mesmo que a recusa do consumidor implique no não funcionamento do programa.

Entretanto, verificou-se que existem dados que são essenciais para que este modelo de proteção possa atingir a sua finalidade que se referem, por exemplo, às informações acerca da data de validade do certificado para verificar se o certificado não expirou, da validade da lista de certificados revogados local e da verificação se o certificado não consta na lista de certificados revogados local.

Para resolver esta questão, propõe-se uma cláusula contratual que estabeleça que na hipótese de o usuário se recusar a fornecer as informações essenciais para a validação do certificado digital, o processo de validação do programa de computador será interrompido, de forma que o usuário não terá acesso ao programa.

Isto poderá implicar na rescisão do contrato de licença de uso do programa e, neste caso, não se caracteriza defeito ou vício do serviço haja vista que o consumidor, tendo conhecimento das peculiaridades de modelo de proteção, deu causa ao seu não funcionamento por se recusar a fornecer os dados necessários ao sistema de proteção.

De modo geral, o maior problema envolvendo a privacidade dos usuários é o fato de que as empresas de software comercializam licenças de uso de programas de computador que apresentam código-fonte fechado e protegidos pelo sigilo, de forma que podem conter neles códigos maliciosos ou operações que violem o direito à privacidade do usuário.

As empresas de software têm o dever de informar o consumidor sobre as propriedades e características de seus programas, inclusive no que concerne aos riscos que podem apresentar.

A certificação digital pode contribuir para a proteção dos direitos de autor de programa de computador através do modelo de proteção por certificação digital proposto por Rocha, desde que sejam assegurados os direitos do consumidor e a privacidade de seus dados pessoais.

Em último caso, tendo em vista a peculiaridade da proteção de programa de computador por certificação digital e suas possíveis implicações legais bem como o fato de que as normas que tratam da matéria foram instituídas através de uma medida provisória de forma muito precária, seria interessante a elaboração de uma lei específica para regulamentar o assunto de forma mais aprofundada.

REFERÊNCIAS

[1] R. O. Blum. A internet e os tribunais. In: R. Demócrito Filho (Org.). "Direito da Informática: temas polêmicos". Bauru: Edipro, 2002. pp. 145-150.

[2] D. Brown, "Fortaleza Digital". Trad. de Carlos Irineu da Costa. Rio de

[3] Janeiro: Sextante, 2005. 331 p.

[4] G. T. Corrêa. "Aspectos jurídicos da internet". São Paulo: Saraiva, 2000. 135 p.

[5] F. E. Z. Glitz. O contrato internacional celebrado pela troca de mensagens eletrônicas: a perspectiva do direito brasileiro. In: L. O. Pimentel (Org.). "Direito Internacional e da Integração". Florianópolis: Fundação Boiteux, 2003. 1071 p.

[6] ITI. Instituto Nacional de Tecnologia da Informação. Disponível em: <http://www.iti.org.br>. Acesso em: 17 de dez. 2005.

[7] O. Kaminski (Org.). "Internet legal: O Direito na Tecnologia da Informação". Curitiba: Juruá, 2003. 291 p.

[8] M. E. Leite. Comércio eletrônico nova modalidade de comércio internacional. In: L. O. Pimentel (Org.). "Direito Internacional e da Integração". Florianópolis: Fundação Boiteux, 2003. 1071 p.

[9] F. Noronha. "Direito das Obrigações" v.1. São Paulo: Saraiva, 2003. 698 p.

[10] P. Peck. "Direito Digital" São Paulo: Saraiva, 2002. 290 p.

[11] M. C. Pereira. "Direito à Intimidade na Internet". Curitiba: Juruá, 2003. 279p.

[12] D. Reinaldo Filho (Org.). "Direito da Informática: temas polêmicos". Bauru: Edipro, 2002. 432 p.

[13] J. L. F. Rocha. "Proteção de Software por Certificação Digital". Dissertação de Mestrado. Universidade Federal de Santa Catarina. Florianópolis, 2001. 76p.

[14] J. A. da Silva. "Curso de Direito Constitucional positivo". 22.ed. rev. e atual. São Paulo: Malheiros, 2003. 878 p.

[15] N. Silveira. "A propriedade intelectual e as novas leis autorais". São Paulo: Saraiva, 1998. 345 p.

[16] L. H. Ventura. "Comércio e contratos eletrônicos". Bauru (SP): Edipro, 2001. 134 p.

[17] C. S. M. Vianna. Software e privacidade: uma defesa do código-fonte aberto na preservação do direito constitucional à vida privada. In: "Jus Navigandi", Teresina, ano 6, n. 57, jul. 2002. Disponível em:<http://jus2.uol.com.br/doutrina/texto.asp?id=2931>. Acesso em: 08 jan. 2006.

[18] M. M. Volpi. Assinatura digital e sua regulamentação no Brasil. In: D. Reinaldo Filho (Org.). "Direito da Informática: temas polêmicos". Bauru: Edipro, 2002. pp. 367-382.

[19] M. Wachowicz. "Propriedade intelectual do software & revolução da tecnologia da informação". Curitiba: Juruá, 2004b. 287 p.

Hélio S. Ramos Júnior é estudante de Direito da Universidade Federal de Santa Catarina (UFSC), foi monitor da Disciplina Informática Jurídica, foi Bolsista de Iniciação Científica pelo CNPq, Conciliador do Juizado Especial Criminal do Fórum Distrital do Norte da Ilha da Comarca da Capital (SC), Pesquisador do Laboratório de Informática Jurídica do Centro de Ciências Jurídicas, atualmente trabalha como estagiário no Centro de Apoio Operacional do Consumidor - Ministério Público de Santa Catarina. É autor e co-autor das seguintes obras: "Considerações legais sobre a privacidade no espaço cibernético" (2003), "Segurança na análise de crédito: um direito do cidadão" (2004), "Os atores sociais e a cidadania na sociedade da informação e do conhecimento" (2004), "A tutela jurídica do consumidor e a publicidade abusiva em rede" (2005), "BuscaLegis: Uma Biblioteca Jurídica Virtual" (2005), "O ato administrativo eletrônico sob a ótica do princípio da eficiência" (2005), "Perspectivas para a teleadministração no Brasil: sistemas inteligentes e software livre na Administração Pública" (2006). E-mail: helio@grad.ufsc.br.