3ª COMISSÃO PERMANENTE

PARECER N.º 2/II/2005

Assunto: Proposta de lei intitulada «*Documentos e assinaturas electrónicas*».

I - Introdução

O Governo da Região Administrativa Especial de Macau (RAEM) apresentou, no dia 12 de Maio de 2005, a proposta de lei intitulada «*Documentos e assinaturas electrónicas*», a qual foi no mesmo dia admitida pela Presidente da Assembleia Legislativa, nos termos regimentais.

Essa proposta de lei foi apresentada ao Plenário no dia 17 de Maio de 2005 e aprovada, na generalidade, em reunião plenária realizada no dia 25 de Maio de 2005, tendo na mesma data sido distribuída a esta Comissão para efeitos de exame e emissão de parecer.

A Comissão reuniu nos dias 2, 10, 14 e 29 de Junho e 11 de Julho de 2005, tendo contado com a presença e a colaboração de representantes do Governo numa dessas reuniões.

Dessa colaboração resultou a apresentação de uma nova versão da proposta de lei que, em parte, reflecte as opiniões expressas no seio da Comissão.

Ao longo do presente Parecer, as referências aos artigos serão feitas com base na nova versão da proposta de lei, apresentada em 30 de Junho de 2005 (versão portuguesa) e em 6 de Julho de 2005 (3.ª versão chinesa, rectificada), excepto quando seja conveniente fazer referência à versão inicial, como tal devidamente identificada.

No decurso dos trabalhos da Comissão, teve esta a oportunidade de efectuar uma visita aos Serviços de Certificação e *SignTrust* dos Correios de Macau, o que em muito contribuiu para o esclarecimento dos aspectos e implicações de natureza técnica desta iniciativa legislativa.

II – Apresentação

Nos termos da Nota justificativa que acompanha a proposta de lei, «*o Decreto-Lei n.º 64/99/M, de 25 de Outubro, aprovou um conjunto de normas legais destinadas a eliminar as (...) barreiras ao desenvolvimento do denominado «comércio electrónico». Porém, o quadro legal nele estabelecido, (...) revela-se hoje insuficiente, em especial pela incapacidade demonstrada para obviar às naturais desconfianças que as transacções por via electrónica ainda suscitam*».

Ainda segundo a Nota Justificativa, «*as vantagens associadas à utilização das novas tecnologias da informação fazem com que a utilização de meios electrónicos na gestão administrativa, comercial e financeira, bem como, em geral, em todos os sectores, seja hoje um instrumento imprescindível para o desenvolvimento das sociedades.*

Contudo, o cabal aproveitamento dessas vantagens suscita problemas de índole jurídica que os dispositivos legais tradicionais se mostram incapazes de resolver adequadamente, sendo frequentemente fonte de dúvidas e

constrangimentos em aspectos tão decisivos como a validade e reconhecimento legal dos contratos efectuados através de meios electrónicos e a força probatória dos documentos processados no âmbito de um intercâmbio electrónico de dados. Por esse facto, torna-se premente a necessidade da criação de um normativo que, sendo internacionalmente aceite, seja igualmente capaz de garantir um ambiente mais seguro de autenticação electrónica e, consequentemente, susceptível de gerar a confiança do sistema nos documentos e transacções efectuadas por via electrónica, de forma a permitir o efectivo aproveitamento das potencialidades oferecidas pelas novas tecnologias da informação. É o que se pretende com o projecto de diploma que ora se apresenta (...).

A presente proposta de lei, permite, no quadro do sistema legal instituído, dotar Macau de um instrumento decisivo para o aprofundamento da utilização das novas tecnologias da informação».

III – Apreciação genérica

1. A Sociedade da Informação é hoje uma realidade presente em múltiplos aspectos da vida quotidiana. Os computadores, e a *internet* em particular, assumiram uma relevância tal na vida moderna que é praticamente impossível ignorar o seu uso e deixar de reconhecer a sua importância: através da *internet* celebram-se negócios, transmitem-se informações, fazem-se compras de bens, acedem-se a serviços. Com as novas tecnologias da informação, a distância deixou de ser um obstáculo e a globalização passou a ser um dado adquirido.

À medida que a utilização das novas tecnologias se vai generalizando, aumenta igualmente o risco inerente ao seu uso. São conhecidos múltiplos casos de falhas nos sistemas de segurança que expõem os utilizadores da

internet a novas formas de criminalidade: da violação da privacidade à utilização abusiva de dados pessoais, passando por fraudes de natureza patrimonial ou outros tipos de crimes. Ao "admirável mundo novo" das novas tecnologias junta-se um lado mais sinistro que impede ou dificulta uma plena utilização de todas as potencialidades que os novos meios de comunicação proporcionam. Torna-se, assim, indispensável reforçar a segurança inerente à utilização da *internet*.

Por outro lado, a generalização das novas tecnologias criou realidades diferentes que necessitam de enquadramento a nível jurídico. As respostas tradicionais que o direito tem para a realidade social necessitam amiúde de adaptação, quando não mesmo de soluções inteiramente inovadoras. «*O comércio electrónico baseia-se na rapidez, conveniência e eficiência. Estes elementos conduzem os sectores comercial e tecnológico a uma constante actualização e desenvolvimento da sua actividade com as mais avançadas inovações. O problema com os métodos comerciais que evoluem a um ritmo rápido é que, muitas vezes, ultrapassam as fronteiras regulamentares que os limitam. (...) Isto resulta particularmente claro do debate actual relativo à substituição do papel e da caneta na celebração de contratos. Os requisitos de forma escrita e de assinatura dos contratos podem ser encontrados na maioria dos ordenamentos jurídicos. Estas regras, porém, foram criadas antes da existência do comércio electrónico e, em muitos casos, não o facilitam. Consequentemente, os governos em todo o mundo estão agora a tentar encontrar uma solução para este problema*»[1].

É no seguimento destas duas linhas de força que se enquadra a iniciativa legislativa ora em apreço. A criação de um regime jurídico para a utilização de

[1] W. Harry Thurlow, *Electronic contracts in the United States and the European Union: Varying approaches to the elimination of paper and pen*, 2001, in http://www.ejcl.org/53/art53-1.html (25/05/2005).

documentos e assinaturas electrónicas surge da necessidade de adaptar o ordenamento jurídico local às exigências decorrentes das novas práticas do comércio e ao imperativo de reforço da segurança na sua utilização.

Convém realçar, desde já, que a proposta de lei em apreço não pretende regular o tópico mais vasto do "comércio electrónico". Este abrange múltiplos aspectos que vão muito para além da questão da utilização de documentos e assinaturas electrónicas. A adaptação do ordenamento jurídico que é visada com a presente iniciativa legislativa não se esgota com a aprovação da futura lei; apenas agora se inicia, devendo ser seguida por outros instrumentos legislativos e regulamentares.

2. Documentos electrónicos

No ordenamento jurídico de Macau, o conceito de documento é definido como «*qualquer objecto elaborado pelo homem com o fim de reproduzir ou representar uma pessoa, coisa ou facto* (artigo 355.º do Código Civil)», adoptando um âmbito amplo que tanto abrange o sentido de *escrito* que exprime uma declaração de ciência ou uma declaração de vontade, mais vulgar na linguagem corrente, como abrange outras formas de representação da realidade, tais como objectos materiais de outra natureza, nomeadamente discos, fotografias, filmes, desenhos, etc[2].

A noção de «documento electrónico» não é diferente daquela que resulta do Código Civil, apenas tendo a especificidade de ser um tipo de documento que resulta de um processamento electrónico de dados [*vd*. alínea 1) do artigo 2.º da proposta de lei]. Razão pela qual é possível afirmar, ao nível dos princípios

[2] Antunes Varela, Miguel Bezerra e Sampaio e Nora, *Manual de Processo Civil*, 2.ª ed., Coimbra, 1985, pp. 505 ss.

gerais, o valor jurídico deste tipo de documento. Não é pelo facto de um documento se apresentar em suporte electrónico que deixa de poder produzir efeitos jurídicos (n.º 1 do artigo 3.º da proposta de lei). Como princípio geral, esta norma apresenta-se como o passo necessário para vencer barreiras de suspeição em relação a este tipo de documentos, uma vez que, caso dúvidas existissem, passa a haver uma equiparação legal entre os documentos em suporte electrónico e aqueles que têm suporte físico.

Adicionalmente, a proposta de lei reitera «*a regra de que o documento electrónico susceptível de representação como declaração escrita satisfaz o requisito legal de forma escrita, desde que a sua integridade possa ser demonstrada* (n.º 2 do artigo 3.º)» e consagra regras quanto à força probatória dos documentos electrónicos (artigo 4.º).

A este nível e com base nos três aspectos mencionados – equiparação na produção de efeitos, satisfação do requisito legal de forma escrita e força probatória -, é fácil descortinar uma preocupação de adaptar o ordenamento jurídico a uma nova realidade social, tal como foi enunciado *supra*. Mas igualmente uma preocupação de conferir certeza ao sistema jurídico, eliminando dúvidas quanto ao valor jurídico dos documentos electrónicos. A Comissão considera de extrema relevância o reforço da certeza com que, a partir de agora, os operadores do direito passam a contar, o que contribuirá para o reforço da segurança, neste particular *segurança jurídica*, na utilização das tecnologias da informação.

O documento em suporte físico, designadamente em papel, com uma assinatura manuscrita nele aposta tem sido a forma adoptada para proferir uma declaração, identificar o seu autor, conferir-lhe autenticidade e efectuar a sua

prova. Contudo, estas funções podem sair prejudicadas quando se passa para a utilização de documentos electrónicos, dada a impossibilidade material de estabelecer uma relação directa e imediata entre um documento electrónico e o seu autor. «*Muitos dos atributos das comunicações em suporte de papel – escrita e assinatura na forma tradicional – contribuem para satisfazer os requisitos legais das assinaturas. O nome de uma empresa e o seu logotipo constantes numa encomenda, o cabeçalho no topo de uma carta ou a assinatura manuscrita no fim de um documento são meios para afirmar a autenticidade, verificação da identidade, não repúdio e outras funções desempenhadas pela forma escrita. Estas características perdem-se ou ficam enfraquecidas quando se passa para o nível dos documentos electrónicos. Com efeito, nas comunicações electrónicas não pode haver a forma manuscrita tradicional de escrever e de assinar devido às diferenças existentes com a forma analógica de escrita e de assinatura e à natureza digital das comunicações electrónicas no ciberespaço*[3]».

De forma a obviar a este problema, especialmente quando se faz a equiparação entre documentos em suporte físico e em suporte electrónico, cumpre encontrar formas que permitam estabelecer com rigor a identidade do autor de um documento electrónico, da sua autenticidade e integridade. Tal como se refere na Nota justificativa, «*aspecto central do reconhecimento de força jurídica aos documentos electrónicos, interna e internacionalmente, é o que se prende com a necessidade de assegurar a sua autenticidade e integridade, o que se consegue mediante a associação ao documento de uma assinatura electrónica*».

[3] Thomas Menzel e Erich Schweighofer, *Digital signatures and the legal criterias for the written form and proof*, in http://www.univie.ac.at/RI/AJLI/3/menzel/menzel1.htm (25/05/2005)

3. Assinaturas electrónicas

Uma assinatura electrónica é, tal como definido na proposta de lei, um «*conjunto de dados sob forma electrónica que, ligados ou logicamente associados a um documento electrónico, podem ser utilizados como método de dar a conhecer a autoria do mesmo* [alínea 2) do artigo 2.º][4]».

Nestes termos, vários métodos de fazer a associação entre um documento electrónico e o seu autor - seja através da digitação de um nome, da identificação de uma impressão digital, da retina ou da íris, ou da utilização de técnicas criptográficas - podem ser abrangidos pela definição de assinatura electrónica [5], aos quais correspondem, no entanto, diferentes níveis de segurança e de certeza. O que significa que, para a futura legislação local, são admissíveis diferentes formas de assinatura electrónica, desde que possam dar a conhecer a autoria do documento em questão, abstendo-se a lei de consagrar qual o método de assinatura electrónica que "prefere". Tal como explicado na Nota justificativa, «*neste âmbito, o diploma assenta, como é tendência*

[4] A nível do direito comparado, refiram-se as definições constantes da legislação da República Popular da China, de Hong Kong, dos Estados Unidos da América e da União Europeia: para a Lei das assinaturas electrónicas da R.P. da China, de 28 de Agosto de 2004, "assinatura electrónica" são os «*dados incluídos ou associados de forma electrónica num texto ou dados em suporte electrónico, com o propósito de identificar o emitente e indicar que este confirma o conteúdo do documento*»; na *Electronic Transactions Ordinance* de Hong Kong (Cap. 553), "assinatura electrónica" é definida como «*quaisquer letras, caracteres, números ou outros símbolos em forma digital ligados ou logicamente associados a um documento electrónico, e que seja executado ou adoptado com a intenção de autenticar ou aprovar um documento electrónico*»; nos Estados Unidos da América, o *Millennium Digital Commerce Act*, de 1999, define "assinatura electrónica" como «*um som, símbolo ou processo ligado ou logicamente associado a um documento e que seja executado ou adoptado por uma pessoa com a intenção de assinar o documento*»; na União Europeia, a Directiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de Dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas electrónicas, define "assinaturas electrónicas" como «*os dados sob forma electrónica, ligados ou logicamente associados a outros dados electrónicos, e que sejam utilizados como método de autenticação*».

[5] Stephen E. Blythe, *Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce with Enhanced Security*, Richmond Journal of Law & Technology, Volume XI, Issue 2 (2005), *in* http://law.richmond.edu/jolt/v11i2/article6.pdf

dominante, num modelo tecnologicamente neutro, permitindo a sua acomodação ao surgimento de novas tecnologias de certificação electrónica. A opção contrária, por um quadro jurídico específico do sistema de assinaturas digitais – o único que, por ora, tem merecido aceitação relevante dos prestadores de serviços de certificação –, obrigaria o legislador a rever significativamente os quadros normativos vigentes sempre que novas tecnologias fiáveis de certificação electrónica surgissem no mercado, o que, face até à natural morosidade do próprio processo legislativo, acabaria por constituir um obstáculo ao desenvolvimento e inovação nesta área».

Importa deixar claro, desde já, que existem diferentes opções a este nível. Alguns sistemas jurídicos determinam o uso de um tipo em particular de assinaturas electrónicas – as assinaturas digitais -, utilizando uma tecnologia específica, nomeadamente códigos ou chaves criptográficas, tal como é o caso de Hong Kong. Outros sistemas há, porém, que deixam a escolha da tecnologia para a criação de assinaturas electrónicas inteiramente à vontade das partes, conferindo, no entanto, valor reforçado a assinaturas que cumpram determinados critérios de segurança, o que neste momento e com a tecnologia presentemente disponível, é em regra conseguido com as assinaturas digitais. Ou seja, presentemente a tecnologia que melhor cumpre os critérios legais para as assinaturas electrónicas qualificadas é a das assinaturas digitais, mas nada impede que surjam, no futuro, outros métodos mais seguros que cumpram igualmente tais critérios, passando a lei a abrangê-los automaticamente, sem necessitar de ser alterada. O que quer dizer que «*a questão de saber o que pode ser utilizado como assinatura electrónica não é tanto uma questão técnica, mas antes uma questão jurídica uma vez que uma determinada tecnologia só*

pode funcionar como assinatura electrónica desde que a lei lhe reconheça efeitos jurídicos[6]».

O modelo seguido pela proposta de lei corresponde à segunda opção enunciada, o que, no parecer da Comissão, se apresenta como a melhor solução.

Se a lei é neutra quanto ao modelo tecnológico para a criação de assinaturas electrónicas, já o não é quanto à produção de feitos jurídicos pelos diferentes tipos de assinaturas. A proposta de lei é clara quando determina que a plenitude de efeitos jurídicos associados aos documentos e assinaturas electrónicas só é alcançado quando as partes, por livre vontade, apõem uma assinatura electrónica qualificada (artigo 5.º), isto é, uma «*modalidade de assinatura electrónica avançada baseada num certificado qualificado e criada mediante um dispositivo seguro de criação de assinaturas, susceptível de garantir eficazmente, de acordo com padrões internacionalmente reconhecidos, a protecção da assinatura contra utilizações fraudulentas* [artigo 2.º, alínea 4)]».

Tal como se refere na Nota Justificativa, «*(...) Prevê-se a possibilidade da existência de diferentes modalidades de assinaturas electrónicas, embora se exija um mais elevado grau de segurança relativamente às assinaturas electrónicas que permitem dotar os documentos a que são apostas de força probatória plena, designadamente que sejam criadas com recurso às mais seguras e eficazes tecnologias e providenciadas por uma entidade certificadora credenciada para o efeito*».

[6] Lorna Brazell, *Electronic Signatures – Law and Regulation,* Sweet & Maxwell, Londres, 2004, p 35 ss.

Quanto a este aspecto, e em síntese, pode afirmar-se que, «*enquanto quase todas as leis conferem efeitos jurídicos básicos às assinaturas electrónicas, independentemente da tecnologia utilizada, é comum que os efeitos jurídicos mais relevantes sejam apenas reconhecidos quando os certificados sejam emitidos por uma entidade que esteja de alguma forma acreditada ou certificada ou que cumpre determinados critérios*[7]».

3.1. Funcionamento das assinaturas electrónicas

As assinaturas electrónicas qualificadas são aquelas que conseguem dar maiores garantias de segurança, bastantes para que a lei confira força jurídica, nomeadamente probatória, aos documentos electrónicos que tenham uma dessas assinaturas apostas e que sejam susceptíveis de representação como declaração escrita (n.º 1 do artigo 4.º).

«*A diferença fundamental entre uma assinatura electrónica e uma assinatura digital é que a assinatura digital é a forma mais sofisticada de assinatura electrónica, que envolve o uso de tecnologia de encriptação para autenticar a integridade da assinatura e do próprio documento. A tecnologia de encriptação usa a criptografia para transformar ou "encriptar" o documento ou dados em algo ininteligível e transformá-lo ou "desencriptá-lo" de volta à sua forma original*[8]». Ou seja, a criptografia é a ciência de disfarçar informação através de processos de codificação e de repor essa mesma informação no seu estado original através de processos de descodificação. A utilização de métodos criptográficos faz com que as assinaturas digitais, utilizando o método de

[7] Kuner, Barcelo, Baker e Greenwald, *An Analysis of International Electronic and Digital Signature Implementation Initiatives*, 2000, in http://www.ilpf.org/groups/analysis_IEDSII.htm (25/5/2005/).
[8] Claire Wright, Will McAuliffe, Anna Gamvros, *Internet Law in Hong Kong*, Sweet & Maxwell, Hong Kong, 2003, pp 194 ss.

"criptografia de chaves públicas", sejam o método presentemente mais utilizado para a criação de assinaturas electrónicas qualificadas[9].

Num sistema de criptografia de chaves públicas (ou criptografia assimétrica) são usadas duas chaves, que são códigos matemáticos aleatoriamente criados, matematicamente relacionados mas que não podem ser obtidos um a partir do outro, para cifrar e decifrar uma mensagem. A chave privada nunca sai da posse do seu titular, enquanto que a chave pública é disponibilizada publicamente. Qualquer informação que seja cifrada com uma das chaves só poderá ser decifrada com a outra. A criptografia assimétrica «*utiliza um algoritmo com duas chaves matematicamente relacionadas. A primeira dessas chaves, denominada de chave privada ou particular, é fornecida à pessoa que pretende utilizar a assinatura digital e tem como função principal transformar um texto legível numa mensagem sem sentido. Por sua vez, a segunda chave, denominada de chave pública, serve para verificar a identidade da assinatura e para dar sentido ao texto criado pela primeira, repondo-o no seu sentido original. A chave pública assemelha-se a um número de telefone dado que estará disponível a todo o indivíduo que pretenda contactar com o titular desta chave. Através desta quem receber um documento electrónico assinado pela chave privada poderá descodificar a mensagem contida e verificar a autenticidade da assinatura*[10]».

Utilizando esta tecnologia num processo de assinatura de um documento electrónico, é preciso:

---

[9] Denis Kelleher, Karen Murray, *IT Law in the European Union*, Sweet & Maxwell, Londres, 1999, pp 99 ss.

[10] Francisco Pereira Coutinho, *Os Notários: Espécie em vias de extinção ou apenas em transição?*, Faculdade de Direito da Universidade Nova de Lisboa, n.º 4, Lisboa, 2003, pp. 20-21, *in* http://www.fd.unl.pt/web/investigacao/wpapers/pdf/2003/wp004-03.pdf

1. criar um par de chaves pública – privada, ficando a chave privada em posse do remetente do documento, que a deve manter secreta, enquanto que a chave pública fica disponibilizada *online*;
2. aplicar a chave privada ao documento para assiná-lo, produzindo um código alfanumérico (algoritmo) único especificamente relacionado com o documento assinado. A chave privada encripta o referido código de forma a prevenir que a assinatura seja copiada;
3. apor a assinatura no documento e enviá-lo ao destinatário;
4. desencriptar o documento através da utilização da chave pública do remetente, o que é feito pelo destinatário. Se a desencriptação foi possível, o destinatário fica a saber que o documento é autêntico, isto é, que vem do pretenso autor. Fica igualmente a saber que o documento não foi alterado se, ao produzir um novo código alfanumérico do documento recebido e ao compará-lo com o documento que foi encriptado, forem ambos compatíveis[11].

3.2. Funções das assinaturas electrónicas

As funções das assinaturas electrónicas não diferem daquelas das assinaturas manuscritas, nomeadamente das assinaturas autógrafas, isto é, feita pelo próprio punho do signatário.

Através da aposição de uma assinatura electrónica num documento podem ser identificadas as quatro funções principais a elas inerentes:

[11] Stephen E. Blythe, *Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce with Enhanced Security*, cit., p. 4 ss; Claire Wright, Will McAuliffe, Anna Gamvros, *Internet Law in Hong Kong*, cit., pp. 195 ss.

1. *Autenticação*: autentica-se a identidade de quem assinou os dados, confirmando-se quem participou numa determinada transação e se essa transacção foi ou não forjada por alguém;

2. *Integridade*: protege-se a integridade dos dados, ficando-se a saber que a mensagem recebida não sofreu alterações, quer acidental, quer maliciosamente;

3. *Não repúdio*: prova-se que determinada pessoa participou numa transacção, não podendo esta negar que enviou ou recebeu determinada informação;

4. *Confidencialidade*: garante-se que a informação que circula não pode ser conhecida por terceiros.

3.3. Entidades certificadoras

O par de chaves pública-privada não tem qualquer associação directa a uma identidade pessoal – é apenas um conjunto de números. Para relacionar inequivocamente uma identidade com um par de chaves, é necessária uma terceira entidade de confiança: a entidade certificadora.

A entidade certificadora é quem cria e assina um certificado qualificado, que é um *documento electrónico que liga uma determinada assinatura electrónica ao seu titular e estabelece os termos de validade da mesma* [alínea 8) do artigo 2.º]. O certificado qualificado pode ser utilizado como forma de identificação digital, como se de um bilhete de identidade electrónico se tratasse, podendo ser utilizado para efectuar transacções electrónicas em redes abertas

com segurança, assinar electronicamente documentos e disponibilizar outros mecanismos para fins de confidencialidade.

«*Devido ao facto de a* internet *ser um mundo virtual, onde interagem um conjunto de pessoas que nunca se contactaram visualmente, é necessária a existência de uma entidade que funcione como ponte entre essas pessoas por forma a garantir que a chave é de quem diz possuí-la. Ora, a solução encontrada para este problema foi atribuir a um terceiro essa função. Os americanos têm chamado a este terceiro de* trusted third party*, sendo que nos países de tradição romano-germânica este pode ser conhecido como notário ou, neste caso, cybernotário. Nestes termos, o cybernotário funciona como* certification authority*, ou entidade certificadora, pois expede certidões de forma electrónica, assegurando que o detentor de um par de chaves é aquele que assinou um documento determinado. Ou seja, a função primacial do certificado é associar um par de chaves com a pessoa que é titular das mesmas. Assim, o destinatário de uma determinada mensagem, quando quiser ter a certeza da identidade e validade de uma determinada assinatura, vai verificar, junto da lista de chaves públicas certificadas pelo cibernotário, se as duas chaves combinam. Por último, importa salientar que o certificado emitido pelo cybernotário também é digitalmente assinado por este. Desta forma, se o destinatário de uma determinada mensagem não se sentir suficientemente seguro com um determinado certificado, poderá sempre verificar a idoneidade da entidade credenciadora junto de uma autoridade superior, que não é mais do que a entidade que reconhece a assinatura digital do cybernotário*[12]».

[12] Francisco Pereira Coutinho, *Os Notários: Espécie em vias de extinção ou apenas em transição?*, cit., pp. 21 ss.

Nos termos da proposta de lei, a função de entidade certificadora pode ser desempenhada tanto por entidades privadas – sociedades comerciais regularmente constituídas na RAEM, cujo objecto social inclua o exercício da actividade de certificação, isto é, de emissão de certificados qualificados, como por entidades públicas.

A Comissão ponderou esta opção, na tentativa de avaliar se as funções desempenhadas pelas entidades certificadoras podem ou devem ser desempenhadas por entidades privadas. A emissão de um certificado qualificado, gerador de uma assinatura electrónica qualificada, permite que os documentos electrónicos possam ter força probatória plena das declarações atribuídas ao seu autor (n.º 1 do artigo 4.º). Este regime, semelhante ao constante do Código Civil para os documentos particulares com reconhecimento notarial da assinatura (*vd.* artigo 370.º), faz uma ligação directa com as funções desempenhadas pelo notariado.

Contudo, enquanto que a função notarial é feita com referência a actos e documentos concretos, a emissão de certificados qualificados faz-se com referência a uma assinatura electrónica que é válida por um período de tempo e que, durante o seu período de validade, pode ser aposta em múltiplos documentos electrónicos.

Por outro lado, o actual direito registal não sai afectado com a presente iniciativa legislativa: a alínea 1) do n.º 2 do artigo 1.º determina que as normas legais que obriguem a utilização de documentos em suporte de papel ou outras formas ou modos especiais de os apresentar, formular, transmitir ou arquivar, designadamente quanto estejam em causa actos notariais ou de registo, não são prejudicadas pelo disposto na proposta de lei. Sem prejuízo, no entanto, das adaptações do notariado decorrentes da sua informatização (*vd.* artigos 25.º, 36.º, n.º 4, 42.º, 61.º e 64.º, n.ºs 2 e 3 do Código do Notariado).

Por fim, de acordo com a informação recolhida no decurso da análise da proposta de lei, é comum ao nível do direito comparado a existência de dualidade de natureza das entidades que exercem a actividade de certificação, havendo mesmo ordenamentos jurídicos que atribuem essa função apenas a entidades privadas.

Avaliadas os diferentes aspectos relativos à natureza das entidades certificadoras, a Comissão considera a opção constante da proposta de lei como equilibrada e apta a permitir que as entidades certificadoras que irão operar na RAEM possam desempenhar a sua função com rigor, credibilidade e segurança, independentemente de terem natureza pública ou privada.

Para tal, é determinante o regime de credenciação das entidades certificadoras que a proposta de lei consagra.

Refere a Nota justificativa que «*no domínio da certificação de assinaturas electrónicas, consagra-se, como é tendência dominante, a liberdade do exercício da actividade em geral. Porém, atenta a necessidade de garantir que a emissão de certificados qualificados, geradores de assinaturas electrónicas qualificadas, obedece a rigorosos padrões de segurança, exige-se, como também é regra internacionalmente aceite, a credenciação prévia das entidades que os queiram emitir (artigo 14.º). (...) A credenciação constitui um procedimento administrativo pelo qual a autoridade competente reconhece às entidades interessadas a aptidão para emitirem certificados que o ordenamento jurídico da RAEM possa reconhecer como qualificados mediante a verificação do preenchimento de determinados requisitos de ordem técnica, humana e financeira (artigo 15.º) e implica a necessidade de acatamento, por parte das entidades credenciadas, de um exigente conjunto de deveres no decurso da actividade de certificação em geral e da emissão de certificados qualificados em especial (cfr., entre outros, os*

artigos 10.º, 21.º, 22.º e 24.º), cuja fiscalização compete a uma autoridade credenciadora, a designar por despacho do Chefe do Executivo (artigo 16.º)».

A autoridade credenciadora é a entidade fiscalizadora da actividade de certificação, tanto *a priori*, aquando da avaliação do pedido de credenciação, como *a posteriori*, no decurso da actividade das entidades certificadoras credenciadas.

Apesar do regime de credenciação, constante da Secção II do Capítulo III da proposta de lei, ser aplicável tanto às entidades públicas, como às entidades privadas que pretendam exercer a actividade, prevê-se que, em casos excepcionais, as entidades públicas possam ser dispensadas de credenciação (artigo 30.º). Tal facto não implica que as mesmas não tenham de demonstrar que dispõem de condições técnicas e humanas adequadas para o exercício da actividade de certificação (n.º 2) e que não estejam sujeitas aos mesmos deveres das entidades certificadoras credenciadas (n.º 4).

Por fim, importa realçar que o regime constante da presente iniciativa legislativa pretende regular a actividade de emissão de certificados qualificados, abstendo-se de regular a emissão de outros tipos de certificados. Perante a Comissão, o Governo reiterou ser esta a sua intenção, o que mereceu total concordância.

3.4. Política das ciências e da tecnologia

Uma breve nota para realçar o facto de a presente iniciativa legislativa se enquadrar no âmbito da política das ciências e da tecnologia da RAEM, cujas bases foram aprovadas pela Lei n.º 9/2000.

Os objectivos aí gizados de elevar o nível científico e tecnológico na RAEM, elevar a produtividade, reforçar a competitividade e promover o contínuo desenvolvimento social e económico, promover o desenvolvimento e utilização da tecnologia informática e promover a generalização do uso da tecnologia informática nos serviços públicos sairão, com certeza, reforçados com a aprovação e implementação da presente iniciativa legislativa.

IV – Apreciação na especialidade

Para além da apreciação genérica apresentada no ponto anterior, a análise efectuada na Comissão teve como propósito, nos termos do artigo 118º do Regimento da Assembleia Legislativa, apreciar a adequação das soluções concretas aos princípios subjacentes à proposta de lei e assegurar a perfeição técnico-jurídica das disposições legais.

Nestes termos, a proposta de lei foi analisada na especialidade, em estreita colaboração com o proponente.

Das questões analisadas na Comissão e das alterações introduzidas no articulado, cumpre destacar as seguintes:

1. Âmbito de aplicação (artigo 1.º, n.º 2)

A aprovação do regime jurídico dos documentos e assinaturas electrónicas trará, necessariamente, importantes consequências jurídicas, tanto para os particulares, como para o sector público. No entanto, devido ao facto das alterações serem de monta, torna-se aconselhável que a adaptação do sistema jurídico seja feita de forma cautelosa e progressiva, tanto mais que a legislação local está pensada para os tradicionais documentos em suporte físico e para as assinaturas manuscritas. Não é intenção do proponente, nem da Comissão, que no momento da entrada em vigor da futura lei todos os actos jurídicos possam ser feitos com recurso a documentos e assinaturas electrónicas. Se tal é possível no tráfego jurídico privado, já o não é em relação a certos actos que requerem graus de segurança e certeza reforçadas. Não que isso não possa ser atingido com recurso a documentos e assinaturas electrónicas; mas pressupõe uma cuidadosa verificação dos múltiplos diplomas legais e regulamentares que, de momento, não pode ser feita. Razão pela qual, o n.º 2 do artigo 1.º determina que a futura lei *não prejudica a aplicação das normas legais, regulamentares ou convencionais que obriguem à utilização de documentos em suporte de papel ou outras formas ou modos especiais de os apresentar, formular, transmitir ou arquivar, designadamente quando estejam em causa actos notariais, de registo, processuais, que titulam relações jurídicas pessoais, relativos a concursos ou situações em que seja exigida a presença física do signatário ou o reconhecimento presencial de assinatura*.

Nestes termos, sempre que a lei exija uma forma solene ou específica para determinados actos, nomeadamente através da apresentação de certos formulários ou do reconhecimento de assinaturas, nas áreas constantes das

alíneas do n.º 2 ou noutras (a enunciação é meramente exemplificativa), continuar-se-á a ter de utilizar a forma tradicional de suporte de documentos até que a lei em causa admita a utilização de suporte electrónico. Este facto, porém, não implica necessariamente alterações legislativas: a adaptação pode ser feita por via regulamentar, tendo o Governo ampla margem de manobra para adaptar as formalidades administrativas (tal como resulta, aliás, dos disposto no artigo 31.º), ou através de mecanismos previstos na própria lei, como é o caso, já mencionado, do Código do Notariado (*vd*. ponto 3.3. do presente Parecer).

Ao nível da redacção, no n.º 2 do artigo 1.º a expressão *«modelos próprios»,* constante da versão inicial da proposta de lei, foi substituída pelo termo *«documentos*» e foi clarificada a delimitação negativa do âmbito de aplicação da futura lei, através da previsão de certas situações em que é inadequada, sem expressa regulamentação das condições para o efeito, a imediata utilização de documentos electrónicos, mas que, em face da redacção anterior, poderiam suscitar dúvidas sobre se essa possibilidade estava ou não aberta.

2. Definições (artigo 2.º)

No artigo relativo às definições, de particular importância num diploma com linguagem técnica tão específica, foi alterada a redacção das definições de «documento electrónico» e de «assinatura electrónica» [alíneas 1) e 2)] e aditada a definição de «endereço electrónico» [alínea 11)].

Na alínea 1), pretendeu-se fazer a aproximação da definição de «documento electrónico» da definição de «documento» constante do Código

Civil, por forma a evitar futuras dúvidas quanto à natureza dos documentos electrónicos. Tal como foi referido no ponto 2 da apreciação genérica do presente Parecer, o documento electrónico é um documento na acepção do Código Civil, tendo apenas a especificidade de resultar de um processamento electrónico de dados.

Na alínea 2), pretendeu-se clarificar o conceito de autenticação anteriormente utilizado, que poderia suscitar dúvidas interpretativas. Deste modo, fica agora claro que o que ali está em causa é a possibilidade de identificação da autoria do documento.

Quanto à alínea 11), a inclusão desta definição destina-se a evitar a «confusão» entre «endereço electrónico» (*cfr.* artigo 6.º, n.º 2) e «endereço de correio electrónico». Deste modo, fica claro que «endereço electrónico» não é a mesma coisa que «endereço de correio electrónico» ou *e-mail*. Optou-se, neste domínio, por uma formulação próxima da utilizada na legislação de Hong Kong e Singapura, nomeadamente.

3. Valor jurídico dos documentos electrónicos (artigo 3.º)

A equiparação entre documentos em suporte físico e em suporte electrónico, que é feita no artigo 3.º, é um elemento fundamental do regime jurídico ora em apreço – não podem ser negados efeitos jurídicos a um documento electrónico apenas pelo facto de este ter um suporte electrónico e não se apresentar no tradicional suporte físico.

Por outro lado, sempre que a lei requeira a forma escrita para certos documentos, tal requisito é satisfeito se o documento tiver suporte electrónico,

desde que o seu conteúdo seja susceptível de representação como declaração escrita e a sua integridade possa ser demonstrada (n.º 2)[13].

4. Força probatória dos documentos electrónicos (artigo 4.º)

A proposta de lei atribui força probatória plena aos documentos electrónicos susceptíveis de representação como declaração escrita e aos quais tenha sido aposta uma assinatura electrónica qualificada (1.ª parte do n.º 1 do artigo 4.º).

No direito processual civil de Macau vigora o princípio da livre apreciação da prova[14], ou seja, salvo disposição legal em contrário, a prova é apreciada segundo as regras da experiência e a livre convicção da entidade competente. Há, todavia, excepções a este princípio, nomeadamente na prova por documentos. Diz-se, por exemplo, no n.º 1 do artigo 370.º do Código Civil que «*o documento particular cuja autoria seja reconhecida nos termos dos artigos antecedentes [reconhecimento notarial] faz prova plena quanto às declarações atribuídas ao seu autor (...)*».

A «prova plena» é aquela que só cede perante prova em contrário, sendo irrelevante gerar uma situação de dúvida no espírito do julgador, uma vez que a lei manda resolver tal situação de dúvida no sentido indicado pela mesma prova[15]. «*Sempre que assim seja, para destruir a demonstração da existência do facto, feita através de elemento dotado de força probatória plena, não basta a contraprova, não chega a neutralização da prova (plena)*

[13] Relativamente à questão do valor jurídico dos documentos electrónicos, *vd.* ponto 2 da Apreciação genérica do presente Parecer.
[14] Quanto ao princípio da livre apreciação das provas, *vd*. Isabel Alexandre, *Provas Ilícitas em Processo Civil*, Almedina, Coimbra, 1998, pp. 101 ss.
[15] Castro Mendes, *Direito Processual Civil*, vol. III, Lisboa, 1980, p. 197.

efectuada. É necessária a prova do contrário. Não basta, noutros termos, criar no espírito do julgador a dúvida sobre a existência do facto (a que se refere a prova plena), tornando o facto subjectivamente incerto. É essencial convencer o juiz da existência do facto oposto, tornar (psicologicamente) certo o facto contrário[16]».

Na situação prevista no n.º 1 do artigo 4.º, é possível atribuir força probatória plena devido ao facto de a aposição de uma assinatura electrónica qualificada garantir a vontade do declarante e a integridade do documento. Sem prejuízo, tal como está previsto na parte final do n.º 1, da arguição e prova da falsidade do documento.

Diferentemente, o documento electrónico que não seja susceptível de representação como declaração escrita e ao qual tenha uma sido aposta uma assinatura electrónica qualificada tem a força probatória das reproduções mecânicas (n.º 2). Isto é, nos termos do artigo 361.º do Código Civil, tais documentos fazem prova plena dos factos e das coisas que representam, se a parte contra quem os documentos são apresentados não impugnar a sua exactidão.

Por fim, o documento electrónico a que não tenha sido aposta uma assinatura electrónica qualificada (n.º 3) ou quando a assinatura electrónica qualificada aposta tenha um certificado que não seja válido (n.º 4) não faz prova plena, antes é apreciado nos termos gerais do direito.

[16] Antunes Varela, Miguel Bezerra e Sampaio e Nora, *Ob. Cit.*, pp. 472- 473.

Com esta diferenciação no regime probatório dos documentos electrónicos, o legislador admite que todos os documentos electrónicos sejam admissíveis em tribunal, mas na prática cria um "incentivo" para a utilização de documentos que utilizem assinaturas electrónicas qualificadas[17].

O n.º 4 do artigo 4.º foi aditado na nova versão da proposta de lei. Em face das dúvidas suscitadas a propósito da expressão «falta de assinatura» usada no n.º 3 do artigo 5.º, entendeu-se deixar claro que a aposição de uma assinatura qualificada cujo certificado tenha caducado, sido revogado ou esteja suspenso, ou quando não sejam as condições dele constantes, não confere ao documento força probatória acrescida, devendo o mesmo ser apreciado «nos termos gerais de direito», como qualquer documento não assinado ou assinado com assinatura não qualificada.

Consequentemente, eliminou-se o n.º 3 do artigo 5.º da versão inicial da proposta de lei por se tratar, agora, de um problema de força probatória do documento e não de um mero problema de (falta de) assinatura.

5. Emissão e recepção de documentos electrónicos (artigo 6.º)

Como é referido na Nota justificativa, «*pela importância de que a temática se reveste, devotou-se especial atenção à problemática da «transmissão de documentos electrónicos» por meios informáticos. Neste domínio, para lá da norma que determina que o documento permanece em poder do remetente até à recepção pelo destinatário (artigo 6.º, n.º 1), justificada pela necessidade de obviar aos problemas que a aplicação das normas do Código*

[17] Kuner, Barcelo, Baker e Greenwald, *An Analysis of International Electronic and Digital Signature Implementation Initiatives*, ob cit.

Civil poderia suscitar, estabelecem-se regras precisas quanto à determinação do momento da recepção (artigo 6.º, n.os 2 e 3)».

Ao regime constante da versão inicial da proposta de lei, aditou-se um novo n.º 4. Tal aditamento prende-se com a necessidade sentida de estabelecer uma regra em relação ao *lugar* de envio e recepção de documentos electrónicos. Para o efeito, a solução encontrada foi criar uma *presunção* de que os documentos são enviados do domicílio ou lugar da empresa e recebidos no domicílio ou lugar da empresa, a não ser que haja lei ou convenção em sentido diverso ou que no certificado de assinatura conste um endereço ou a indicação de um lugar diferente.

A introdução desta norma justifica-se em virtude de actualmente estar consagrada norma idêntica no Decreto-Lei n.º 64/99/M, de 25 de Outubro, que a presente proposta revoga, tendo-se entendido ser prudente não deixar de fazer referência a este aspecto.

6. Emissão de certificados qualificados (artigo 10.º)

O n.º 4 da versão inicial da proposta de lei dispunha que «em caso de suspensão, revogação ou caducidade de um certificado, nenhuma entidade certificadora pode emitir certificado relacionado com os mesmos dados de criação de assinatura».

Considerou-se adequado proceder à sua eliminação por forma a evitar a sugestão, contida na fórmula original, de que normalmente poderão ser emitidos mais do que um certificado a propósito da mesma assinatura, situação que importa evitar.

7. Obrigações do titular de uma assinatura electrónica qualificada (artigo 11.º)

Da inserção sistemática deste artigo já resultaria que as obrigações nele impostas ao titular da assinatura diziam respeito ao titular de uma *assinatura qualificada*. Entendeu-se oportuno, não obstante, clarificar que é essa efectivamente a solução pretendida. Relativamente às demais assinaturas, que não estão especialmente reguladas na lei, as exigências ali postas dependem da vontade do próprio titular.

8. Certificados emitidos no exterior (artigo 13.º)

No decurso da análise da presente iniciativa legislativa verificou-se a existência de uma lacuna na alínea 2) do n.º 1 do artigo 13.º, a qual se referia, na versão inicial, a *«instrumentos de direito internacional»*, mas não, também, a acordos inter-regionais no âmbito da República Popular da China (por exemplo, entre Macau e Hong Kong). Uma vez que tais acordos não são considerados instrumentos de direito *internacional* e porque não devem ficar excluídos do regime ora consagrado, acrescentou-se a referência a «acordos regionais».

9. Obrigatoriedade de credenciação (artigo 14.º)

A alteração ao anterior n.º 1 deste artigo (agora norma única), visa clarificar que a credenciação respeita à entidade certificadora que pretenda exercer a actividade de emissão de certificados qualificados e não, como a redacção anterior sugeria (sobretudo na versão chinesa), que *cada certificado* precisa de ser autonomamente credenciado.

A obrigatoriedade de credenciação tanto abrange as entidades públicas, como as entidades privadas, sem prejuízo do regime excepcional para as primeiras constante do artigo 30.º. Tendo sido ponderada a hipótese de estabelecer um regime de credenciação apenas para as entidades privadas, considerou-se que não se mostrava adequado uma vez que as entidades públicas intervêm na certificação em «concorrência» e em igualdade com as entidades privadas. Não se justificaria, por isso, o estabelecimento, de um «regime geral» de dispensa das entidades públicas ou de um regime «diferenciado» de credenciação.

Quanto à eliminação do n.º 2, justifica-se por razões de ordem sistemática, em virtude da aparente contradição do seu conteúdo com a epígrafe do artigo, sendo certo que não implica nenhuma alteração substancial, dado que, no silêncio da lei, a actividade de certificação fora dos casos previstos no artigo 14.º será livre.

10. Requisitos de credenciação (artigo 15.º)

Na alínea 1) do n.º 3 do artigo 15.º foi eliminada a referência à «pronúncia» como critério indiciador da falta de idoneidade. Visa-se com esta alteração uma melhor adequação da norma com o princípio da presunção de inocência.

Esta alteração justificou ainda a eliminação da referência ao caso julgado na alínea 2) deste mesmo número, por razões de harmonização do regime.

11. Recusa de credenciação (artigo 19.º)

À redacção inicial do artigo 19.º foi aditado um novo n.º 3. Com a introdução deste novo número, visa-se preencher uma lacuna, respeitante à definição do tipo de recurso em relação à decisão de não credenciação. Optou-se por consagrar o *recurso contencioso para o Tribunal Administrativo*, por ser a solução que neste contexto (em que estão em causa empresas públicas e privadas e conhecimentos técnicos muito especializados) faz mais sentido. Além disso, não está definida a autoridade credenciadora (ou a sua natureza), razão que torna «pouco recomendável» o recurso hierárquico.

12. Caducidade e revogação da credenciação (artigo 20.º)

Verificou-se, quanto a este artigo, a necessidade de «correcção» da parte final do n.º 1, de forma a adequá-lo às entidades certificadoras públicas (as quais, rigorosamente, não são «dissolvidas»).

Esta alteração suscitou, por seu turno, a necessidade de prever uma norma que «evitasse» a automática caducidade da credenciação das entidades públicas em caso de superior decisão da sua extinção. Neste sentido, optou-se por introduzir um n.º 2, permitindo, em relação a estas entidades públicas, a «transmissão» da credenciação quando a actividade (e os meios respectivos) seja cometida a outra entidade ou serviço público.

Ainda quanto ao n.º 1, aumentou-se o prazo de caducidade ali previsto, de 3 para 6 meses. Ponderou-se, quanto a este aspecto, que o prazo inicialmente previsto poderia vir a revelar-se demasiado curto para o efeito da instalação de

todos os equipamentos necessários para se dar início à actividade de certificação.

13. Auditor externo de segurança (artigo 26.º)

Introduz-se um novo n.º 2 ao artigo 26.º, contendo uma disposição destinada a especificar as funções do auditor externo de segurança, o que se justifica em virtude de se tratar de uma função de auditoria que foge aos «padrões comuns».

A introdução deste número implicou a alteração da parte final do n.º 3 deste artigo 26.º e da parte final do n.º 4 do artigo 27.º, de forma a harmonizar a redacção da proposta.

14. **Responsabilidade civil (artigo 28.º)**

O artigo 28.º consagra o regime de responsabilidade civil das entidades certificadoras credenciadas por danos causados pelo incumprimento dos deveres que lhes incumbem no exercício da actividade de certificação. Todos os danos causados, de forma dolosa ou negligente, pela entidade certificadora credenciada devem ser ressarcidos, não recaindo sobre o particular o ónus de provar que tal entidade actuou dolosa ou negligentemente. Neste aspecto, e por força desta norma, procede-se à inversão do ónus da prova, cabendo à entidade certificadora provar que não actuou de forma dolosa ou negligente.

O regime de responsabilidade por factos ilícitos (responsabilidade extracontratual) encontra-se consagrado no Código Civil.

O princípio geral é, nos termos do n.º 1 do artigo 477.º do Código Civil, que «*aquele que, com dolo ou mera culpa, violar ilicitamente o direito de outrem ou qualquer disposição legal destinada a proteger interesses alheios fica obrigado a indemnizar o lesado pelos danos resultantes da violação*». A regra, em sede

de prova da responsabilidade extracontratual encontra-se no artigo 480.º do Código Civil, segundo o qual cabe ao lesado provar a culpa do autor da lesão.

«*Num sistema de responsabilidade subjectiva, a culpa do agente é elemento essencial da obrigação de reparar o dano, pelo que aquele que exige a responsabilidade terá de alegar e provar que existem os pressupostos dela. Significa que, aquele que exige a responsabilidade terá de alegar que o réu praticou o facto do qual pretende fazer derivar a responsabilidade e que praticou com culpa, isto é, ao autor cumpre fazer a prova do facto ilícito e, como a ilicitude depende da culpa do agente, terá também de provar que este procedeu com culpa*[18]».

Não obstante a regra enunciada no parágrafo anterior, o próprio Código Civil, no artigo 337.º, prevê as situações em que haverá inversão do ónus da prova, nomeadamente por dispensa ou liberação desse ónus ou sempre que a lei o determine. «*A inversão do ónus da prova ocorre quando não recai sobre a parte tradicionalmente onerada com a prova do facto o ónus de demonstrar, mas sobre a contraparte a quem incumbe o ónus de provar o facto contrário*[19]».

Com o enquadramento legal referido, o artigo 28.º da proposta de lei mais não faz que consagrar um caso de inversão do ónus da prova. O particular que seja lesado por um acto culposo praticado por uma entidade certificadora credenciada no exercício da actividade de certificação verá a sua pretensão facilitada, dado que não necessita fazer prova da culpa, antes cabendo à entidade certificadora fazer a prova de que actuou sem culpa [«*(...) excepto se*

[18] Rui Manuel de Freitas Rangel, *O Ónus da Prova no Processo Civil*, Almedina, Coimbra, 2000, pp.174-175.
[19] *Idem*, p. 178.

provar que não actuou de forma dolosa ou negligente (parte final do n.º 1 do artigo 28.º)]»[20].

15. Dispensa de credenciação (artigo 30.º)

Está aqui em causa a *dispensa de credenciação* dos serviços e entidades públicas, por se entender adequado que, em casos excepcionais, os serviços públicos possam ser de tal ser dispensados (tal, aliás, como fica desde logo realçado com a nova redacção do artigo 14.º).

Além disso, em consonância com o n.º 4 do artigo 18.º, estabelece-se a necessidade de publicação no *Boletim Oficial* do despacho de dispensa bem como a sua fundamentação.

Segundo o proponente, é necessária a existência de um mecanismo excepcional que permita que as entidades públicas possam ser autorizadas a exercer a actividade de certificação, mesmo quando não estejam reunidas as condições para haver um processo de credenciação. É o que se verificará, por exemplo, enquanto não for constituída a autoridade credenciadora. No entanto, tal como resulta do artigo 30.º, tais entidades serão sujeitas a uma cuidada avaliação das condições que dispõem para o exercício da referida actividade, o que garante o rigor no processo de autorização. O Governo, perante a Comissão, reiterou o carácter excepcional da dispensa de credenciação.

[20] Quanto à questão da responsabilidade civil por uso de assinaturas electrónicas, *vd*. M.H.M. Schellekens, *Electronic Signatures – Authentication Technology from a Legal Perspective,* Asser Press, The Hague, 2004, pp. 101 ss.; Relativamente às questões probatórias no âmbito das assinaturas electrónicas, *vd*. Lorna Brazell, *ob. Cit.*, pp. 194-203.

16. Revogações (artigo 34.º)

Com a aprovação da futura lei dos documentos e assinaturas electrónicas revogar-se-á o Decreto-Lei n.º 64/99/M, de 25 de Outubro, que foi pioneiro na consagração de normas legais destinadas a eliminar as barreiras ao desenvolvimento do comércio electrónico. Porém, tal como se refere na Nota justificativa, «*o quadro legal nele estabelecido, baseado na lei-modelo da* United Nations Comission on International Trade Law (UNCITRAL)*, revela-se hoje insuficiente, em especial pela incapacidade demonstrada para obviar às naturais desconfianças que as transacções por via electrónica ainda suscitam*». Mostra-se, assim, adequada a opção de substituição integral do regime constante do referido Decreto-Lei pelo da futura lei.

O facto de o Decreto-Lei n.º 64/99/M, de 25 de Outubro, fazer referência ao sistema de Intercâmbio Electrónico de Dados (EDI), sem contudo o regular, tem levado a que alguns operadores tenham suscitado dúvidas quanto ao futuro enquadramento legal do referido sistema.

O EDI é um sistema de troca de dados estruturados baseados em formatos de mensagens normalizados, entre sistemas computacionais, por meios electrónicos. Dados estruturados, significa um método, não ambíguo, de representar dados existentes num documento, seja ele uma factura, uma encomenda ou qualquer outro tipo de documento. O método para assegurar a correcta interpretação da informação pelo sistema computacional, é definido pela normalização. O conceito importante que devemos notar é que a troca electrónica de informação, no contexto do EDI puro, significa efectivamente, sem intervenção humana[21].

[21] http://students.fct.unl.pt/users/rpav/edi/edi.html (7/7/05)

Apesar de ser um sistema aplicado em operações comerciais efectuadas através de meios informáticos, o sistema EDI não é em si mesmo um sistema de certificação de assinaturas electrónicas, particularmente de assinaturas qualificadas. Razão pela qual, quando questionado pela Comissão, ter o Governo afirmado que a utilização do sistema EDI não sai prejudicada pela entrada em vigor da futura lei, podendo com ela coexistir. De facto, se é certo que o novo regime dos documentos e assinaturas electrónicas não implicará a "conversão" do sistema EDI e dos certificados por ele emitidos, em certificados qualificados, para os efeitos do regime constante da presente iniciativa legislativa, nem por isso os documentos emitidos nesse domínio deixarão de ter o valor jurídico e a força probatória previstos nos artigos 3.º e 4.º, n.º 3.

17. Entrada em vigor (artigo 35.º)

Considerou-se que a previsão, constante da versão inicial da proposta de lei, da entrada em vigor da lei no dia seguinte ao da sua publicação não se mostrava adequada.

No ordenamento jurídico local, «*entre a publicação e a vigência da lei decorrerá o tempo que a própria lei fixar; na falta de fixação, a lei entra em vigor no sexto dia posterior ao da publicação* (n.º 2 do artigo 4º do Código Civil)».

Desta norma resulta a possibilidade de o legislador fixar, casuisticamente, a data da entrada em vigor de cada lei, atendendo às suas características próprias e, sobretudo, resulta a enunciação de um prazo de *vacatio legis*, ainda que supletivo, que mais não é que o prazo que foi assumido como "normal" para mediar entre a publicação da lei e a sua entrada em vigor. O

período de *vacatio legis* destina-se a possibilitar o conhecimento da lei pelos seus destinatários antes de a mesma começar a produzir efeitos. Mais do que possibilitar um potencial conhecimento da lei pelos seus destinatários, este prazo de *vacatio legis* reforça a própria legitimação das normas jurídicas. É uma indicação clara de que não se deseja a existência de "leis-surpresa", ignoradas pelos seus destinatários e, como tal, incumpridas por estes.

«*O alargamento do período da vacatio justifica-se perante diplomas de especial complexidade, seja no seu conhecimento pelos destinatários, seja na tomada de medidas de execução pelos serviços competentes*[22]».

No caso concreto da presente iniciativa legislativa, considerou-se mais adequado prever um período de 30 dias entre a data de publicação da futura lei e a data da sua entrada em vigor.

18. Ajustamentos técnico-jurídicos

Para além dos aspectos abordados nos pontos anteriores, a Comissão considerou melhoramentos de redacção de várias normas visando o seu aperfeiçoamento técnico-jurídico, sem reflexos no conteúdo substancial das mesmas.

V – Conclusão

[22] M. Cordeiro, *Da aplicação da lei no tempo e das disposições transitórias*, *in* Legislação, n.º 7, Abril-Junho 93, pp. 7-29

Em conclusão, apreciada e analisada a proposta de lei, a Comissão:

a) é de parecer que a proposta de lei reúne os requisitos necessários para apreciação e votação, na especialidade, pelo Plenário;

b) sugere que, na reunião plenária destinada à votação na especialidade da presente proposta de lei, o Governo se faça representar, a fim de poderem ser prestados os esclarecimentos necessários.

Macau, 13 de Julho de 2005.

A Comissão,

Cheang Chi Keong
(Presidente)

Leonel Alberto Alves

Kou Hoi In

Hoi Sai Iun

Philip Xavier

Vitor Cheung Lap Kwan

João Bosco Cheang

Iong Weng Ian
(Secretária)