

ASSINATURA ELECTRÓNICA E CERTIFICAÇÃO DIGITAL

Miguel Pupo Correia

Mestre em Ciências Jurídico-Empresariais (FD-UC)

Professor na Universidade Lusíada – Lisboa

Advogado

1. Introdução

1.1. A influência das telecomunicações na transformação do mundo do Direito registou uma profunda mutação desde que, a partir dos anos 80 do séc. XX, a tecnologia digital nas redes e equipamentos de telecomunicações, deu origem à rápida criação e diversificação dos meios e serviços de telecomunicação, à redução progressiva de custos e preços, ao imparável dinamismo comercial do seu mercado; e, a partir de meados dos anos 90, se evoluiu de uma concepção “fechada” para uma concepção “aberta” das telecomunicações, graças ao explosivo crescimento da Internet e à generalização da acessibilidade aos respectivos serviços ou aplicações aos próprios utilizadores domésticos.

A cultura jurídico-económica tradicional estava - e ainda está, em larga medida... - baseada no uso de documentos escritos em papel, pelo que todo esse alicerce conceitual ficou posto em questão quando se deparou a possibilidade de eles passarem a ser remetidos por via electrónica.

Depara-se, então, a principal dificuldade: a comunicação telemática é muito directa e imediata, mas torna-se impessoal quando não implica a transmissão de voz e/ou imagem dos participantes. Num contexto de correio electrónico ou de grupos de discussão, caracterizado pela transmissão de mensagens escritas, o destinatário tem pouca possibilidade de se certificar da identidade do remetente, a não ser pela que este mesmo declara, o que coloca em crise a aplicação de todas as regras legais e sociais que dependem da identificação de uma pessoa em comunicação com outra. Além disso, os textos contidos em ficheiros de computador ou mensagens de correio electrónico são em regra facilmente alteráveis por qualquer pessoa que a eles tenha acesso, o que põe em causa a sua integridade e, por conseguinte, o seu valor como meio probatório.

Estas fragilidades tornam-se cruciais quando a comunicação electrónica tem um objectivo juridicamente relevante, nomeadamente quando se destina a transmitir uma declaração de vontade integrante de um negócio jurídico, *maxime* de um contrato, ou de uma relação administrativa. A necessidade de inteira *confiança* dos parceiros em transacções de comércio electrónico, ou em procedimentos administrativos conduzidos por via telemática, exige a certeza da identidade da outra parte, bem como da inalterabilidade dos textos transmitidos, para eliminar o receio de fraudes através da simulação de identidades pessoais ou falsificação do teor dos documentos, por parceiros ou terceiros de má fé.

Assim, o valor fundamental da *segurança jurídica*, esteio basilar da *confiança* que constitui a mola propulsora da adopção generalizada de qualquer forma de instrumental de relacionamento entre os sujeitos de direito, privados e públicos, exige a adaptação ou completamento dos textos legais baseados nas concepções tecnológicas tradicionais, ou a criação de normas tendentes a contemplar certas questões que as tecnologias da informação colocam de forma inovadora.

1.2. Desta preocupação fundamental resultou uma grande multiplicidade de iniciativas de variadas entidades de acção internacional, no sentido de criar um enquadramento normativo das várias questões ligadas ao denominado *lato sensu comércio electrónico* e que, assim, tendem a criar um quadro internacional orientador dos legisladores nacionais. Destaco apenas as principais:

a) A UNCITRAL/CNUDCI – Comissão das Nações Unidas para o Desenvolvimento do Comércio Internacional, que adoptou em 1996 uma “Lei Modelo sobre Comércio Electrónico” e, em 2001, uma “*Lei Modelo sobre Assinaturas Electrónicas*”;

b) A OCDE – Organização para a Cooperação e Desenvolvimento Económico, sobretudo a partir de 1998, quando aprovou, numa Conferência Ministerial em Ottawa, Canadá, um Plano de Acção para o EC, intitulado “Um Mundo sem fronteiras: concretizar o potencial do comércio electrónico mundial”;

c) A CCI – Câmara de Comércio Internacional, que, entre diversas iniciativas, promoveu a elaboração do *GUIDEC – General Usage for International Digitally Ensured Commerce*, publicado em 1997 e revisto em 2001, que constitui um importante repositório de elementos de informação e orientação sobre o CE.

d) A *União Europeia*, que tem desenvolvido um vasto conjunto de iniciativas, desde finais dos anos 80, com um vasto conjunto de estudos preparatórios no âmbito do “TEDIS - Programa comunitário relativo à transferência electrónica de dados para uso comercial, que utilize as redes de comunicação”⁽¹⁾, seguidos de diversas comunicações da Comissão⁽²⁾, e culminando com vários diplomas de regulamentação comunitária, entre as quais avulta, pelo interesse que tem para o nosso tema de hoje, a Directiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13.12.1999, relativa a um quadro legal comunitário sobre as assinaturas electrónicas ⁽³⁾;

Pouco a pouco, também as legislações nacionais têm vindo a assumir as questões jurídicas da realidade do comércio electrónico, consagrando normas específicas destinadas a regular as implicações deste ambiente tecnológico de comunicação de mensagens ⁽⁴⁾.

⁽¹⁾ Inclusivamente de carácter jurídico. Vd., p. ex., “*TEDIS - Situation juridique des Etats Membres au regard du Transfert Electronique de Données*” - Comissão das Comunidades Europeias - estudo elaborado pelo Escritório LODOMEZ-CROUQUET -Setembro 1989; e “*TEDIS - Situation juridique des Etats Membres de l'AELE au regard du Transfert Electronique de Données Commerciales*” - Comissão das Comunidades Europeias - estudo elaborado pelo escritório de advogados DUBARRY, GASTON-DREYFUS, LEVEQUE, LE DOUARIN, SERVAN-SCHREIBER & VEIL, sob a direcção de J.L. LODOMEZ.

⁽²⁾ “Uma Iniciativa Europeia sobre o Comércio Electrónico” – Comunicação da Comissão (COM(97)157); “Para um Quadro Europeu para Assinaturas Digitais e Criptografia” – Comunicação da Comissão (COM(97)503); e “Comércio Electrónico e Fiscalidade Indirecta” – Comunicação da Comissão (COM(1998)374 final, de 17.6.1998).

⁽³⁾ J.O.C.E, L 13, de 19.1.2000.

⁽⁴⁾ Para um repositório muito abrangente das iniciativas legislativas existentes, consulte-se: *Digital Signature Law Survey*, por Simone van der Hof & Bert-Jaap Koops, <http://rechten.uvt.nl/simone/ds-lawsu.htm>.

1.3. Portugal foi um dos países pioneiros na publicação de leis nesta matéria (o terceiro da Europa, a seguir à Alemanha ⁽⁵⁾ e à Itália ⁽⁶⁾), através da publicação do DL n° 290-D/99, de 2.8, referente aos documentos electrónicos e às assinaturas digitais, logo seguido do DL n° 375/99, de 18.9, sobre a factura electrónica ⁽⁷⁾.

Desde já faço notar que o DL n° 290-D/99 foi publicado antes da já referida Directiva 1999/93/CE relativa a um quadro legal comunitário sobre as assinaturas electrónicas, pelo que aquele diploma nacional, na sua versão inicial, não podia constituir formalmente a transposição desta Directiva para a ordem jurídica interna portuguesa. Contudo, os trabalhos preparatórios da Directiva foram tidos em conta na elaboração daquele diploma nacional.

A Directiva 1999/93/CE devia ser transposta para os ordenamentos nacionais dos Estados-Membros até ao dia 19.7.2001⁽⁸⁾. No nosso País, só veio a fazê-lo o DL 62/2003, de 3 de Abril. Este considerável atraso não era crucial, porque o conteúdo normativo da Directiva já estava largamente consagrado no nosso ordenamento interno. Apenas alguns aspectos de pormenor teriam de ser introduzidos na lei nacional para estabelecer uma transposição correcta e bastante. Não era necessário ir tão longe na adopção da terminologia da Directiva como se foi no DL n° 62/2003, de modo que coloca questões algo delicadas, que adiante referirei.

A propósito, não deixarei de lamentar a tendência, que se vem verificando em numerosos diplomas nacionais de transposição de directivas comunitárias, para a cópia dos termos destas, por vezes directa. Esquece-se que cada sistema jurídico dos Estados-Membros deve reflectir as respectivas especificidades culturais, sociais, económicas e jurídicas. O que é explicitamente salvaguardado pelo art. 249° do Tratado que institui a Comunidade Europeia, ao dispor: «A *directiva vincula o Estado-membro destinatário quanto ao resultado a alcançar, deixando no entanto às instâncias nacionais a competência quanto à forma e aos meios*». Como bem assinala MOTA DE CAMPOS ⁽⁹⁾, no elenco dos actos comunitários só o *regulamento* «é um rígido instrumento de uniformização jurídica», ao passo que a *directiva* é «uma alavanca mais flexível, adaptada ao objectivo menos ambicioso de simples *aproximação das legislações nacionais*, que permite atender aos particularismos nacionais deixando aos Estados-membros uma certa margem de liberdade na implementação das regras adoptadas a nível comunitário».

Assim, não existia motivo válido para serem postos de lado a *forma* e os *meios* que o legislador português adoptou no Decreto-Lei n° 290-D/99 – como são

⁽⁵⁾ Artigo 3 – *Signaturgesetz–SIG* - da Lei federal que estabeleceu as condições gerais para serviços de informação e comunicação (*Informations- und Kommunikationsdienste-Gesetz – IuKDG*), de 13.06.1997.

⁽⁶⁾ O art. 15, n° 2, da “Lei Bassanini” – Lei de 15.03.1997, n° 59 -, estabeleceu que «os actos, dados e documentos formados pela administração pública ou pelos privados com instrumentos informáticos ou telemáticos, os contratos estipulados nas mesmas formas, bem como o seu arquivo e transmissão com documentos informáticos, são válidos e relevantes para todos os efeitos da lei». Para regulamentação desta norma, o Decreto de 10.11.1997, n° 513 aprovou o regime dos documentos e contratos informáticos e seus requisitos de validade e eficácia, incluindo a assinatura digital.

⁽⁷⁾ Para mais detalhada análise destes diplomas, vd. MANUEL LOPES ROCHA, MIGUEL PUPO CORREIA, MARTA FELINO RODRIGUES, MIGUEL ALMEIDA ANDRADE e HENRIQUE JOSÉ CARREIRO, “*Leis do Comércio Electrónico – Notas e Comentários*”, Coimbra Editora, Coimbra, 2001.

⁽⁸⁾ Sobre o estado e problemas da transposição da Directiva 1999/93/CE, vd. JOS DUMORTIER e outros, “*The Legal and Market Aspects of Electronic Signatures*”, ICRI – Interdisciplinary centre for Law & Information Technology e Katholieke Universiteit Leuven, 2003, in <http://www.secorvo.de/publikationen/electronic-sig-report.pdf>.

⁽⁹⁾ “*Manual de Direito Comunitário*”, ed. Fundação Calouste Gulbenkian, Lisboa, 2000, p. 307.

eloquentemente os casos dos conceitos e definições respectivas nele adoptados – se fosse de considerar adequadamente satisfeita a finalidade fundamental da Directiva 1999/93/CE de harmonização do direito dos Estados-membros nesta matéria. Ora, este resultado, parece-me, estava substancialmente satisfeito pela versão inicial daquele Decreto-Lei.

E impunha-se usar de toda a cautela e rigor tecnológico e jurídico na revisão do nosso DL n.º 290-D/99, em ordem à introdução dos tais aspectos de pormenor a que me referi, em que se faria necessária uma compatibilização com os termos daquela Directiva, já que entre os dois diplomas não existia identidade de enfoque e de conteúdo.

O DL n.º 290-D/99 visava – e continua a visar, apesar de tudo! – objectivos algo diferentes dos da Directiva 1999/93/CE, embora não incompatíveis com os desta, o que tornava necessário que na transposição do regime comunitário se usasse das convenientes cautelas e se tivesse uma clara noção desta diversidade de perspectivas, o que não tenho a certeza que tenha sucedido ⁽¹⁰⁾.

O DL n.º 290-D/99 foi essencialmente norteado pelo objectivo de criar a base jus-privatística para o desenvolvimento das relações jurídicas de diversa natureza que se concretizam através de documentos electrónicos. Inspirando-se no certo enfoque da primeira lei italiana sobre esta matéria, o nosso diploma teve essencialmente presente criar a base normativa fundamental para o enquadramento dos *negócios jurídicos electrónicos*, destinada a proporcionar soluções adequadas para a salvaguarda da *segurança jurídica* com vista ao desenvolvimento das relações dos diversos campos do “comércio jurídico” em sentido amplo.

A realidade que aquele diploma nacional encara de frente é a de que estas relações se materializam em *documentos electrónicos*, pelo que é essencial: (a) definir as regras básicas sobre o valor probatório destes documentos, que implica a problemática da sua assinatura, e (b) regular a eficácia da transmissão de tais documentos como forma de comunicação das declarações de vontade que eles contenham, através das quais se formam negócios jurídicos e estabelecem entre os respectivos parceiros as relações de direito privado ou público. Daí a importância posta por ele na afirmação da validade e eficácia dos documentos electrónicos, equiparando-os para todos os efeitos legais aos documentos tradicionais em papel.

É sabido que o Direito Civil é *direito comum*, posto que os seus princípios e regras – principalmente os pertinentes à *relação jurídica* e ao *direito das obrigações* - constituem o fundamento basilar de todas as relações de todos os ramos do Direito. Pois bem: foi a pensar exactamente nisto que se quis construir, no DL n.º 290-D/99, um ordenamento geral da “relação jurídica por meios electrónicos”, capaz de suportar as implicações desta realidade em todos os ramos de direito; e, bem entendido, desde logo as relações de carácter civil e comercial, tendo designadamente em vista o favorecimento da expansão do *comércio electrónico*, portador de enormes potencialidades de desenvolvimento económico.

⁽¹⁰⁾ Sobre este confronto, bem como sobre a análise do nosso tema em geral, é imprescindível a consulta do excelente estudo de MIGUEL ALMEIDA ANDRADE “*As insondáveis razões de uma mudança desnecessária. O Decreto-Lei n.º 62/2003 e a transposição para a ordem jurídica interna da Directiva 1999/93/CE, relativa a um quadro legal comunitário para as assinaturas electrónicas*”, in <http://www.oa.pt/direitonarede/detalhe.asp?idc=11741&scid=11762&idr=11761&ida=12748>

Já a perspectiva da Directiva 1999/93/CE tem um enfoque bastante diverso do nosso diploma nacional: o que nela se pretendeu foi, primordialmente, desenvolver as trocas comerciais no âmbito do espaço económico europeu e a prestação transfronteiras de serviços de certificação ⁽¹¹⁾.

É, pois, um documento normativo voltado para impulsionar as actividades económicas das empresas que estão na base do sistema de assinaturas electrónicas - as *entidades certificadoras* e outras fornecedoras de meios e serviços ligados às denominadas *assinaturas electrónicas* -, na crença de que assim contribuirá para expandir o uso dos respectivos meios tecnológicos e, assim, facilitar as próprias trocas comerciais. Não é por acaso que PATRICK VAN EECKE e JOS DUMORTIER, autores do estudo em que se baseou o projecto da Directiva, num artigo de apresentação desta ⁽¹²⁾, afirmam logo de início: «A Directiva é baseada nos princípios de liberdade de estabelecimento e de livre prestação de serviços e nas regras relativas à aproximação das leis (i.e. os Artigos 47 (2), 55 e 95 do Tratado de Amsterdão)» (tradução minha). Daí que as suas preocupações fundamentais sejam, principalmente, a “neutralidade tecnológica” das assinaturas electrónicas e a liberdade incondicionada de acesso à actividade de certificação.

Trata-se, pois, para o legislador comunitário, de desenvolver a actividade económica de prestação de serviços de certificação electrónica, subalternizando o papel da assinatura como alicerce do valor probatório dos documentos e da inerente segurança do comércio jurídico.

1.5. O regime jurídico vigente entre nós nesta matéria é, como já se referiu, constituído pelo DL nº 290-D/99, com as alterações introduzidas pelo DL nº 62/2003, cujo escopo consiste – como declara o seu art. 1º - em transpor para a ordem jurídica interna a Directiva 1999/93/CE. É de se notar que o DL 290-D/99 continua a ser a referência correcta da lei vigente, visto que ele apenas foi modificado pelo DL nº 62/2003 e republicado em anexo a este na sua versão consolidada actual.

É conveniente ainda assinalar que a efectividade da aplicação deste regime depende em boa medida – *maxime*, para a credenciação de entidades certificadoras no nosso País – da publicação da regulamentação prevista no actual art. 39º do DL 290-D/99, que continua a ser aguardada.

A novidade do tema do regime especial dos documentos electrónicos e da sua assinatura – que continua relativamente desconhecido, apesar dos 4 anos já decorridos sobre a publicação do DL nº 290-D/99– e a preocupação de dar a conhecer e compreender o melhor possível o significado das soluções legais em questão, obrigam-me a uma exposição geral daqueles temas, ao longo da qual procurarei fazer ressaltar as alterações agora introduzidas.

Começarei por tratar dos documentos electrónicos, passando depois ao regime das assinaturas.

2. Prova dos contratos: os documentos electrónicos

⁽¹¹⁾ Cfr. MANLIO CAMMARATA e ENRICO MACCARONE, “I problemi del recepimento della direttiva 1999/93/CE”, in <http://www.interlex.it/docdigit/recep1.htm>.

⁽¹²⁾ “A Common Legal Framework for Electronic Signatures Within the European Union”, in “Analysis & Perspective”, vol. 4, nº 48, 22.12.99, p. 1200 e ss.

2.1. O princípio da liberdade de forma (art. 219º C. Civil) remove à partida qualquer obstáculo de ordem geral à admissibilidade pelo nosso ordenamento jurídico de que as declarações de vontade negociais se materializem através de meios de comunicação electrónica. Pode, então, formar-se um contrato verbalmente por telefone, ou por troca de mensagens escritas por fax, telex, correio electrónico. Na ponta da evolução estão actualmente os chamados contratos *click-wrap*, geralmente de compra e venda ou prestação de serviços, baseados numa proposta constante de uma página da Internet, e formados através da aceitação dos respectivos termos e condições manifestada apenas por um “click” com o “rato” ou comando equivalente num ícone ou botão contendo a expressão “Aceito” ou sinónima, eventualmente seguida de um comando complementar do tipo “Enviar” ou semelhante ⁽¹³⁾.

Em todos os casos de manifestação escrita das declarações negociais, estamos perante *documentos*, que exprimem o conteúdo volitivo das pessoas participantes numa negociação destinada a criar ou a dar execução a um negócio jurídico – *maxime*, um contrato - civil ou comercial (consultas, propostas de condições, encomendas, aceitações, facturas, recibos, etc.). Assim, também as mensagens escritas por meios electrónicos e respectivos registos informáticos devem ser considerados como verdadeiros *documentos*, face à amplitude da definição do art. 362º do C. Civil, que é sabiamente ampla e tecnologicamente neutra. Como ensinam PIRES DE LIMA e ANTUNES VARELA ⁽¹⁴⁾, «essencial à noção de *documento* é a função *representativa* ou *reconstitutiva* do objecto». Tal noção abrange, portanto, não só os escritos, mas outros objectos, entre os quais aqueles Autores citam os discos e “cassetes” audio e video, as fitas cinematográficas. Daí que, naturalmente, se devam entender analogamente abrangidos os registos electromagnéticos (contidos em discos e bandas) em que essencialmente consistem os documentos electrónicos.

Também o art. 368º do C. Civil considera como documentos as "reproduções fotográficas ou cinematográficas, os registos fonográficos e, de um modo geral, quaisquer outras reproduções mecânicas de factos ou coisas", redacção que, não obstante influenciada pelo "estado da técnica" na época da sua redacção, pode abarcar, por mera interpretação extensiva e actualista, todas as formas de reprodução e transmissão de voz, dados e imagens por meios electrónicos, como *reproduções de factos ou coisas* e, portanto, no âmbito da relevância probatória do conteúdo dos respectivos originais.

Não obsta a este entendimento a inviabilidade de esses registos reproduzirem a realidade original de forma absolutamente íntegra: como bem refere E. GIANNANTONIO ⁽¹⁵⁾, «a reprodução mecânica entendida como reprodução perfeitamente fiel do original não existe; nenhum fenómeno é exactamente igual a

⁽¹³⁾) ALEXANDRE DIAS PEREIRA, “*Serviços da Sociedade de Informação – Alguns Problemas Jurídicos do Comércio Electrónico na Internet*”, in <http://www.fd.unl.pt>, p. 19; ANA MARGARIDA MARQUES, MAFALDA ANJOS e SÓNIA QUEIROZ VAZ, “*101 Perguntas e Respostas do Direito da Internet e da Informática*”, CentroAtlântico, Lda, Famalicão-Lisboa, 2002, p. 136; MARK GROSSMAN, ALLISON KIMBERLY HIFT e RAQUEL ROTHMAN, “*Click-Wrap Agreements – Enforceable Contracts or Wasted Words*”, in <http://www.becker-poliakoff.com>; GOLDS Solicitors, “*The mouse the click and the contract*”, in <http://www.golds.co.uk>; CHRISTIAN STEWART, “*Internet Law: A click-wrap agreement helps with online transactions*”, in <http://www.amarillonet.com>.

⁽¹⁴⁾ *Cód. Civil Anotado*, 1967, vol. I, p. 236.

⁽¹⁵⁾ *Manuale di Diritto dell'Informatica*, Pádua, Cedam, 2ª ed., 1997, p. 379, baseando-se na citação de L. MONTESANO (*Sul documento informatico come rappresentazione meccanica nella prova civile*, in *Il diritto dell'informazione e dell'informatica*, 1987, p. 25) em face do art. 2712 do C.Civil italiano, que foi a fonte do art. 368º do nosso Código.

outro. (...) A fidelidade da reprodução, de facto, não deve ser entendida de modo absoluto, mas relativo, isto é, em relação aos fins para os quais é utilizada a reprodução (...). Pode assim dizer-se que também o documento electrónico constitui uma reprodução mecânica quando a actividade de tratamento e, por isso, de transformação não incida sobre os elementos essenciais para os fins da relevância probatória do facto.»⁽¹⁶⁾

Portanto, a equiparação dos documentos electrónicos a quaisquer outros documentos era e continua a ser perfeitamente sustentável em face do regime “clássico” do Código Civil. Mas esse princípio tornou-se uma aquisição expressa e incortornável da ordem jurídica portuguesa a partir da entrada em vigor do DL n.º 290-D/99, cujo primeiro tema fulcral é a definição de regras basilares sobre os *documentos electrónicos*.

Desde logo, o art. 2.º, al. a), deste diploma, define *documento electrónico* como «o documento elaborado mediante processamento electrónico de dados». Note-se que não se define aqui o que seja *documento*, fazendo-se, assim, uma remissão implícita para a definição constante do art. 362.º do Cód. Civil, já citado.

O documento electrónico é, pois, basicamente o documento formado mediante o uso de um equipamento informático, *maxime* de um computador.

Esta categoria dos documentos não é completamente homogénea, podendo classificar-se, consoante o modo como os documentos são produzidos pelo computador, em: *documentos electrónicos em sentido estrito*, que são memorizados em forma digital em memórias magnéticas ou ópticas, e são destinados apenas a ser lidos pelo computador, pelo que não podem ser lidos ou apercebidos directamente pelo homem; e *documentos electrónicos em sentido amplo*, ou simplesmente *documentos informáticos*, que são todos os gerados através dos equipamentos periféricos do computador - impressora, “plotter”, etc. -, de modo a serem lidos ou interpretados pelo homem⁽¹⁷⁾.

2.2. Embora o conceito de *documento* englobe uma grande variedade de objectos, não há dúvida de que existe uma *acepção restrita* deste conceito, que abrange apenas os *escritos* que corporizam uma declaração de ciência ou de vontade⁽¹⁸⁾, significado que transparece de variadas disposições legais, nomeadamente a maior parte das que se referem à prova documental.

Ora, a lei não define o que é *documento escrito*, embora faça largo uso deste conceito, mormente ao exigir que revistam essa forma determinados actos jurídicos, quer para fins meramente probatórios (forma *ad probationem*), quer como requisito da

⁽¹⁶⁾ No sentido de que os documentos informáticos «são *ex natura* documentos não assinados que reproduzem dados constantes da memória do computador», pelo que se lhes aplica o art. 368.º C. Civil, cfr. A. RIBEIRO MENDES, “Valor Probatório dos Documentos Emitidos por Computador”, in Colóquio “Informática e Tribunais”, Ministério da Justiça, Lisboa, 1991, p. 522. Todavia, este autor acrescenta logo de seguida que «não se tratando de documentos particulares subscritos pelo seu autor (ou por outrem, a rogo deste) não tem sentido invocar o disposto nos artigos 374.º a 376.º do Código Civil». Esta opinião parece-me actualmente ultrapassada pela evolução tecnológica e legislativa que no texto se descreve.

⁽¹⁷⁾ Sobre a distinção, cfr. E. GIANNANTONIO, obra cit., p. 366 e ss.

⁽¹⁸⁾ A. VARELA, “Manual de Processo Civil”, Coimbra Editora, Coimbra, p. 489, e A. RIBEIRO MENDES, obra cit., p. 520. Também para CARNELUTTI (*apud* E. GIANNANTONIO, obra cit., p. 364, nota 1), o *documento em sentido amplo* é qualquer coisa que represente um facto, ao passo que o *documento em sentido estrito* é o escrito.

sua validade (forma *ad substantiam*). É, pois, importante reunir as principais notas caracterizadoras do que seja um *escrito*, designadamente as seguintes ⁽¹⁹⁾:

- a) Constitui escrito qualquer conjunto de sinais (arábicos, numéricos, estenográficos, criptográficos, ideográficos, etc.) expressos numa determinada linguagem, na qual represente um significado compreensível;
- b) Não é necessário que o escrito provenha da mão humana, podendo resultar do emprego de meios mecânicos ou electrónicos;
- c) Não é preciso que tais sinais sejam indeléveis (pense-se nas memórias magnéticas), desde que se conservem por um período de tempo minimamente correspondente ao desempenho da função para que o escrito foi elaborado;
- d) Não é relevante o suporte sobre o qual é impressa a mensagem (não é necessário escrever sobre meios móveis e transmissíveis como os cartulares = em papel), sendo possível, p. ex., ter documentos escritos em monitores de computador, filmes, placas de pedra ou barro, paredes, etc..

A esta luz, os chamados *documentos informáticos*, produto da impressão de um ficheiro de computador, caso reünam as características definidoras acima apontadas, podem ser com segurança qualificados como *documentos escritos*. Na realidade, nada permite distinguir um de tais documentos, processado em papel ou suporte equivalente pela impressora conectada a um computador, de um escrito dactilografado por uma outra clássica forma de escrever.

Mais complexa poderá ser, no entanto, a análise da questão de saber se podem considerar-se como documentos escritos os *documentos electrónicos em sentido estrito*, isto é, documentos mantidos em memória de computador, por nela terem sido gerados ou recebidos por transmissão telemática. Mas é indiscutível que, numa perspectiva *finalística*, existe substancial equivalência do *documento electrónico em sentido estrito* aos documentos escritos cartulares ou em papel ⁽²⁰⁾, já que um escrito é um conjunto de sinais apostos por qualquer meio ou técnica sobre um suporte qualquer, desde que tais sinais se mantenham legíveis após o transcurso de algum tempo, de modo a satisfazer as duas finalidades essenciais do documento escrito: a reflexão e registo por um período de tempo útil de um determinado conteúdo declarativo.

Este entendimento é sustentável num entendimento amplo da noção de *escrito* subjacente ao art. 363º, 1, do C. Civil., correspondendo ao entendimento corrente de *escrito* como «representação do pensamento em caracteres convencionais» ⁽²¹⁾.

Deste modo, podia já extrair-se da conjugação dos artigos 363º, nº 1, e 368º do C. Civil o entendimento que permitia abarcar no conceito de *documento escrito* o documento elaborado num computador, assim como a reprodução electrónica de uma mensagem transmitida por via telemática.

⁽¹⁹⁾ Neste sentido, F. ANTOLISEI, *Manuale di Diritto Penale*, Giuffrè, Milão, 1982, p.s. II, 586, *apud* D. TAGLINO, *Il valore giuridico del documento elettronico*, Roma, 1996, in <http://freepage.logicom.it/DanyPage/tesi.zip>, p. 4.

⁽²⁰⁾ Neste sentido, R. BORRUSO, *Tre tesi di fondo dell'informatica giuridica*, in *Giur. Italiana*, 1986, IV, 224; e *Computer e diritto*, t. I, Giuffrè, Milão, 1988, p. 41; e R. CLARIZIA, *Informatica e conclusione del contratto*, Giuffrè, Milão, 1985, p. 100; ambos *apud* D. TAGLINO, obra cit., p. 5; e E. GIANNANTONIO, obra cit., p. 384.

⁽²¹⁾ *Lello Universal – Dicionário Enciclopédico Luso-brasileiro*, 1988, t. 1, p. 875, verbete “Escrita”.

Mas este entendimento tornou-se expressamente adoptado pelo nº 1 do art. 3º do DL nº 290-D/99, o qual torna claro que o documento electrónico cujo conteúdo seja susceptível de representação como declaração escrita é havido, para todos os efeitos, como um documento escrito. Assim, a mera circunstância de o texto ser criado ou recebido e estar arquivado num suporte informático e ser acessível à leitura apenas no monitor de um computador, antes e à margem da sua impressão em papel, não retira a esse texto o carácter de um escrito.

E, por isso, se o acto documentado estiver legal ou convencionalmente sujeito ao requisito de forma escrita, esse requisito será para todos os efeitos de considerar como preenchido por um documento electrónico que contenha a declaração integrante desse acto.

2.3. A eficácia jurídica dos documentos em geral e dos documentos electrónicos em especial está, como já dissemos, fortemente dependentemente da *confiança*, *credibilidade* ou *fiabilidade* que possam merecer como reproduções – melhor se diria *revelações* – de factos ou objectos, o que depende essencialmente de dois factores: *genuinidade* e *segurança*. É *genuíno* o documento quando não sofreu alterações. É *seguro* tanto mais quanto mais difícil for alterá-lo e mais fácil for descobrir as alterações que tenha sofrido e reconstituir o texto original ⁽²²⁾.

Tem especial pertinência a valorização destes factores no tocante aos documentos electrónicos, já que estes podem sofrer alterações decorrentes dos factores de *risco* para a genuinidade e a segurança dos documentos, factores esses que são de dois tipos: *erros*, devidos a actuações humanas involuntárias, falhas técnicas ou factores externos; e *fraudes*, isto é, actuações humanas intencionais ⁽²³⁾.

Podemos configurar três tipos fundamentais de problemas que se devem equacionar em tema de *segurança* do documento electrónico:

- a) Por um lado, o da *autenticidade* do documento, ou seja, na lição de CARNELUTTI ⁽²⁴⁾, a correspondência entre o autor aparente e o autor real do documento. Este requisito comprova-se normalmente através de uma *assinatura*, tema que iremos desenvolver adiante;
- b) Por outro lado, o da *integridade* do documento, isto é, o da sua preservação contra alterações que lhe modifiquem o conteúdo. Na verdade, uma vez criado o documento, em termos de assumir a sua forma definitiva, ele não pode ficar sujeito a alteração, já que esta dará causa a um novo documento, diferente e independente do documento primitivo. Ora, os documentos conservados em memórias comuns de computadores ou com elas relacionadas (bandas magnéticas ou “diskettes”) são facilmente modificáveis por qualquer um que tenha a eles acesso através do respectivo computador, o que põe em risco imediato a sua integridade. Daí que, para a satisfação deste requisito, os documentos electrónicos hajam de ser preservados contra modificações através da sua inserção em arquivos protegidos: memória ROM (*read only memory*) do disco rígido do computador, ou disco óptico (CD-ROM), etc.;

⁽²²⁾ E. GIANNANTONIO, obra cit., pp. 375 e segs.

⁽²³⁾ Cfr. A. RIBEIRO MENDES, obra cit..

⁽²⁴⁾ *Apud* V. CARRACOSA LÓPEZ *et al.*, *La contratación informática: el nuevo horizonte contractual*, Ed. Comares, Granada, 1997, p. 67.

- c) Ainda por outro lado, há que referir o pressuposto da *confidencialidade* do documento, ou seja, a sua preservação contra o acesso por pessoas não autorizadas, que, não sendo em si mesmo basicamente imprescindível, todavia funciona como um requisito de reforço da sua *integridade*, quando os interessados pretendam que o documento não seja acessível a terceiros não autorizados. São actualmente muito desenvolvidas, para preservar a confidencialidade dos documentos electrónicos, as técnicas de *criptografia*⁽²⁵⁾, basicamente consistentes na criação de condições de ininteligibilidade dos dados para quem não possua as chaves de cifragem-decifragem.

O problema da segurança e da autenticação e, por isso, do valor probatório dos documentos electrónicos reveste-se da maior delicadeza em se tratando de documentos desmaterializados, conservados apenas em memória de computador, isto é, de *documentos electrónicos em sentido estrito*. E não se pode esquecer que tal questão possui significativa importância, dado que um dos objectivos mais significativos a satisfazer através da adopção de um ambiente de documentação electrónica, é exactamente o da desmaterialização documental, com os efeitos dinamizadores e as poupanças de encargos que daí resultam para a actividade empresarial e administrativa.

2.4. Se, como já vimos, os *documentos electrónicos* podem e devem considerar-se como documentos *escritos*, é preciso todavia examinar quais as condições do seu *valor probatório*, designadamente no tocante ao requisito legal da *assinatura* do documento escrito pelo seu autor (art. 373º, nº 1, do C. Civil).

Este requisito é de enorme importância, porque um documento não assinado não tem legalmente valor superior a qualquer outro meio de prova comum, sujeito a livre apreciação do julgador, isto é, não pode de modo nenhum atingir a *força probatória plena* que cabe aos documentos particulares assinados cuja letra e assinatura, ou só assinatura, sejam consideradas verdadeiras (art. 376º C. Civil).

Foi esta importante questão que o Decreto-Lei nº 290-D/99 veio resolver, ao dispor que o requisito de forma escrita de documento particular assinado é inequivocamente satisfeito se o acto constar de documento electrónico com *assinatura digital* – expressão agora alterada para *assinatura electrónica qualificada* ⁽²⁶⁾ - do respectivo outorgante (art. 3º, nº 2).

Importa desde já fazer notar que a Directiva 1999/93/CE não interfere com esta matéria: face aos Considerandos 17, 20 e 21 da Directiva ⁽²⁷⁾ e do seu artigo 5º ⁽²⁸⁾,

⁽²⁵⁾ Sobre este tema, cfr. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões, tendo em vista a segurança e a confiança na comunicação electrónica*, COM(97)503, de Outubro de 1997.

⁽²⁶⁾ Adiante explicarei esta alteração.

⁽²⁷⁾ «17) A presente directiva não tem por objectivo harmonizar as disposições nacionais relativas à legislação contratual, designadamente a celebração e a execução de contratos, ou outras formalidades de natureza não contratual que exigem assinaturas; por esse motivo, as disposições relativas aos efeitos legais das assinaturas electrónicas não devem prejudicar os requisitos formais constantes da legislação nacional no que respeita à celebração de contratos ou às regras relativas à forma, que determinam o lugar onde um contrato é validamente celebrado. (...) 20) A definição de critérios harmonizados relativos aos efeitos legais das assinaturas electrónicas, criará um quadro legal comunitário coerente em toda a Comunidade; as legislações nacionais determinam os diferentes requisitos para o reconhecimento legal das assinaturas manuscritas; podem ser utilizados certificados para confirmar a identidade de uma pessoa que assine electronicamente; a existência de certificados qualificados e de assinaturas electrónicas avançadas

parece-me evidente que a matéria do valor probatório dos documentos assinados é reservada pela Directiva às legislações nacionais, não constando dela disposições específicas a este respeito.

Assim, há que distinguir com nitidez entre a questão do *valor probatório dos documentos electrónicos* – que a lei interna portuguesa pode perfeitamente regular, sem oposição ou interferência das normas comunitárias – e a do *valor jurídico das assinaturas electrónicas*, nomeadamente das *digitais*.

O que nos transporta para a análise em detalhe da questão, a um tempo tecnológica e jurídica, da assinatura electrónica, à qual vou passar agora a referir-me, visto que ele se prende de forma inafastável com o tema do valor probatório dos documentos electrónicos assinados.

3. Assinatura dos documentos electrónicos

3.1. O valor probatório dos documentos electrónicos depende entre outros requisitos, do da *assinatura* pelo seu autor. Realmente, decorre do art. 373º, nº 1, do C. Civil, que os documentos particulares devem ser *assinados* pelo seu autor.

Já vimos que deste requisito é manifesta, por isso que um documento não assinado não tem legalmente valor superior a qualquer outro meio de prova comum, sujeito a livre apreciação do julgador, isto é, não pode de modo nenhum atingir a *força probatória plena* que cabe aos documentos particulares assinados cuja letra e assinatura, ou só assinatura, sejam consideradas verdadeiras (art. 376º C. Civil).

Mas o que é que se entende por *assinatura*? A nossa lei civil não contém uma definição deste conceito fundamental, pelo que teremos de encetar a seu respeito um itinerário interpretativo.

É corrente na doutrina portuguesa tradicional o entendimento de que o legislador se quer referir à assinatura *autógrafa*, isto é, ao sinal identificativo do seu autor, em

tem por objectivo obter um nível de segurança mais elevado; as assinaturas electrónicas avançadas baseadas num certificado qualificado e criadas por um dispositivo seguro de criação de assinaturas apenas podem ser consideradas como juridicamente equivalentes às assinaturas manuscritas se obedecerem aos requisitos que para estas são exigidos; 21) Para contribuir para uma aceitação generalizada dos métodos de reconhecimento das assinaturas electrónicas, deve garantir-se que estas possam ser utilizadas como elementos de prova para efeitos processuais perante as jurisdições de todos os Estados-Membros; o reconhecimento legal das assinaturas electrónicas deve basear-se em critérios objectivos e não estar ligado à autorização do prestador de serviços de certificação envolvido; a determinação dos domínios legais em que podem ser utilizados documentos electrónicos e assinaturas electrónicas é regida pelas legislações nacionais; a presente directiva não prejudica o poder de tribunais nacionais decidirem quanto à conformidade com os requisitos da presente directiva, nem afecta as disposições nacionais em matéria de liberdade de apreciação judicial das provas».

(²⁸) «1.Os Estados-Membros assegurarão que as assinaturas electrónicas avançadas baseadas num certificado qualificado e criadas através de dispositivos seguros de criação de assinaturas:

- a) Obedecem aos requisitos legais de uma assinatura no que se refere os dados sob forma digital, do mesmo modo que uma assinatura manuscrita obedece aqueles requisitos em relação aos dados escritos, e
 - b) São admissíveis como meio de prova para efeitos processuais.
2. Os Estados-Membros assegurarão que não sejam negados a uma assinatura electrónica os efeitos legais e a admissibilidade como meio de prova para efeitos processuais apenas pelo facto de:
- se apresentar sob forma electrónica;
 - não se basear num certificado qualificado;
 - não se basear num certificado qualificado emitido por um prestador de serviços de certificação acreditado;
 - não ter sido criada através de um dispositivo seguro de criação de assinaturas. »

regra construído a partir do seu nome civil escrito, completo ou abreviado, sinal esse escrito pelo próprio punho do autor ⁽²⁹⁾.

Contudo, não me parece sequer conforme com a realidade histórico-legislativa o entendimento tradicional de que o requisito da assinatura previsto na lei só seria satisfeito pela tradicional *assinatura autógrafa*. Já em 1930 a Comissão de Redacção das Leis Uniformes sobre as Letras e Livranças e sobre os Cheques frisava que «a palavra *assinatura* é aqui empregada num sentido amplíssimo, para designar qualquer sinal material que sirva, segundo os usos do país, para identificar, em qualquer papel ou título, a personalidade daquele que a apõe». E a doutrina e jurisprudência dos Estados Unidos, relativamente à exigência de assinatura dos documentos constante dos chamados “*Statutes of Frauds*”, vêm adoptando o entendimento liberal de que não é exigida forma específica para a assinatura, a qual pode ser impressa, dactilografada, ou feita por qualquer outra marca, desde que tenha sido aposta, ou adoptada pela parte ou seu agente, para o fim de autenticar o escrito. Idêntica orientação tem sido detectada na jurisprudência dos tribunais ingleses.

Portanto, bem vistas as coisas, nem sequer foi necessário o recente desafio das novas realidades geradas pela tecnologia informática para que essa maneira de ver as coisas começasse a ser posta em crise.

3.2. Tentemos, então, uma visão *funcional* do conceito de assinatura. Para que serve a assinatura?

Em geral, *a assinatura constitui um sinal ou meio, susceptível de ser usado com exclusividade por uma dada pessoa através da sua aposição num documento, sinal esse através do qual o autor deste revela a sua identidade pessoal de forma inequívoca, manifesta as suas declarações de vontade ou conhecimento dele constantes e, na medida do possível, procura preservar a integridade do documento, quando é transmitido a outra pessoa.*

A doutrina tradicionalista – ainda arreigada à ideia de que só pode haver *assinatura autógrafa* - entendia que o documento electrónico não poderia ser considerado como documento escrito particular, por lhe faltar a aposição da assinatura ⁽³⁰⁾. Mas esta visão foi ultrapassada pela evolução do pensamento jurídico, revelada por diversas soluções normativas e por múltiplas posições doutrinárias e de organizações internacionais, que progressivamente têm vindo a acolher a compatibilidade de um entendimento mais amplo do requisito da assinatura com uma eficaz tutela dos interesses de segurança jurídica envolvidos.

Ganhou assim progressiva influência a opinião de que podem ser admitidas modalidades de *assinatura electrónica*, à luz de uma *concepção funcional*, isto é, que tenha em conta as funções essenciais desempenhadas pela assinatura dos documentos

⁽²⁹⁾ Vd, no sentido desta orientação tradicional, A. VAZ SERRA, “*Provas - Direito Probatório Material*”, BMJ 111º-154 e ss; e A. VARELA *et al.*, obra cit., p. 497. Na Jurisprudência, é neste sentido o Acórdão da Relação do Porto de 19.10.1978, *Col. Jur.*, 1978 – 4º, p. 1257.

⁽³⁰⁾ E. GIANNANTONIO, obra cit., pp. 392 e ss. No mesmo sentido G. VERDE, *Per la chiarezza di idee in tema di documentazione informatica*, in *Riv. Dir. Proc.*, 1990, p. 721; BUSTI, *Nuovi documenti del contratto di trasporto di cose*, Cedam, Pádua, 1983, p. 145; e F. PARISI, *Il contratto concluso mediante computer*, Cedam, Pádua, 1987, p. 64; todos *apud* D. TAGLINO, obra cit., p. 7. Vd. tb. os autores citados por D. TAGLINO, obra cit., p. 6 e seg.; e quanto ao direito francês, A. BERTRAND, “*Computers, Telecommunications, Value Added Services and Evidence in Civil Law*”, in “*Legal and Economic Aspects of Telecommunications*”, 1990, p. 706.

(³¹). Uma vez que os documentos electrónicos não comportam a tradicional *assinatura autógrafa*, que é característica da “civilização do papel”, neles podem ser usados, consoante as circunstâncias, diversos outros meios de autenticação que se costumam agregar sob a designação genérica de *assinatura electrónica*.

Sob esta designação, são abrangidos vários processos ou meios técnicos de *autenticação* ou *assinatura “lato sensu”*(³²), dos quais se destacam fundamentalmente os seguintes:

- a) *Código secreto*: Consiste numa combinação de algarismos ou letras que condiciona o acesso à utilização de sistemas informáticos, consistindo as formas mais utilizadas num código de acesso (*password*), constituído de forma alfanumérica, ou num código numérico que constitui um número pessoal de identificação (PIN), sendo em geral combinadas com a utilização de um cartão magnético ou portador de um microprocessador (*chip*). Pressupõe-se que a *password* ou o PIN é conhecido apenas do seu proprietário (o utilizador) e que existe algures num ficheiro informático onde o gestor do sistema (“*system manager*”) não deve ter acesso fácil (seria até desejável que não pudesse tê-lo a não ser com a colaboração daquele). Em regra, o utilizador pode alterar o código quantas vezes quiser (de forma automática face ao sistema informático) e essa alteração frequente é mesmo incentivada em muitas empresas (p. ex., com a caducidade do código ao cabo de um certo prazo).
- b) *Assinatura digitalizada*: É constituída pela reprodução da assinatura autógrafa do autor, memorizada como imagem por uma “scanner” e depois aposta como cópia em cada documento que se deseje assinar. Embora PARISI (³³) objecte a esta modalidade de assinatura electrónica a circunstância de ela não permitir uma distinção entre a assinatura original e a reproduzida, por serem exactamente iguais, a verdade é que isso acontece sem tirar nem pôr no caso da chancela ou outro meio de reprodução dita mecânica. Além disso, é de se notar que a segurança da autenticidade deste “chancela electrónica” não é menor do que a das chancelas tradicionais: estas poderão ser utilizadas por pessoa diversa do seu autor apenas se este o consentir; o mesmo acontece com aquela, já que o autor da assinatura memorizada por “scanner” pode guardá-la sob uma *password* só dele conhecida, inibindo assim a sua utilização abusiva por terceiro (³⁴).

(³¹) THIERRY PIETTE-COUDOL e outros, obra cit. p. 32.; e sobre esta *concepção funcional* da assinatura e os requisitos que dela resultam para a plena validade da assinatura electrónica, o já citado Y. POULLET, “*Probate Law: From Liberty to Responsibility*”, in “*The EDI Law Review*”, 2-1994, pp. 85 e ss.

(³⁶) B. AMORY, “*Electronic Data Interchange (EDI) and the conclusion of contract*”, comunicação à “*TEDIS Legal Workshop*”, Bruxelas, 19-20.06.1990, pp. 25 e ss.; A. BERTRAND, *ob. e loc. cit.*, pp. 704 e ss.; A. GALTUNG, “*Evidential Issues in an Electronic Data Interchange Context According to Norwegian Law*”, in “*Law, Computers & Artificial Intelligence*”, vol. 1, nº 3, 1992, pp. 345 e ss.; O. HANCE, “*Business et Droit d’Internet*”, ed. McGraw Hill, 1996, pp. 170 e ss.

(³³) Obra cit.

(³⁴) A esta luz, numa prática de relações negociais em termos de comércio electrónico pode perfeitamente convencionar-se (normalmente por normas adequadas de um *Interchange Agreement*, que garantam por outros modos a segurança das transacções estabelecidas entre as respectivas partes) no sentido de serem aceites como assinaturas meras indicações impressas dos nomes dos autores dos documentos, ou reproduções digitalizadas das suas assinaturas autógrafas.

- c) *Chave biométrica*, baseada no reconhecimento de características físicas do indivíduo por equipamento adequado (impressões digitais, face, íris, sangue). Abrange vários processos que apresentam a vantagem de uma identificação praticamente perfeita e inquestionável da pessoa, mas possuem inconvenientes que os tornam praticamente pouco utilizáveis. Por um lado, não asseguram por si sós a função de manifestação de vontade do autor, que só pode ser assegurada por um outro processo associado àquele. Por outro lado, na maior parte dos casos o reconhecimento da pessoa por certa ou certas características físicas necessita de conferência com um espécime autêntico para proporcionar a identificação do seu autor⁽³⁵⁾.
- d) *Assinatura digital* ou *criptográfica*, que comporta duas modalidades, consoante os sistemas em que se baseia:
- a. *Criptografia simétrica com chave única*: funciona a partir de uma mesma chave possuída pelo emitente e pelo receptor da mensagem e que serve simultaneamente para codificá-la e descodificá-la. Apresenta como inconvenientes: a necessidade da multiplicação das chaves consoante os vários interlocutores de uma mesma pessoa ou empresa; a maior facilidade de a chave cair em poder de um terceiro; e a possibilidade de uma das partes atribuir falsamente declarações à outra, uma vez que a chave é a mesma para ambas;
 - b. *Criptografia assimétrica com chave pública*: utiliza uma “chave pública” e uma “chave privada”, a primeira das quais descodifica as mensagens encriptadas com a segunda. Dada a sua relevante importância, por ser a base do sistema traçado na Directiva 1999/93/CE (apesar da fantasiada “neutralidade tecnológica” com que esta se adorna...), vou em seguida explicar um pouco mais detalhadamente em que consiste.

3.3. A chamada *assinatura digital* ⁽³⁶⁾ - no seu sentido corrente e usual, que se refere apenas à *assinatura digital de criptografia assimétrica* - consiste numa modalidade de assinatura electrónica em sentido restrito – a bem dizer, é a única modalidade actualmente testada e generalizadamente reconhecida e utilizada... - composta por uma espécie de “*selo electrónico*”, que é acrescentado a uma mensagem e que é criado através de um sistema criptográfico assimétrico, que gera e atribui ao respectivo titular uma “chave privada” e uma “chave pública”.

O titular do par de chaves, para assinar um documento, utiliza a sua *chave privada* (que deve conservar cuidadosamente guardada e sigilosa), e a assinatura

⁽³⁵⁾ Cfr. BRUCE SCHNEIER, “*Biometrics: Truths and Fictions*”, in “Crypto-Gram Newsletter” 15.8.1998, <http://www.counterpane.com/crypto-gram-9808.html>

⁽³⁶⁾ Sobre este tema, cfr., MANUEL LOPES ROCHA, MIGUEL PUPO CORREIA, MARTA FELINO RODRIGUES, MIGUEL ALMEIDA ANDRADE e HENRIQUE JOSÉ CARREIRO, obra cit., passim. Vd. tb., além dos documentos citados nas notas precedentes: O. HANCE, “*Business et Droit d’Internet*”, ed. McGraw Hill, 1996, p. 170 e ss; R.T. NIMMER, *The formation of contracts electronically*, 1996; J. ROSENOER, “*CyberLaw - The Law of Internet*”, Springer, New York, 1996, p. 238 e ss; KENNETH ALLEN, *Utah Digital Signature Program*; A. MONTI, *Il documento informatico nei rapporti di diritto privato*, InterLex, 21.11.1997; G. BUONOMO, *Atti e documenti in forma digitale*, InterLex, 21.11.1997; A. STERBENZ, *Digital Signaturen – Eine Introduction*, 1996, Instituto para protecção de dados aplicada e tecnologia da comunicação da Universidade Técnica de Graz; T.S.BARASSI, *The Cybernotary: Publica Key Registration and Certification and Authentication of International, Legal Transactions*; D. GREENWOOD, *Electronic Signatures and Records: Legal, Policy and Technical Considerations*, 1997.

será verificada pelo destinatário da mensagem com a *chave pública* correspondente àquela. O par *chave pública/chave privada* é gerado por um algoritmo matemático que assegura que a assinatura apenas poderá ser verificada pela *chave pública* se tiver sido criada com a correspondente *chave privada*. Entre as duas chaves existe uma relação matemática tal que: não se consegue calcular uma chave a partir da outra; e quando um conjunto de dados for cifrado com uma das chaves, só a outra chave pode decifrá-lo.

O “selo electrónico” que forma a assinatura digital é constituído por uma série de dados (letras, algarismos, símbolos), cuja aposição numa mensagem se processa em dois momentos: primeiro, o “software” adequado realiza uma “hash function”, que dá origem a uma espécie de resumo (“hash”) dos dados da mensagem; logo a seguir, a *chave privada* cifra este “hash” gerando assim a assinatura digital, que é então aditada à mensagem electrónica e transmitida para o destinatário da mensagem (documento electrónico) conjuntamente com esta.

O destinatário da mensagem, ao recebê-la com a assinatura digital, aplica a esta a *chave pública*, obtendo assim a prova de que a mensagem provém do remetente-signatário: para tal, usando o mesmo algoritmo, o destinatário cria um “hash” da mensagem, que é comparado com o “hash” proveniente do remetente; se os dois “hashs” forem iguais, comprova-se que a mensagem não foi alterada.

Note-se que o objectivo da assinatura digital não é o de tornar a mensagem ilegível, pois a mensagem em si mesma não é cifrada. A assinatura digital é apenas adicionada à mensagem electrónica, mantendo esta intacta e perfeitamente legível⁽³⁷⁾.

Assim, na síntese de A. STERBENZ⁽³⁸⁾, a assinatura digital:

- É autêntica, pois prova ao destinatário que o subscritor assinou o documento e este é uma manifestação da sua vontade;
- Não pode ser falsificada, pois prova o facto de o documento ter sido assinado pelo subscritor e não por outra pessoa;
- Não pode ser usada de novo: é parte do documento e não pode ser transferida para outro documento;
- Impede que o documento seja modificado depois de assinado;
- Não pode ser contestada, por ser uma prova de que o signatário marcou o documento.

A verificação positiva de uma assinatura digital (assimétrica) conduz, portanto, a um elevado grau de autenticidade da autoria e da integridade do documento ao qual ela seja aposta, porquanto comprova seguramente que a assinatura foi aposta pelo seu titular e que o documento não foi alterado desde o seu envio ao destinatário.

3.4. Do que referi atrás (nº 3.2), resulta a existência de variados meios tecnológicos enquadráveis à partida no conceito de *assinatura electrónica* (em sentido amplo).

Vejamos agora em que termos este conceito foi adoptado na versão original do DL nº 290-D/99 e na Directiva 1999/93/CE. Importa assinalar algumas diferenças, das

⁽³⁷⁾ Em todo o caso, há a possibilidade de o sistema ser simultaneamente usado para gerar a assinatura digital e para cifrar a mensagem com ela assinada.

⁽³⁸⁾ Obra cit.

quais resultou a introdução pelo DL 62/2003, sob o influxo daquela Directiva, de algumas alterações ao DL 290-D/99. Vejamos:

Na versão original do DL 290-D/99, a *assinatura electrónica* era definida (art. 2º, al. a)), como o «resultado de um processamento electrónico de dados susceptível de constituir objecto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento electrónico ao qual seja aposta, de modo que:

- i) identifique de forma unívoca o titular como autor do documento;
- ii) a sua aposição ao documento dependa apenas da vontade do titular;
- iii) a sua conexão com o documento permita detectar toda e qualquer alteração superveniente do conteúdo deste».

Adoptava-se, assim, um *sentido restrito* da definição de assinatura electrónica, que exigia a reunião daqueles três requisitos, correspondentes às três funções fundamentais: identificação inequívoca do seu autor, autonomia da sua aposição e inalterabilidade do documento assinado.

Note-se que, das modalidades de *assinatura electrónica em sentido amplo* a que me referi atrás, várias não satisfazem a estes três requisitos e não poderiam, pois, enquadrar-se nesta definição. Assim sucede com: os *códigos secretos* (*password* e PIN), posto que se trata de meros meios de acesso a sistema e não de autenticação de documentos, pelo que não identificam inequivocamente o autor do documento, nem são apostos a este, nem permitem detectar alterações deste; com a *assinatura digitalizada*, visto que, sendo copiada de um ficheiro, a sua aposição ao documento não depende apenas da vontade do titular, além de não permitir detectar alterações posteriores do documento; as *chaves biométricas*, que também são *meros meios de acesso a sistemas e instalações*, pelo que, tal como os códigos secretos, não realizam nenhuma das três funções da assinatura electrónica *stricto sensu*; e a *assinatura digital de criptografia simétrica* (*chave única*), porque, sendo a sua única chave utilizada tanto para gerar a assinatura como para a verificar, é lógico que não pode haver a certeza de quem foi o autor da assinatura: se quem é o titular dela, se uma outra pessoa a quem foi fornecida com o objectivo primário de verificar a assinatura do outro.

Não quer isto dizer, porém, que estas formas de *assinatura electrónica em sentido amplo* não possam ser utilizadas como meio de autenticação da autoria de documentos, se as circunstâncias específicas de cada tipo de uso e os interesses em jogo o recomendarem. Tal é possível através da adopção de algum desses meios por uma *convenção sobre a prova*, amplamente possibilitada, não só em geral pelo art. 345º do Código Civil, mas especificamente pelo nº 4 do art. 3º do DL nº 290-D/99.

A Directiva 1999/93 e o DL 62/2003 (art. 2º, al. b)) vieram, porém, consagrar a acepção mais ampla de *assinatura electrónica*: «resultado de um processamento electrónico de dados susceptível de constituir objecto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento electrónico».

E, depois, criaram um conceito mais restrito – dir-se-á talvez melhor: intermédio - de *assinatura electrónica avançada* (art. 2º, al. c)): «assinatura electrónica que preenche os seguintes requisitos:

- i) Identifica de forma unívoca o titular como autor do documento;
- ii) A sua aposição ao documento depende apenas da vontade do titular;
- iii) É criada com meios que o titular pode manter sob seu controlo exclusivo;

iv) A sua conexão com o documento permite detectar toda e qualquer alteração superveniente do conteúdo deste.»

Se bem se notar, esta definição comporta os mesmos requisitos que constavam da definição restrita de *assinatura electrónica* constante da versão inicial do DL 290-D/99, já que a aparentemente nova sub-alínea iii) é um mero corolário da sub-alínea ii) e está contida numa correcta interpretação desta.

Ora bem: a versão primitiva do DL 290-D/99 admitia dentro do conceito (que, como mostrei, era restrito) de *assinatura electrónica* o de *assinatura digital*, na modalidade de *criptografia assimétrica*. Era o que constava da definição da al. c) do art. 2º: «processo de assinatura electrónica baseado em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento electrónico ao qual a assinatura é aposta e concordância com o seu conteúdo, e ao declaratório usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento electrónico foi alterado depois de aposta a assinatura».

Ora, o DL 62/2003 manteve no art. 2º a definição de *assinatura digital*, que apenas passou da al. c) para a actual al. d), e nela modificou a frase “processo de assinatura electrónica” para “processo de assinatura electrónica avançada”, adaptando assim a redacção (neste como em muitos outros pontos), à nova terminologia.

Mas, depois, acrescentou ao art. 2º uma nova al. g) – totalmente fora da ordem imposta pela lógica da sequência e hierarquia de conceitos... - com um novo conceito de *assinatura electrónica qualificada*, que define como: «Assinatura digital ou outra modalidade de assinatura electrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura».

Portanto, a *assinatura digital* é configurada agora como uma espécie dentro do género *assinatura electrónica qualificada*, que por sua vez é uma espécie dentro do género *assinatura electrónica avançada*.

3.6. Qual a utilidade desta escalada de conceitos? Será que, além da *assinatura digital* (de *criptografia assimétrica*) existem outros meios tecnológicos que possam ser classificados como *assinaturas electrónicas qualificadas* ou como *assinaturas electrónicas avançadas*?

Os já citados predecessores do projecto da Directiva 1999/93/CE, PATRICK VAN EECKE e JOS DUMORTIER ⁽³⁹⁾ parecem entender que sim, mas fazem-no apenas no domínio das hipóteses e em termos tais que me leva a crer que não têm razão e, sobretudo, que não tomaram na devida conta e peso a gravidade das implicações deste assunto para a segurança do comércio jurídico, valor fundamental a ponderar.

Referem, na verdade, que a definição de *assinatura electrónica avançada* é semelhante à de *assinatura digital* adoptada pela norma ISO 7498-2. E, embora acentuem que esta definição é “tecnologicamente neutral” – ou seja, comportaria vários processos tecnológicos, o que é estranho, porque a assinatura digital está

⁽³⁹⁾ Obra e local cit., p. 1201.

tecnologicamente bem caracterizada... -, acabam por afirmar, mais adiante ⁽⁴⁰⁾, que «embora os requisitos de segurança decorrentes do Anexo (III da Directiva) estejam escritos numa forma tecnologicamente neutral, eles claramente espelham a bem conhecida tecnologia da assinatura digital».

Portanto, a terminologia da Directiva está feita a pensar numa só e única realidade: a *assinatura digital*, embora camuflada para dar a entender que é polivalente, que serve para uma pluralidade indeterminada de outras tecnologias de assinatura electrónica.

E seria, segundo aqueles autores, dentro do conceito de *assinatura digital* que se descobriria a pluralidade de aplicações do conceito de *assinatura electrónica avançada*, dado que eles entendem que «as assinaturas digitais, tal como definidas pela ISO, podem ser realizadas na prática não só usando criptografia assimétrica, mas também usando criptografia simétrica associada com dispositivos de criação de assinaturas à prova de alteração ilícita, impenetráveis (“tamper-proof”) e dispositivos de verificação de assinatura também “tamper-proof”».

Aparentemente, este ponto de vista encaixa com a definição de *assinatura electrónica avançada* constante do regime da Directiva, porque, apesar de a *criptografia simétrica* (sistema de chave única, a que me referi atrás) se basear no uso de uma mesma chave criptográfica pelo autor da assinatura e pelo verificador da autoria dela, se o dispositivo de verificação de assinatura (isto é: a memória onde resida a chave criptográfica única à disposição do destinatário do documento e que deve poder verificar a origem da assinatura) for à prova de intrusão (“tamper-proof”), o verificador não poderá ter acesso à chave única de modo a poder usá-la para gerar assinaturas.

Sucedo, contudo, que esta ideia é puramente “wishful thinking”, porque corresponde a um ideal que não existe, já que têm sido recorrentemente detectadas vulnerabilidades nos dispositivos “tamper-proof”, que levam os peritos a substituir essa expressão pela mais prudente e algo eufemística de “tamper-resistant”... ⁽⁴¹⁾

Cito, a propósito, o seguinte texto expressivo: «*How tamper-proof is ‘tamper-proof’? Classically, ‘tamper-proof’ means that a component is shielded, i.e. it cannot be penetrated. Nevertheless, in order to handle the difficulty of finding out that some components were ‘imperfectly’ tamper-proof, experts in the area introduced an alternative designation, ‘tamper-resistant’, to express that fact. However, the imprecision of the latter is uncomfortable, leading to what we call the “watch-maker syndrome”: - “Is this watch water-proof?”; - “No, it’s water-resistant.”; - “Anyway, I assume that I can swim with it!”; - “Well yes, you can! But... I wouldn’t trust that very much...”*»

Deste modo – e porque não se pode esquecer que estamos num domínio de absoluta sensibilidade a eventuais falhas de segurança -, entendo que o sistema de assinatura de criptografia simétrica não satisfaz o fundamental requisito da *assinatura electrónica* (agora cognominada de “*avançada*”...) de que a sua aposição ao documento dependa apenas da vontade do titular, visto que a pessoa que tenha em seu poder um dispositivo de verificação de assinatura (ainda que qualificado de “tamper-proof”, *rectius* “tamper-resistant”...) poderá eventualmente vir a usá-lo para gerar assinaturas em nome do titular da chave única.

⁽⁴⁰⁾ Ibidem, p. 1204.

⁽⁴¹⁾ Cfr. PAULO VERÍSSIMO; NUNO FERREIRA NEVES e MIGUEL PUPO CORREIA (Eng.), “*Intrusion-Tolerant Architectures: Concepts and Design. In Architecting Dependable Systems*”, R. Lemos, C. Gacek, A. Romanovsky (eds.), LNCS 2677, Springer Verlag, 2003.

Portanto, a assinatura com um sistema de criptografia simétrica (chave única) não deve considerar-se como satisfazendo os requisitos da *assinatura electrónica avançada*, ou da designada simplesmente *assinatura electrónica* na versão original do DL 290-D/99. Ademais, ela é desprovida de interesse prático, porque o sistema de assinatura digital de criptografia assimétrica (de par de chaves, privada e pública) é muito mais seguro e eficaz e, por isso mesmo, é o que está largamente generalizado, pelo que a escolha daqueloutra não oferece qualquer utilidade relevante.

3.7. E daí que toda a estrutura normativa da Directiva 1999/93/CE e do DL 62/2003, mesmo empregando estes novos conceitos, esteja arquitectada sobre os pressupostos tecnológicos da *assinatura digital de criptografia assimétrica*: chaves privada e pública (respectivamente equivalentes aos conceitos de *dados de criação de assinatura* e *dados de verificação de assinatura*), dispositivos (seguros) de criação e de verificação de assinatura, certificado, entidade certificadora, etc.

Apesar disso, a preocupação principal do DL nº 63/2003 consistiu na transposição formalista dos conceitos da Directiva 1999/93/CE, como se vê pela inserção no texto da lei de conceitos tão herméticos quanto realmente inúteis (penso que já o demonstrei) como são os seguintes:

- *Assinatura electrónica avançada*, equivalente à inicial definição de assinatura electrónica,

- *Assinatura electrónica qualificada*, género com uma única espécie: a assinatura digital de criptografia assimétrica,

- *Dados de criação de assinatura* e *dados de verificação de assinatura*, eufemismos que significam o mesmo que “chave privada” e “chave pública”, respectivamente,

- *Dispositivo de criação de assinatura* e *dispositivo seguro de criação de assinatura*, expressões totalmente ilógicas do ponto de vista jurídico, pois pretendem conceptualizar com sabor tecnológico a existência ou não de cautelas quanto à guarda da chave privada – por isso é que o “dispositivo” que a contém é “seguro” ou não “seguro”... – e a própria função intrínseca da chave privada na criação da assinatura,

- *Certificado qualificado*, repetição inútil do conceito de *certificado* (antes designado mais apropriadamente de *certificado digital*, pois é específico da assinatura digital), como adiante veremos;

- *Produto de assinatura electrónica*, que, além de terminologicamente incorrecto (uma assinatura electrónica não produz nada...) ainda por cima é confuso, por demasiado genérico, pois nada mais significa do que um meio técnico destinado a ser utilizado na prestação de serviços ou na criação de uma *assinatura electrónica qualificada* (e não de toda e qualquer assinatura electrónica...).

Note-se, no entanto, que foram mantidas no art. 2º do DL nº 290-D/99 as definições de *assinatura digital*, *chave privada* e *chave pública*, sinal de que o nosso legislador de 2003 se lembrou de que o que continua a existir e a valer, realmente, na linguagem corrente e na prática técnica e económica relevante, é a *assinatura digital de criptografia assimétrica*.

Mas tão mal andou o legislador que, depois, estoutros conceitos desaparecem completamente do articulado do DL n° 290-D/99 ⁽⁴²⁾, o que nos permite imaginar em que palpos de aranha se verão os futuros intérpretes que tiverem que apurar onde é que as disposições do diploma acolhem as já bem conhecidas *assinatura digital, chave privada e chave pública!*...

Em suma: o legislador do DL n° 62/2003 mostrou-se mais preocupado com a introdução da terminologia de Bruxelas do que com a realidade prática existente e as necessidades da confiança dos agentes económicos e da segurança do comércio jurídico!

3.8. O DL 62/2003 (tal como a Directiva 1999/93) não acrescentou nada a não ser categorias artificiais - *assinatura electrónica avançada e qualificada* -, sob o pretexto de que tal era necessário para assegurar a chamada *neutralidade tecnológica*, isto é, que os ditos conceitos intermédios seriam necessários para assegurar a introdução imediata de novas modalidades que venham a surgir mercê da inovação tecnológica.

Esta ideia da *neutralidade tecnológica*, como bem assinala o Dr. MIGUEL ALMEIDA ANDRADE, no excelente estudo que já citei atrás ⁽⁴³⁾, é correcta em abstracto, mas tem um pressuposto que não é exacto: o de que as diversas tecnologias são plenamente equivalentes e que a sua aplicação depende das mesmas regras de direito. O que pura e simplesmente não é verdade.

E é por isso mesmo que, além de PATRICK VAN EECKE e JOS DUMORTIER, que já citei, também a EESSI – European Electronic Signature Standardisation Initiative reconhece que, afinal, a Directiva 1999/93/CE não é estritamente neutra do ponto de vista tecnológico, pois «implicitamente define um quadro técnico» que é o da *assinatura digital!*... ⁽⁴⁴⁾

Não resisto a citar a advertência seriíssima de MANLIO CAMMARATA, em texto recente acerca deste assunto (onde foca outros aspectos da questão que aqui não tenho espaço para abordar) ⁽⁴⁵⁾:

«A posição do legislador italiano fundava-se no conceito de que a emanção de qualquer regra jurídica deve seguir os princípios do direito, assumindo a tecnologia como instrumento. Aos técnicos cabe a competência (essencial) para estabelecer as regras técnicas, mas as leis devem ser escritas por juristas. Veja-se, sobre este ponto, a intervenção de E. Maccarone “La supremazia del diritto sulla tecnologia”: *A importância das tecnologias - escrevia Maccarone há poucos meses – é fundamental e inegável, mas nenhuma sociedade pode fundar sobre elas a sua própria existência: o direito deve dar as regras, isto é, aquela mistura de sabedoria, moralidade, compromisso, conhecimento, equidade, desumana humanidade e experiência sobre as quais se fundam todas as sociedades. Se isto é verdadeiro, então seja bem-vindo o contributo das ciências e da tecnologia, mas não pretendam estas apoderar-se das nossas regras de convivência civil, do direito.*» (Tradução minha).

⁽⁴²⁾ Cfr. MIGUEL DE ALMEIDA ANDRADE, “As insondáveis razões...” cit.,

⁽⁴³⁾ *Supra*, nota 9.

⁽⁴⁴⁾ *Apud* MIGUEL DE ALMEIDA ANDRADE, obra cit.

⁽⁴⁵⁾ MANLIO CAMMARATA, “Una catena di errori che parte da Bruxelles”, 10-07-03, in <http://www.interlex.it/docdigit/sparita3.htm>

3.9. Em suma: a Directiva e o DL 62/2003, que lhe copiou a terminologia, não conduzem a lado nenhum senão à tecnologia já conhecida, internacionalmente testada, geradora de confiança, e legalmente aceite entre nós – como em numerosíssimos países dos cinco continentes, da *assinatura digital*.

Ora, para isso não era necessário alterar o DL 290-D/99 inicial, e torná-lo na confusão de conceitos em que se tornou, por dois motivos essenciais:

- a) Porque o seu art. 1º, nº 2, já dizia que: «O regime previsto no presente diploma pode ser tornado aplicável a outras modalidades de assinatura electrónica que satisfaçam exigências de segurança idênticas às da assinatura digital.». Solução, aliás, muito mais prudente do que a da aplicação automática do regime do diploma a essas novas modalidades, porque nada assegura, à partida, que elas garantam plena equivalência à assinatura digital, de modo a merecerem a aceitação universal que esta, depois de largamente testada, pôde merecer. Provavelmente, uma nova tecnologia de assinatura electrónica qualificada exigirá outros pressupostos tecnológicos e, por consequência, outros conceitos. Ou seja, a sua introdução será inviável sem uma alteração da estrutura legal. E, então, muito provavelmente, toda esta confusa terminologia não terá servido para nada a não ser para criar insegurança nos destinatários da lei, que somos todos nós e, deste modo, para dificultar e prejudicar a difusão alargada deste importantíssimo sustentáculo do comércio electrónico!
- b) Porque - como melhor explicarei mais adiante - as partes nas relações jurídicas estabelecidas mediante o uso de documentos electrónicos são livres – ao abrigo do nº 4 do art. 3º do DL nº 290-D/99 - de estabelecer uma convenção adoptando, para os devidos efeitos probatórios, um outro método de assinatura desses documentos diferente do da *assinatura digital de criptografia assimétrica*. O que permite, na actualidade, a dose exacta de neutralidade tecnológica: essas outras modalidades de assinatura electrónica podem ser adoptadas se os sujeitos das relações jurídicas o quiserem, por convir aos seus interesses. Nada de mais justo, conveniente, razoável e seguro!

Confirma-se, assim, que as alterações introduzidas pelo DL nº 62/2003 não trouxeram nada de substancialmente novo à nossa ordem jurídica, já que, salvo alguns detalhes de pormenor, o DL nº 290-D/99, na sua versão inicial, já reflectia a substância das soluções daquela Directiva e era harmónico com ela.

Não há justificação, portanto, para que o DL nº 62/2003 tenha copiado as expressões conceituais e definições adoptadas naquela Directiva, com a agravante de que merecem fortes reservas a sua razoabilidade intrínseca e o seu enquadramento na nossa ordem jurídica interna.

Apesar de tudo, em síntese final e como farol hermenêutico para o actual DL nº 290-D/99, tenha-se bem presente esta ideia: a realidade tecnológica contemplada pelo seu regime jurídico continua a ser a mesma: a *assinatura digital de criptografia assimétrica*. Esta é que existe no mercado, devidamente testada sob o ponto de vista da segurança que proporciona, e em condições de funcionar generalizadamente.

3.10. Como já referi atrás, a verificação positiva de uma assinatura digital conduz a um elevado grau de certeza jurídica da autenticidade da autoria e da integridade do

documento ao qual ela seja aposta, porquanto comprova seguramente que a assinatura foi aposta pelo seu titular e que o documento não foi alterado desde o seu envio ao destinatário. Consequentemente, a um documento assim assinado pode ser atribuída por lei a força probatória de um original escrito e assinado pelo seu subscritor.

São estes o sentido e os fundamentos do comando contido no n.º 1 do art. 7.º do DL n.º 290-D/99, que enuncia enfaticamente o valor jurídico da *assinatura electrónica qualificada* (=assinatura digital), declarando-a equivalente à assinatura autógrafa dos documentos com forma escrita sobre suporte de papel e formulando uma presunção jurídica – obviamente ilidível por prova do contrário – de que no documento electrónico ao qual foi aposta uma assinatura digital se verificam as três funções desta e os correspondentes efeitos práticos e jurídicos:

- a) *Função identificadora*, pela qual a assinatura atribui inequivocamente a declaração ao signatário, estabelecendo a autoria deste, ou em seu nome próprio, ou como representante de uma pessoa colectiva;
- b) *Função finalizadora ou confirmadora*, que não só exprime a conclusão espacial do documento escrito, mas também o assentimento do signatário quanto às declarações de vontade e/ou de conhecimento dele constantes, assumindo-as como sendo próprias dele e estando correcta e completamente expressas no texto precedente ⁽⁴⁶⁾;
- c) *Função de inalterabilidade*, já que a verificação positiva de uma assinatura digital pelo destinatário comprova que o documento ao qual ela foi aposta não foi alterado depois da aposição da assinatura, até à sua recepção pelo destinatário.

Trata-se, aliás, um enunciado, ao que se saiba, até agora não fora feito no nosso direito positivo para qualquer outro tipo de assinatura – nem mesmo a autógrafa –, o que desde já traduz um valor acrescentado assinalável da presente norma.

Alguns aspectos normativos específicos ajudam a consolidar o valor probatório conferido pela assinatura digital ao documento a que seja aposta.

Assim, o art. 7.º, n.º 2 proíbe a *contitularidade* de uma assinatura digital – ou seja, do respectivo certificado e do inerente par de chaves criptográficas – por duas ou mais pessoas. Mas permite que seja dela titular uma *pessoa colectiva*. Neste caso, será de regra a definição das pessoas singulares habilitadas com poderes de representação que lhes permitam utilizar a chave privada para aposição de assinaturas digitais: tal definição poderá constar do próprio certificado da assinatura ou de um certificado complementar (cfr. os arts. 7.º, n.º 2, e 28.º, n.º 2, do diploma citado).

Muito importante é também a equiparação legal da assinatura digital a todos os *outros sinais identificadores* que sejam exigidos por lei ou convenção (art. 7.º, n.º 3). Assim, nos documentos assinados por este meio, deixará de ser necessário o carimbo de uma sociedade, o selo branco de um serviço público, etc.

⁽⁴⁶⁾ Esta função implica necessariamente, à luz do *princípio da confiança*, na sua vertente da proibição de *venire contra factum proprium*, a característica do *não repúdio*, que significa que o autor do documento assinado com assinatura digital fica impedido de negar a autoria do documento. A literatura anglo-saxónica tende a autonomizar a *non repudiation* como função da assinatura digital.

Lamentavelmente, porém, e sem qualquer motivo razoável, o DL nº 62/2003 suprimiu o antigo nº 4 do art. 7º do Decreto-Lei nº 290-D/99, que continha, pedagogicamente, o enunciado normativo dos elementos constitutivos do regime da assinatura digital, que se desenvolvem em outras normas deste diploma e que são:

- a) Existência de um par de chaves criptográficas, pública e privada;
- b) Utilização da chave privada para geração da assinatura digital;
- c) Correspectividade necessária da chave privada à chave pública;
- d) Emissão de um certificado que contenha a chave pública, por uma entidade certificadora credenciada nos termos deste diploma;
- e) Validade do certificado, quer quanto à sua emissão, quer por não estar suspenso, nem revogado, nem caduco por ultrapassagem do seu prazo de validade; o que teria por consequência a sua inexistência jurídica, ou seja, ter-se o documento por não assinado (art. 7º, nº 5).

4. O valor probatório dos documentos electrónicos assinados

4.1. Passo agora, no itinerário lógico da exposição que me propus, a completar o tema do valor probatório dos documentos electrónicos, com as implicações do regime da *assinatura* disciplinada pelo DL nº 290-D/99.

Assim, importa ressaltar que só o documento electrónico portador de uma *assinatura electrónica qualificada exarada ao abrigo de um certificado emitido por uma entidade certificadora que se ache credenciada ao abrigo do DL nº 290-D/99* é que gozará da força probatória prevista no art. 376º do Cód. Civil (vd. o nº 2 deste artigo).

Ou seja: se a entidade certificadora emitente do certificado não se achar credenciada em conformidade com a lei portuguesa (ou não beneficiar da equiparação que o art. 38º da actual versão do Decreto-Lei nº 290-D/99 atribui às entidades certificadoras credenciadas noutros Estados-membros da União Europeia), o documento não será destituído de valor probatório, mas este não será superior ao que resultar da sua apreciação nos termos gerais de direito. Ou seja: não deixará de ser um documento escrito e assinado, mas não poderá ter força probatória plena, antes será apreciado segundo o livre critério do julgador.

Em termos homólogos, o nº 3 do artigo 3º deste diploma disciplina o valor probatório dos documentos electrónicos que não revistam forma escrita, submetendo-o ao regime dos arts. 368º do Cód. Civil e 167º do Cód. de Processo Penal, desde que aos documentos em causa seja aposta uma *assinatura electrónica qualificada*, certificada por uma entidade credenciada nos termos do DL nº 290-D/99 e que reúna os demais requisitos neste formulados. Vale aqui a mesma consideração acabada de fazer quanto aos certificados emitidos por entidade não credenciada.

4.2. Mas o nº 4 do mesmo artigo 3º consagra ainda um outro importante aspecto relativo à força probatória dos documentos electrónicos, ao dispor que: «*O disposto nos números anteriores não obsta à utilização de outro meio de comprovação da autoria e integridade de documentos electrónicos, incluindo outras modalidades de assinatura electrónica, desde que tal meio seja adoptado pelas partes ao abrigo de válida convenção sobre prova ou seja aceite pela pessoa a quem for oposto o documento.*»

Esta norma confere pleno relevo à autonomia da vontade (art. 405º do Cód. Civil), reconhecendo valor probatório à identificação da autoria - isto é, à assinatura *lato sensu* - de documentos electrónicos, ou de comprovação da sua integridade, que resulte de um meio técnico eleito mediante uma *convenção sobre prova* ou aceite pela pessoa perante a qual se pretenda fazer valer o documento.

Poderão deste modo assinar-se documentos por outros processos técnicos, que constituam modalidades de mera *assinatura electrónica* em sentido amplo (al. *b*) do art. 2º do DL nº 290-D/99), ou que sejam outra modalidade de *assinatura electrónica avançada* (al. *c*) do mesmo artigo). Está, assim, explicitamente consagrada na lei a validade, p. ex., de convenções em contratos de uso de PIN para utilização de cartões bancários, ou para uso de *password* para acesso a certos serviços de telecomunicações, etc.

Esta norma, que já existia na versão original do DL nº 290-D/99 – tendo apenas sido adaptada a sua redacção pelo DL nº 62/2003 à terminologia da Directiva 1999/93/CE – consagra, ao fim e ao cabo, de modo juridicamente muito mais consistente, a “*neutralidade tecnológica*” que a Directiva teve em vista, pois consente amplamente que as partes convençionem, de forma expressa ou tácita, o uso de formas de assinatura electrónica condizentes com os seus interesses. Mas consagra-a – note-se bem – com respeito pela vontade das partes e não à revelia destas e por imposição tecnocrática.

Aliás, o nº 5 deste mesmo art. 3º do nosso diploma ressalva o valor probatório, apreciado em termos gerais de direito, dos documentos electrónicos aos quais não seja aposta qualquer assinatura electrónica, ou uma assinatura electrónica que não reúna os requisitos de “qualificada certificada por entidade certificadora credenciada”.

Ou seja: os nºs 4 e 5 do art. 3º conjugam-se para consagrar na nossa ordem interna o efeito jurídico visado pelo nº 2 do art. 5º da Directiva, de que «não sejam negados a uma assinatura electrónica os efeitos legais e a admissibilidade como meio de prova para efeitos processuais» apenas por não obedecer aos requisitos da assinatura electrónica qualificada certificada por uma entidade credenciada. Circunstância que me parece não ter sido cabalmente apercebida pelo legislador do DL nº 62/2003, que teria poupado bastante trabalho e nos pouparia à confusa terminologia que veio introduzir se a tivesse na devida conta...

E é evidente que os documentos assinados segundo o meio técnico eleito pelas partes por via convencional terão o valor probatório que elas lhes tenham do mesmo modo querido atribuir, sem limitação: poderão, portanto, atribuir-lhe valor de prova plena.

Tal tipo de convenção sempre seria, aliás, perfeitamente compatível com os termos do art. 345º do Cód. Civil, já que dela não parece, em princípio, poder resultar uma inversão do ónus da prova⁽⁴⁷⁾, nem a exclusão ou admissão de um meio de prova, ou a violação de determinações legais fundadas em razões de ordem pública⁽⁴⁸⁾.

⁽⁴⁷⁾ Aliás, mesmo sobre o ónus da prova são, em princípio, admissíveis convenções deste tipo, a menos que versem sobre direito indisponível ou dificultem excessivamente o exercício do direito (nº 1 do art. 345º).

⁽⁴⁸⁾ A adopção de uma convenção sobre a prova pode ser solução adequada em qualquer meio de comércio electrónico e mesmo no que toca à vida interna de uma empresa, como forma de conferir valor probatório aos documentos electrónicos *stricto sensu* nela gerados.

4.3. Eliminando as dúvidas que poderia suscitar uma interpretação extensiva ou actualizadora das normas do art. 387º do Cód. Civil (que alude especificamente a “cópias fotográficas”) e do art. 168º do Cód. de Processo Penal) que se refere a “reprodução mecânica” de documentos), o art. 4º do Decreto-Lei nº 290-D/99 (que se mantém inalterado) veio clarificar o valor jurídico das cópias dos documentos electrónicos, dispondo: «As cópias de documentos electrónicos, sobre idêntico ou diferente tipo de suporte, são válidas e eficazes nos termos gerais de direito e têm a força probatória atribuída às cópias fotográficas pelo nº 2 do artigo 387º do Código Civil e pelo artigo 168º do Código de Processo Penal, se forem observados os requisitos aí previstos.»

Esta norma aplica-se tanto às cópias que constituam *documentos electrónicos em sentido estrito* como também às cópias consistentes em *documentos informáticos*, sendo essa a consequência da frase «sobre idêntico ou diferente tipo de suporte.»

É de se notar que a cópia que mantenha a forma electrónica – isto é, que seja um *documento electrónico em sentido estrito* – pode por sua vez receber uma assinatura electrónica qualificada (art. 7º, nº 1) e, deste modo, atingir a força probatória plena, verificados que sejam os termos dos nºs 2 e 3 do art. 3º do DL nº 290-D/99.

4.4. Tem particular interesse o artigo 5º do Decreto-Lei nº 290-D/99 (que o DL nº 62/2003 apenas reviu quanto à terminologia da assinatura), que clarifica a viabilidade da emissão de documentos electrónicos pelos serviços e organismos públicos de qualquer natureza, designadamente para a formalização dos respectivos actos administrativos, desde que tais documentos contenham assinaturas electrónicas qualificadas apostas pelos agentes competentes.

Segundo o nº 1 daquele artigo, os organismos públicos podem emitir documentos electrónicos com assinatura digital aposta em conformidade com as normas do Decreto-Lei nº 290-D/99. Esta norma, dado o seu teor genérico, deve entender-se aplicável a todos os documentos originados pelas diversas actividades desses organismos e serviços públicos: quer aqueles que digam respeito à sua actuação especificamente *administrativa*, quer os que relevem das suas relações de natureza *jurídico-privada*.

E o nº 2 do mesmo art. 5º especifica dois aspectos de grande importância, relativamente aos documentos electrónicos dimanados daqueles organismos:

Por um lado, torna inequívoco que os *actos administrativos* daqueles organismos podem ser praticados e formalizados através de meios informáticos, mediante documentos electrónicos, referindo até os tipos de operações - a criação, emissão, arquivo, reprodução, cópia e transmissão (inclusive por meios de telecomunicações) - que podem incidir sobre tais documentos no domínio da actuação administrativa ou privada dos mesmos. Com ressalva, evidentemente, de eventuais requisitos específicos desses actos eventualmente estabelecidos em normas legais, como sejam os que exijam a sua prática presencial, ou elementos formais não reproduzíveis nos documentos electrónicos, etc., casos em que deverá ser emitida lei que adapte esses pressupostos ou requisitos ao ambiente informático.

Por outro lado, estabelece que «os dados relativos ao organismo interessado e à pessoa que tenha praticado cada acto administrativo devem ser indicados de forma a torná-los facilmente identificáveis e a comprovar a função ou cargo desempenhado pela

pessoa signatária de cada documento». Exige, portanto, uma identificação cabal do agente administrativo autor do acto e do título funcional ao abrigo do qual o pratica.

Estas normas devem ser conjugadas com o art. 26º do Decreto-Lei nº 135/99, de 22 de Abril ⁽⁴⁹⁾, que: (a) veio estabelecer o dever de as direcções-gerais, serviços equiparados e institutos públicos disponibilizarem endereços de comércio electrónico para efeito de contactos pelos cidadãos e entidades públicas e privadas e divulgá-lo de forma adequada; e (b) equipara o valor da correspondência transmitida por via electrónica à trocada em suporte de papel, devendo ser-lhe conferido idêntico tratamento pela Administração e pelos particulares, e ressaltando apenas os efeitos que dependem de assinatura ou autenticação dos documentos, até à adopção de um diploma regulador da autenticação dos documentos electrónicos.

Este diploma a que se refere o nº 3 do art. 26º do Decreto-Lei nº 135/99 é, segundo nos parece, o Decreto-Lei nº 290-D/99, cujo art. 5º, conjugado com aquele art. 26º, integra de forma extremamente relevante o disposto nos arts. 122º e 123º do Código de Procedimento Administrativo, deles resultando que:

- a) Os actos administrativos podem ser validamente praticados mediante documentos electrónicos;
- b) Tais documentos electrónicos satisfazem o requisito legal de forma escrita quando contenham um escrito;
- c) Os documentos electrónicos que formalizem esses actos administrativos podem ser criados, emitidos, arquivados, reproduzidos, copiados e transmitidos em forma de documentos electrónicos (em sentido estrito) e inclusive ser transmitidos por meios telemáticos; podem, assim, ser realizadas em forma electrónica todas as funções de documentação, incluindo, p. ex., a passagem de certidões electrónicas de documentos electrónicos, a notificação de actos e documentos electrónicos por correio electrónico, etc.;
- d) A comunicação de actos administrativos – sejam quais forem os fins para que seja efectuada - a outros organismos ou aos administrados deve considerar-se validamente efectuada se o for por meio telemático, em documento electrónico escrito e assinado;
- e) O requisito da assinatura do autor do acto é cabalmente satisfeito mediante a aposição de uma assinatura digital em conformidade com os requisitos do Decreto-Lei nº 290-D/99, devendo dar a conhecer o organismo público, a pessoa do autor do acto e a função ou cargo do agente administrativo signatário do documento.

Por outro lado, o mencionado art. 5º reveste-se de grande importância para esclarecer a questão da viabilidade de revestirem forma de documento electrónico os actos jurídicos para os quais norma legal exija forma de *documento autêntico*, ou seja, que tenham de ser exarados por um agente da entidade ou oficial público revestido de competência legal para esse fim (artigo 369º do C. Civil).

⁽⁴⁹⁾ Que confirma a linha de orientação traçada já no “Livro Verde para a Sociedade da Informação em Portugal”, na “Iniciativa Nacional para o Comércio Electrónico”, aprovada pela Resolução do Conselho de Ministros nº 114/98 (“*Diário da República*”, I Série-B, nº 201, de 1.9.1.1998), e, mais concretamente, na Resolução do Conselho de Ministros nº 60/98 (“*Diário da República*”, I série-B, nº 104, de 6-5-1998)

A conjugação do disposto no art. 3º com o art. 5º do Decreto-Lei nº 290-D/99 viabiliza a emissão de documentos electrónicos *autênticos*, desde que estes sejam exarados por um agente da entidade ou oficial público revestido de competência legal para esse fim e este neles aponha a sua assinatura digital devidamente certificada.

É à luz desta possibilidade que se justifica a exigência da identificação da pessoa e do cargo ou função do agente autor contida no nº 2 deste art. 5º, devida à circunstância de uma parte significativa dos documentos emergentes da prática de actos administrativos revestirem a natureza de *documentos públicos autênticos*, dotados da especial força probatória prevista pelo art. 369º do Cód. Civil ⁽⁵⁰⁾.

5. A certificação da assinatura

5.1. O valor da assinatura digital depende de o seu titular possuir um *certificado* válido, emitido por uma *entidade certificadora* devidamente credenciada por um organismo competente (arts. 2º, al. p), e 8º do citado DL 290-D/99, na versão alterada). Tal organismo é o ITIJ – Instituto das Tecnologias de Informação na Justiça (DL nº 234/2000, de 25.9).

O *certificado digital* – ou simplesmente *certificado* - é um documento electrónico, acessível em ambiente informático a qualquer interessado na sua consulta, que cria a certeza de que a pessoa que apõe uma assinatura digital é a titular da respectiva chave pública e, por conseguinte, também da respectiva chave privada. Trata-se, pois, de um documento dotado de um especial valor probatório, cujos emissão, conteúdo e condições de validade, revogação e suspensão são detalhadamente especificados pelos artigos 28º a 31º da versão actual do DL nº 290-D/99.

Também aqui o DL 62/2003 adoptou uma estranha terminologia, ao distinguir entre *certificado* – que define como o «documento electrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular» - e *certificado qualificado* – que define como «certificado que contém os elementos referidos no artigo 29.º e é emitido por entidade certificadora que reúne os requisitos definidos no artigo 24.º».

Acontece, porém, que todo o novo regime do diploma se refere apenas ao *certificado qualificado*, pelo que o conceito de *certificado* acaba por ter por única utilidade o de servir de base ao de *certificado qualificado*...

5.2. No tocante à emissão do certificado, avulta a preocupação de que seja cuidadosamente verificada pela entidade certificadora a *identidade da pessoa* a favor de quem emitir o certificado, bem como em que seja assegurada a *inalterabilidade dos dados* constantes deste, sendo também enfatizado o dever de fornecimento aos titulares dos certificados das *informações necessárias* para uma utilização correcta e segura do sistema de assinatura digital (art. 28º da actual versão do DL 290-D/99).

Reveste-se de extrema importância a obrigação da entidade certificadora elaborar e manter actualizado e disponível à consulta de qualquer interessado um registo

⁽⁵⁰⁾ Reconheço, no entanto, que, no estado actual do nosso direito notarial, existem obstáculos ao preenchimento pelos documentos electrónicos de todas as formalidades legais exigidas para os *actos notariais*, em especial as relativas ao formalismo dos respectivos livros e à presencialidade da assinatura dos outorgantes e do funcionário (cfr. o art. 363º, 2, Cód. Civil e o arts.7º a 34º e 46º, 1, al. n, do Cód. do Notariado).

ou repositório dos certificados por ela emitidos, suspensos e revogados (nº 5 do art. 28º). É a esse *repositório* que se deverão dirigir todas as pessoas que pretendam verificar a autenticidade de uma assinatura digital constante de um documento electrónico.

A esta luz, bem se compreende a importância da enumeração dos elementos mínimos que os certificados devem conter (artigo 29º), bem como as regras sobre a suspensão e revogação dos certificados, que essencialmente têm a ver com a eventual perda ou suspeita de perda de confidencialidade da chave privada (artigo 30º).

Esta eventualidade constitui o fulcro das *obrigações do titular do certificado* e do respectivo par de chaves, enunciadas no artigo 31º do diploma em apreço: ele deve fundamentalmente tomar todas as medidas necessárias para preservar a confidencialidade da chave privada; se suspeitar da sua perda, pedir de imediato a sua suspensão e, se confirmada tal perda, a sua revogação; e, a partir de alguma destas medidas, respeitar a proibição de utilizar a chave privada para gerar assinaturas digitais.

5.3. O *acesso à actividade de certificação*, concebida como actividade económica de prestação de serviços, comporta o regime jurídico definido nos arts. 9º e seguintes do DL nº 290-D/99. Também nesta matéria o DL nº 62/2003 introduziu várias alterações, que não terei possibilidade de analisar nesta ocasião ⁽⁵¹⁾. Limito-me, assim, a mencionar os pontos mais salientes desse regime:

Em primeiro lugar, é consagrado o *princípio da liberdade de acesso à actividade de certificação*, bem como o *carácter facultativo da respectiva credenciação*, ou seja, da obtenção por qualquer entidade certificadora de um título de exercício da actividade atribuído pela Administração Pública do Estado Português. Logo, qualquer pessoa singular ou colectiva pode exercer em Portugal a actividade de entidade certificadora, com ou sem credenciação (art. 9º, nº 1).

Como já dissemos, a propósito do nº 5 do artigo 3º, o requisito legal da credenciação constitui apenas um pressuposto para que os documentos electrónicos portadores de tal tipo de assinatura gozem do especial valor probatório que as disposições deste Decreto-Lei lhe conferem. E é de notar que são equiparadas às entidadesificadoras credenciadas no País as que forem reconhecidas por qualquer Estado-membro da União Europeia (art. 38º).

No entanto, os documentos portadores de assinaturas digitais baseadas em chaves criptográficas emitidas por entidades não credenciadas não são destituídos de valor probatório, embora de menor grau, pois apenas serão livremente apreciados nos termos gerais de direito (art. 3º, nº 4).

É também livre a *escolha da entidade certificadora*, sendo vedado que seja condicionada a celebração de um dado negócio jurídico à opção pelos serviços de uma dessas entidades determinada (artigo 10º).

A credenciação de uma entidade certificadora não depende de autorização prévia, isto é, de um acto dependente de uma vontade discricionária da Administração Pública Portuguesa, mas sim e somente da reunião de um conjunto de requisitos subjectivos e devidamente documentados (artigos 12º a 16º), os quais, se verificados, darão automaticamente origem ao deferimento da credenciação, que poderá ser tácito se

⁽⁵¹⁾ Para detalhada análise, veja-se o já citado estudo de MIGUEL ALMEIDA ANDRADE, “As insondáveis razões de uma mudança desnecessária...”, *passim*.

não for comunicado no prazo de três meses (artigo 17º) e só poderá ser recusado com fundamento na inobservância de tais requisitos (artigo 18º).

Têm também o mesmo carácter vinculado as hipóteses legais de caducidade (artigo 19º) e de revogação (artigo 20º) da credenciação.

Esta liberdade de acesso não significa, porém, um desinteresse do legislador e da Administração Pública pelo correcto exercício da actividade de certificação, em termos que legitimem a indispensável confiança por parte dos sujeitos jurídicos. Assim, o Decreto-Lei nº 290-D/99 define um regime exigente a respeito do exercício da actividade pelas entidades certificadoras, no qual avulta um conjunto de importantes obrigações que elas deverão observar (arts. 24º a 27º e 32º e seguintes).

Ainda não se acha publicada – aguarda-se para breve - a regulamentação prevista no art. 39º, nº 1, do DL nº 290-D/99, a qual deverá contemplar as normas de carácter técnico e de segurança, definidoras, entre o mais, dos padrões (“*standards*”) técnicos e dos procedimentos administrativos relativos à emissão dos certificados de assinaturas digitais.

A propósito, é oportuno informar que foi publicada em 15.07.2003 uma Decisão da Comissão que dá a conhecer os números de referência das normas técnicas adoptadas em matéria de assinatura electrónica.