A falácia da neutralidade na assinatura digital

O Projeto de Lei nº 1.589/99, da Câmara dos Deputados, estabelece, em seu artigo 14, que "considera-se original o documento eletrônico assinado pelo seu autor mediante sistema criptográfico de chave pública". Com isso, equipara o documento eletrônico ao documento tradicionalmente conhecido, desde que tenha sido assinado por criptografia de chave pública, outro nome pelo qual também é conhecida a criptografia assimétrica.

Curiosamente, desde que o Anteprojeto foi entregue à Câmara pela OAB-SP, que o redigiu, apareceram críticas aqui e ali no sentido de que tal dispositivo iria "engessar a tecnologia", ou que o projeto não seria "tecnologicamente neutro", ao "optar" pela criptografia assimétrica como único meio de produzir assinaturas digitais, em detrimento de outras "novas tecnologias", ainda inexistentes, mas que poderiam vir a ser criadas.

Essa crítica nunca vem acompanhada de qualquer argumentação, valendo-se apenas de frases de efeito, apelando para o uso de uma palavra extremamente sonora nestes nossos dias: "tecnologia". Com o uso desta palavra mágica, fica fácil cativar o interlocutor e, assim, desmerecer o PLC 1.589/99. Entretanto, uma análise mais detida verificaria que o argumento carece de qualquer fundamento, seja do ponto de vista técnico – ou tecnológico, se quiserem -, jurídico, econômico ou político.

Analisando a questão, primeiramente do ponto de vista técnico, não se pode deixar de explicar o que é criptografia, ou o que é esta sua variante chamada de "criptografia assimétrica". Não poucas vezes vimos a crítica partir da boca de quem – eventualmente de boa-fé – sequer sabia exatamente o que é criptografia assimétrica.

A criptografia é tão antiga quanto a própria escrita, não é uma "tecnologia" que surgiu com a informática, e nisto reside o primeiro equívoco de quem levanta tal crítica. Teve, a criptografia, ao longo da História, aplicação praticamente exclusiva à esfera militar, mas hoje é considerada uma ciência, ramo da Criptologia, que por sua vez é um ramo das Ciências Exatas. Na nova sociedade da informação, a criptografia tem demonstrado imprescindível utilidade para a proteção da transmissão e armazenamento de informações e para a segurança de sistemas computadorizados. O estudo dos métodos e técnicas de codificar uma mensagem é o objeto de estudo da Criptografia. O outro ramo da Criptologia se chama Criptoanálise, e tem por objeto o estudo científico dos métodos para "quebrar" a mensagem cifrada sem conhecer a senha.

Em princípio, todas as formas de cifrar e decifrar uma mensagem utilizavam uma mesma chave, para ambas as funções. Um exemplo milenar deste tipo de criptografia é o chamado “cifrado de César”: para cifrar um texto, cada letra era substituída pela terceira letra seguinte no alfabeto; para decifrar, utiliza-sea mesma chave – três -, utilizando uma função inversa – recuar letras no alfabeto. Nos nossos dias, estes cifrados são realizados mediante complexas fórmulas matemáticas, mas seguem o mesmo princípio: para cifrar, usa-se uma função matemática que tem como variáveis a mensagem original e a chave, resultando na mensagem cifrada; para decifrar, emprega-se uma função inversa, que tem como variáveis a mensagem cifrada e a mesma chave utilizada para cifrar, o que retorna à mensagem original. Esta forma de cifrar é chamada de criptografia simétrica.

Uma dificuldade que sempre existiu na utilização da criptografia simétrica é a necessidade de combinarem previamente os interlocutores qual será a chave, precisando, para isso, de um primeiro canal seguro de comunicação, imune à interceptação por terceiros. Para contornar esta dificuldade, há tempos já se perseguia uma forma de criptografar a mensagem sem ter que compartilhar a chave secreta com o interlocutor; ou seja, uma forma de codificação que utilizasse duas chaves, uma para cifrar – a chave pública -, e outra para decifrar – a chave privada.

Distribuída livremente a chave pública, qualquer um pode cifrar a mensagem dirigida ao titular da chave privada, mas só este poderá decifrá-la. Somente em 1976, porém, a partir de profundo desenvolvimento da teoria dos números, este modelo conseguiu ser implementado por Whitfield Diffie e Martin Hellman, que descobriram o algoritmo conhecido por Diffie-Hellman. Em 1977, foi descoberto outro algoritmo de criptografia assimétrica, o RSA. Passados 25 anos, poucos algoritmos mais foram encontrados, dado que são raras e difíceis as operações matemáticas que permitem esta engenhosa maneira de cifrar e decifrar. Vários deles se mostraram inseguros, ou pouco práticos, de modo que, para gerar assinaturas, são normalmente utilizados apenas os algoritmos RSA, DSA e El-Gamal.

A assinatura digital, no caso, é produzida cifrando-se a mensagem com a chave privada, de modo a poder ser conferida com a chave pública; isto é, se a chave pública decifrar a mensagem, isto significa que ela provém daquele que detém a chave privada.

Criptografia assimétrica, pois, não é mais uma tecnologia passageira. A expressão “tecnologia” estaria mais adequada se se referisse às técnicas pelas quais a criptografia assimétrica pode ser implementada: os algoritmos RSA, DSA e El-Gamal poderiam ser chamados de “tecnologias”. O Projeto 1.589/99, então, não “engessa a tecnologia”, pois não estabelece que somente possam ser utilizados os algoritmos hoje conhecidos. Descobertos outros algoritmos assimétricos – e demonstrado que são seguros -, certamente poderão ser utilizados.

Por outro lado, argumentar que uma “nova tecnologia” possa produzir assinaturas digitais sem cifrar o documento eletrônico, mais parece um argumento falacioso. Registros eletrônicos são facilmente alteráveis, daí a dificuldade inicial em aceitá-los como prova documental. A única maneira de evitar que sejam adulterados é criptografá-los. Se o documento eletrônico não for de modo algum cifrado, poderá ser fraudado. Por sua vez, se utilizada a mesma chave para cifrar e decifrar – criptografia simétrica, portanto -, não se consegue demonstrar a autoria do documento eletrônico, porque ambos os interlocutores conhecem a chave secreta, podendo, tanto um como o outro, ter gerado aquele registro

cifrado. O que sobra? A criptografia assimétrica!

Criptografia assimétrica, portanto, é um modelo, um conceito, que pode ser implementado de maneiras – ou tecnologias – diferentes, e que tem suas bases em teorias matemáticas longamente experimentadas e desenvolvidas. Daí o ceticismo quanto à possibilidade de "novas tecnologias", sem utilizar criptografia, surgirem do nada, sem estarem calcadas em teorias demonstradas. Nem se concebe, por outro lado, que o documento eletrônico possa ter sua autenticidade e integridade protegidas e demonstradas sem a utilização deste modelo, ou alguma variante dele.

Algumas "tecnologias" que se esboçam como "alternativa" à criptografia assimétrica, ou distorcem a essência do conceito de documento, ou mistificam técnicas que não são apropriadas para gerar assinaturas. Assim, enviar o documento para uma terceira pessoa, que ficaria encarregada de receber, por meio de alguma "nova tecnologia", a aprovação do outro interlocutor, como alguns já chegaram a propor, é uma idéia que, mesmo realizada de modo seguro e por um terceiro confiável, não pode ser comparada à prova documental.

Nenhum registro inalterável é produzido nesta relação, que possa ser assemelhado ao papel firmado com assinatura manual. Isto, na verdade, poderia ser equiparado a uma prova testemunhal, consistente na afirmação do terceiro de que "presenciou" o contato entre as partes. Cá entre nós, uma prova bastante frágil! A biometria, por sua vez, não permite a geração de assinaturas digitais, embora muitos pensem justamente o contrário. Bruce Schneier, um dos mais respeitados profissionais de segurança de computadores do mundo, autor de livros que venderam dezenas de milhares de cópias, esclarece, em seu boletim mensal (disponível em:) que "dados biométricos são poderosos e úteis, mas eles não são chaves.

Eles são úteis em situações onde há um caminho confiável entre o leitor e o verificador; nestes casos tudo o que você precisa é um identificador único. Eles não são úteis quando você precisa das características de uma chave: sigilo, aleatoriedade, a habilidade de atualizar e destruir".

Noutras palavras, dados biométricos são muito úteis para controlar o acesso a uma sala reservada, por meio de um sistema fechado, que esteja protegido e situado dentro desta mesma sala; mas não servem como assinaturas.

Por amor à argumentação, aceitemos a hipótese de que amanhã uma "nova tecnologia" possa ser inventada, para produzir uma assinatura digital sem de modo algum cifrar o arquivo eletrônico. Neste caso, passemos ao argumento jurídico. Não se entende que mal haveria em legislar mais uma vez, para acrescentar no sistema jurídico esta nova possibilidade tecnológica. Esta, aliás, seria a opção mais salutar.

Contratos realizados por meio eletrônico já são plenamente válidos perante o nosso sistema jurídico, já que os atos jurídicos não dependem de forma especial, senão quando a lei expressamente o exigir. O problema com tais negócios é a questão da prova da celebração destes atos jurídicos.

O que a sociedade precisa, portanto, é de uma lei que atribua segurança jurídica quanto à validade, como prova judicial, dos registros eletrônicos com que se documentam estas transações. Se a única maneira hoje existente de se atribuir autenticidade e integridade ao documento eletrônico é por meio da criptografia assimétrica, a lei só deve prestigiar esta possibilidade, sinalizando aos contratantes, mas

também aos julgadores, que somente quando assinados por criptografia assimétrica os registros eletrônicos podem servir como prova.

Deixar de dizê-lo na lei significa manter a mesma insegurança que já impera: nem as partes saberão como documentar suas manifestações de vontade, nem terão certeza se o juiz, no caso de eventual litígio, reconhecerá aqueles registros eletrônicos como prova.

Nem se pense, por outro lado, que a descoberta de uma "nova tecnologia", num futuro próximo, vá exigir imediata alteração da lei. É que esta "nova tecnologia" só poderia ser considerada segura, do ponto de vista técnico, depois de exaustivamente testada e aprovada, não apenas por quem a vende, mas pela comunidade científica independente.

Se o Projeto 1.589/99 consagrou o uso de criptografia assimétrica, o fez porque os sistemas que a implementam são públicos, e têm resistido às tentativas de criptoanálise realizadas pela comunidade científica ao longo de duas décadas. Dessa resistência a tais "ataques" é que advém a confiança do legislador na sua segurança, para poder comparar a assinatura digital à assinatura manual. Destaque-se que testar a funcionalidade de sistemas de segurança não é o mesmo que testar outros tipos de produto ou de software.

Aqui, uma comparação com os automóveis pode ser ilustrativa: o conforto, a potência, ou o prazer de dirigir um automóvel podem bem ser testados pelo próprio consumidor; o cinto de segurança, porém, aparentemente funciona, mas só poderá ter sua eficácia comprovada pelo usuário comum no dia em que se chocar de frente com outro veículo. Ou o alarme anti-furto: o vendedor demonstra que se tocar aqui, forçar ali, ou balançar acolá, o alarme disparará estridentemente como que anunciando uma invasão de seres extraterrenos; aos nossos olhos parece seguro, até o dia em que não encontramos o veículo no local em que estava estacionado…

Se queremos uma lei para atender à necessidade de segurança da sociedade, dos consumidores e empresários, esta lei só deve admitir como prova judicial aquilo que seja reconhecidamente seguro. Estamos lidando com uma questão bastante delicada, ao atribuir força probatória a registros eletrônicos.

Imaginem que uma lei "tecnologicamente neutra" seja aprovada, alguém apresente com publicidade eficiente um novo sistema de assinaturas digitais, milhares de contratos sejam assim efetuados, e meses depois algum adolescente peralta demonstre como fraudar o sistema… Exemplos assim existem, em concreto, de rotundos fiascos tecnológicos! E pode ser ainda pior: alguém pode descobrir como fraudar o sistema e não contar aos quatro ventos, preferindo explorar a falha em seu próprio proveito, para fins evidentemente escusos. Portanto, se e quando uma nova tecnologia de assinaturas digitais for descoberta, deve ser perante o Legislativo, legítimo representante da sociedade, que a discussão sobre sua oportunidade e segurança deve ser debatida. Afinal, não se trata da venda de videogames; está em jogo a segurança jurídica dos contratos!

Do ângulo econômico, devemos ressaltar que a utilização da criptografia assimétrica é hoje algo muito barato, gratuito até, se considerarmos que os algoritmos RSA, DSA e El-Gamal têm uso liberado, sem reserva de direitos ou patentes, e existem diversos softwares livres, de código aberto, que implementam eficientemente as funções de cifrado, assinatura e gerenciamento de chaves. E, aliás, por terem seu

código-fonte aberto, estão sujeitos a exame por especialistas em segurança de todo o mundo, sendo certamente mais seguros do que os programas de criptografia comerciais, que têm o código-fonte fechado.

A “neutralidade tecnológica” da lei pode bem favorecer aqueles que, em detrimento da reconhecida segurança destas técnicas de domínio público, pretendam alavancar seus lucros com a venda de sistemas proprietários obscuros, ou “soluções tecnológicas” de eficácia não demonstrada.

Por último, resta analisar a questão do ponto de vista político. A quem interessa uma lei “tecnologicamente neutra”? Dada a brilhante escolha destas duas palavras pelos que lançaram o argumento, isto aparentemente seria de interesse geral. Afinal, quem pode ser contra a “tecnologia”? E quem não é “neutro”, só pode ser tendencioso, malicioso, oportunista, ou sabe-se lá o que… Todavia, a expressão “neutralidade tecnológica” esconde, na verdade, a proteção a interesses políticos nada neutros.

É interessante, portanto, analisar o contexto existente em 1996, quando foi elaborada a lei modelo da UNCITRAL, de cuja tradução literal redundou o Projeto de Lei nº 672/99, do Senado Federal, e que pode ser considerada um paradigma da “neutralidade tecnológica”. Em 1996, o acesso público e irrestrito à Internet ainda engatinhava, e a criptografia era conhecida por uns poucos “micreiros” que freqüentavam o underground da rede; além, é claro, dos organismos militares e de inteligência, usuários originais deste tipo de conhecimento.

Nos EUA, a exportação de produtos de criptografia era restrita, estando equiparados aos armamentos militares, norma que vigorou plenamente até o início de 2000. Não interessava – como ainda não interessa – aos serviços de inteligência norte-americanos que a criptografia se tornasse popular. O norte-americano Philip Zimmermann chegou a ser processado durante quatro anos por ter, em 1991, disponibilizado na Internet um potente software de criptografia assimétrica – o PGP, sigla de Pretty Good Privacy – com seu correspondente código-fonte.

Ora, a mesma criptografia assimétrica que gera assinaturas digitais também pode gerar mensagens cifradas indevassáveis, servindo para proteger o sigilo das comunicações eletrônicas. Isto é bom para o cidadão e sua privacidade, é bom para as empresas e seus segredos comerciais e industriais, mas é ruim para os serviços de espionagem e inteligência que querem vasculhar a rede com sistemas como o ECHELON. Uma lei modelo, em 1996, para contar com a aprovação dos EUA, jamais poderia falar em criptografia, cuja exportação era proibida, e ainda se tentava impor restrições para seu uso interno.

Hoje, embora as restrições à exportação de criptografia tenham sido relaxadas, se o terceiro mundo engolir uma outra “tecnologia”, melhor para eles.

Antecedentes já existiram: ao final da Segunda Guerra, as poderosas máquinas de cifrado dos nazistas – conhecidas por “Enigma” – foram apreendidas e vendidas a países do terceiro mundo, sem, contudo, mencionar-se que durante a guerra seu sistema havia sido decifrado pela inteligência britânica. Ou os nossos legisladores tomam cuidado, ou vai acontecer de novo…

Augusto Tavares Rosa Marcacini *é vice-presidente da Comissão Especial de Informática Jurídica da OAB-SP e Coordenador da Subcomissão de Certificação Eletrônica. Mestre e Doutor em Direito pela Faculdade de Direito da USP. Professor de Direito Processual Civil da Universidade São Judas Tadeu.* ***Marcos da Costa*** *é Presidente da Comissão de Informática do Conselho Federal da OAB-SP. Presidente da Comissão de Informática Jurídica da OAB-SP. Professor do Curso de Negócios na Era*

Digital da FGV-PEC.

Date Created
11/06/2001