Aspectos Legais da Gestão da Digital de documentos de Arquivo Electrónico – aspectos a considerar no âmbito do Inquérito-Crime

Manuel Eduardo Aires Magriço, Magistrado do Ministério Público, DIAP de Lisboa

RESUMO

No âmbito da construção dos SI - Sistemas de Informação adquire cada vez maior relevância e pertinência a *preservação digital*, com carácter de integridade, disponibilidade, autenticidade e confidencialidade a longo termo, sobretudo quando reflectimos sobre os SI de natureza crítica e na preservação da nossa cultura e identidade.

Actualmente, as tecnologias de informação são um dos principais, se não o principal, suporte, para a produção e armazenamento de dados. Informação de diversos tipos é produzida e mantida electronicamente, estando dependente de um sistema intermediário composto pelo *software* e *hardware* que contribuíram para a sua criação. A rápida taxa de **obsolescência tecnológica**, inerente à indústria informática, levanta problemas críticos de preservação de informação, operacionalmente indispensável aos Sistemas de Informação.

O Regime Jurídico Aplicável aos Documentos Electrónicos e Assinatura Digital foi construído com o objectivo principal de *incrementar o comércio electrónico, de forma a criar um ambiente seguro para a autenticação electrónica.*

Contudo, verificamos ainda que todo o regime dos documentos electrónicos e das assinaturas digitais tem como referência o regime do Código Civil, raciocinando no âmbito de uma realidade física, o que desde logo se afigura redutor, designadamente com a utilização das novas tecnologias associadas ao *cloud computing*, à desmaterialização e à virtualização da informação.

Torna-se, por isso necessário, melhorar as estratégias legais actualmente existentes, com o desiderato de assegurar a preservação digital da informação, evitando a obsolescência tecnológica, a qual poderia derivar numa situação de grave conturbação social, sobretudo se provocar a indisponibilidade de Sistemas de Informação de natureza crítica. Torna-se por isso necessário associar um PPD – Plano de Preservação Digital de Segurança da Informação, procurando certificar os SI, na sua globalidade, enquanto fontes fidedignas de produção de informação, indicando-se a título de exemplo *os Serviços do Ministério Público – área crime.*

Palavras-chave: sistema de informação, assinatura electrónica, documento electrónico, preservação digital e segurança da informação

1. INTRODUÇÃO

O Regime Jurídico Aplicável aos Documentos Electrónicos e Assinatura Digital encontra-se plasmado no Decreto-Lei n.º 290-D/99, de 2 Agosto, com as alterações introduzidas pelo Decreto-Lei n.º 165/2004, de 6 de Julho e o Decreto-Lei n.º 116-A/2006, com a última alteração introduzida pelo Decreto-Lei n.º 88/2009, de 9 de Abril[1].

Este diploma foi complementado pelo Decreto-Regulamentar n.º 25/2004, de 15 de Julho[2].

O objectivo principal subjacente à publicação do Regime Jurídico Aplicável aos Documentos Electrónicos e Assinatura Digital é, de acordo com o preâmbulo do referido diploma, o seguinte:

- *incrementar o comércio electrónico, de forma a criar um ambiente seguro para a autenticação electrónica.*

Sobre a problemática da autenticação electrónica refere o Acórdão do Tribunal da Relação de Lisboa, de 21.06.2011 [Des. Graça Araújo] que "*a aposição informática das letras que representam o nome do remetente de um e-mail, **sem qualquer tipo de certificação**, não equivale à assinatura do devedor exigida pela alínea c) do n.º 1 do artigo 46.º do Código de Processo Civil*".[3] [4]

---

[1] Disponível em URL: http://www.gns.gov.pt/NR/rdonlyres/8149D82F-D20B-4C4B-BE82-EA5335E5E3F9/0/DL882009.pdf. Acedido em 14 de Outubro de 2011.

[2] Disponível em URL: http://dre.pt/pdf1sdip/2004/07/165B00/42694278.pdf. Acedido em 14 de Outubro de 2011.

[3] Disponível em URL: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/8e497d46d599c183802578e80054cc79?OpenDocument&Highlight=0,documento,aut%C3%AAntico. Acedido em 14 de Outubro de 2011.

[4] *Transcreve-se por facilidade de exposição o ARTIGO 46.º do Código de Processo Civil*[4]*:*
(Espécies de títulos executivos)
À execução apenas podem servir de base:
a) As sentenças condenatórias;
b) Os documentos exarados ou autenticados por notário que importem constituição ou reconhecimento de qualquer obrigação;
c) Os documentos particulares, assinados pelo devedor, que importem constituição ou reconhecimento de obrigações pecuniárias, cujo montante seja determinado ou determinável nos termos do artigo 805.º, ou de obrigação de entrega de coisas móveis ou de prestação de facto;
d) Os documentos a que, por disposição especial, seja atribuída força executiva.

No caso submetido perante os Tribunais o exequente decidiu exigir o pagamento de uma dívida perante os Tribunais, no montante de 209.468,58€, acrescida de juros de mora vencidos no montante de 1.397,64€. Para tanto, deu à execução o e-mail datado de 11.5.10, *"assinado e enviado pelo Sr. Paulo, na qualidade de administrador da executada, em que esta reconhece dever à exequente a quantia de 209.468,58€, como contrapartida dos serviços que por esta lhe foram prestados"*.

O Tribunal decidiu que o mero envio de uma mensagem de correio electrónico, pretensamente reconhecendo uma dívida em relação a um destinatário, por si só, não é suficiente para se reconhecer uma dívida.

O Tribunal refere como fundamento da sua decisão que a lei não esclarece se os documentos informáticos podem constituir títulos executivos. Efectivamente, no **artigo 46.º do Código de Processo Civil**, não se fala *expressis verbis* em títulos executivos **extrajudiciais virtuais,** nem tais títulos se encontram cobertos pela remissão feita na alínea d) do nº 1 do mesmo diploma legal para disposição especial. Considerando a aludida tipicidade dos títulos executivos, podia então concluir-se que, de *jure condito (de acordo com as condições da lei),* que aqueles documentos não poderiam constituir, pura e simplesmente, base para a execução.

Há, porém, continua o Tribunal, **a possibilidade de os equiparar a documentos escritos**, pelo que se justifica que tenha a noção dos aspectos principais que aproximam e diferenciam os documentos electrónicos dos documentos físicos – em papel.

Efectivamente, raciocina o Tribunal, em virtude das suas condições específicas de reprodução e transmissão técnicas, **uma parte da doutrina tem-se mostrado relutante em equiparar o regime dos documentos particulares tradicionais aos produzidos pelas novas tecnologias**.

A principal diferença, em relação aos comuns documentos escritos, reside no vínculo entre informação (contida e transmitida por signa) e suporte (res): vínculo fraco entre a informação codificada com o sistema binário em suporte técnico, enquanto não imediatamente legível e facilmente manipulável e alterável, inclusivamente pelos sujeitos a quem a mesma é destinada, os quais, por sua vez podem influenciar o seu

conteúdo, modificando-o. Vínculo, pelo contrário, intenso nos documentos em papel, de imediata legibilidade, sobre cujas características se fundam as regras relativas à validade e autenticidade dos documentos manuscritos ou dotados de assinatura autógrafa, das quais derivam os conceitos de documento original e de cópia.[5]

Sob este último perfil, **o complexo *iter* que atesta a conformidade da cópia com o original**, mal se adapta aos documentos electrónicos. **Tendo em atenção o procedimento de formação do documento informático surge evidente a dificuldade em individualizar o documento original e de distingui-lo da cópia** (…). As características de funcionamento dos instrumentos das novas técnicas não permitem distinguir o original da cópia do ponto de vista ontológico, **dada a sua absoluta identidade; nem sempre é possível saber se se trata de documento original, no sentido supra descrito, bem podendo encontrar-se numa memória de um computador de que se perdeu o rasto"**[6] - M. Enza La Torre, *Contributo Alla Teoria Giuridica Del Documento*, Giuffrè, Milano, 2004, página 272.

É preciso levar em conta que aquilo que se lê no visor e se imprime não é o documento electrónico original, mas **sim uma cópia,** ou uma interpretação de um código de um determinado software.

No caso de documentos electrónicos exige-se, como se referiu, uma assinatura segura do devedor.

Não basta justapor um conjunto de letras/palavras que indicam um nome para se satisfazer as exigências de segurança do sistema acima descrito e devidamente explicitadas.

Para existir assinatura (*a fortiori* electrónica - repare-se que a lei, a propósito das sentenças, distingue muito claramente entre assinatura, com o nome completo ou abreviado, e rubrica – artigo 157º do Código de Processo Civil -) , é necessário um

[5] (2004) La Torre, Maria Enza, *Contributo Alla Teoria Giuridica Del Documento, Giuffrè, Milano, pág-272.*

[6] A não ser que recorramos a serviços periciais especializados.

elemento individualizador que não se obtém, na verdade, mediante o simples digitar de um qualquer nome no teclado do computador.

Mesmo nos EUA, cuja lei apenas prevê a assinatura simples, exige-se para esta ser válida "um som, um símbolo ou um procedimento" que possa ter alguma individualidade (Electronic Signatures in Global and National Commerce Act, de 30.06.2000)[7].

Assim, conclui o Tribunal, sem uma assinatura electrónica segura não se crê que o título executivo, como documento típico que é, cumpra cabalmente a sua função.

II. O REGIME JURÍDICO APLICÁVEL AOS DOCUMENTOS ELECTRÓNICOS E ASSINATURA DIGITAL

Para obstar a estas situações, e em linha com esta decisão do Tribunal da Relação de Lisboa, reconhece-se também no **Regime Jurídico Aplicável aos Documentos Electrónicos e Assinatura Digital [**Decreto-Lei n.º 290-D/99, de 2 Agosto] que "a verificação da autenticidade e da integridade dos dados, facultada pelas assinaturas electrónicas em geral, e pela assinatura digital em particular, **não prova necessariamente a identidade do signatário que cria as assinaturas electrónicas**", pelo que é necessário *instituir um sistema de confirmação por entidades certificadoras, às quais incumbe assegurar os elevados níveis* ***de segurança do sistema indispensáveis para a criação da desejada confiança no tocante às assinaturas de documentos electrónicos.***

Deste modo, conforme o artigo 1.º deste diploma, visa-se regular:
- *a validade, eficácia e valor probatório dos documentos electrónicos;*
- *a assinatura electrónica e;*
- *a actividade de certificação das entidades certificadoras estabelecidas em Portugal.*

[7]*Electronic Signatures in Global and National Commerce Act*, de 30.06.2000. Disponível em URL: http://www.fca.gov/download/public%20law%20106-229%20e-sign.pdf. Acedido em 14 de Julho de 2011.

No âmbito do presente estudo apenas iremos abordar as questões legais relacionadas com a *validade, eficácia e valor probatório dos documentos electrónicos assinados electronicamente*, ou seja, aquele tipo de informação que é elaborada mediante o processamento electrónico de dados tendo em vista a demonstração de uma realidade, e as questões relacionadas com a aposição de uma assinatura electrónica qualificada, *no âmbito da legislação supra identificada.*

Neste aspecto tem especial relevância os termos do disposto no artigo 20.º do Decreto-Regulamentar n.º 25/2004, de 15 de Julho, que estabelece que a documentação referente ao funcionamento dos serviços de certificação, incluindo avarias operacionais especiais e a informação respeitante ao registo é mantida em ficheiro electrónico e **conservada pelo período mínimo de 20 anos**, o que por si só, obriga à elaboração de um PPD - Plano de Preservação Digital, com integração de um plano de continuidade de negócio, que assegure que essa informação se encontre disponível, integral e autêntica, face ao decurso do tempo, e tendo em conta o perigo de obsolescência tecnológica (2010, Barbedo et alia, página 14].

A informação objecto de conservação nos termos deste artigo inclui, entre outros, os seguintes dados:

a) Ciclo de vida do par de chaves da entidade certificadora e de todas as chaves de titulares que são geridas pela entidade certificadora;

b) Ciclo de vida dos certificados qualificados;

c) Ciclo de vida de chaves geradas por dispositivos seguros fornecidos;

d) Fornecimento de dispositivos seguros de criação de assinatura;

e) Pedidos relacionados com a revogação de certificados.

2.1. O documento electrónico

Antes de avançarmos no nosso campo de reflexão torna-se necessário, desde logo, identificar o que se entende por documento electrónico.

De acordo com a definição legal (artigo 2.º, n.º 1) entende-se por documento electrónico: *o documento elaborado mediante processamento electrónico de dados.*

Desde logo, verificamos que na definição de documento electrónico se recorre a má técnica legislativa na medida em que a definição contém o definido - "documento".

Para melhor interpretação, e de acordo o princípio da unidade do sistema jurídico, teremos que nos socorrer do artigo 362.º do Código Civil nos termos do qual *"diz-se documento qualquer* ***objecto*** *elaborado pelo homem com o fim de reproduzir ou representar uma pessoa, coisa ou facto".*

Este dispositivo normativo encontra-se inserido no Capítulo II, Subsecção I do Código Civil, relativo à *definição de regras de avaliação de capacidade probatória dos documentos*. A capacidade probatória traduz-se assim na possibilidade de *demonstração da realidade dos factos* – cfr. Artigo 342.º do Código Civil.

No caso do documento electrónico deveremos considerar que o mesmo se traduz numa forma de representação de uma realidade *mediante o processamento electrónico de dados,* que se efectua tipicamente através da intermediação *de hardware* e de *software*, a que se associa determinada capacidade probatória.

De acordo com o regime legal subjacente, verificamos que o *documento electrónico satisfaz a forma escrita quando o seu conteúdo seja susceptível de representação como declaração escrita,* ou seja tipicamente um documento em formato Word.

No que concerne à capacidade probatória dos documentos electrónicos que tenham aposta uma assinatura electrónica qualificada certificada por uma entidade certificadora credenciada, verificamos que o regime legal remete para o regime probatório previsto para os *documentos particulares* – artigo 3.º, n.º 2 do Decreto-Lei n.º 290-D/99, de 2 de Agosto e artigo 376.º do Código Civil.

Verifica-se, deste modo, perante este regime legal enquadrador, que o Estado não tem habilitação legal, em termos genéricos, para produzir documentos electrónicos autênticos, que são aqueles que *são exarados, com as formalidades legais, pelas autoridades públicas nos limites da sua competência ou, dentro do círculo de actividades que lhe é atribuído, pelo notário ou outro oficial público provido de fé*

pública; ***todos os outros documentos são particulares*** – artigo 363.º, n.º 2 do Código Civil.[8]

Assim, por exemplo, caso se trate de um documento em formato Word, e lhe seja aposta uma assinatura electrónica qualificada certificada por uma entidade certificadora credenciada, teremos de distinguir entre **a assinatura** e o **próprio conteúdo do documento** - artigo 376.º do Código Civil e artigo 3.º, n.º 2 do Decreto-Lei n.º 290-D/99, de 2 de Agosto. Assim:

a) Caso a parte contra quem é apresentada o documento, impugnar a autoria da assinatura, incumbe à parte que apresentar o documento a prova da sua veracidade, nos termos do nº. 2 do artigo 374º. do Código Civil;
b) Não sendo impugnada a autoria da letra ou assinatura, o documento "*faz prova plena quanto às declarações atribuídas ao seu autor*", nos termos do disposto no artigo 376º., n.º 1 do Código Civil.
c) Caso a parte contra quem é apresentada o documento alegar a sua falsidade do seu conteúdo (declaração escrita), estatui-se que os "factos *compreendidos na declaração consideram-se provados na medida em que forem contrários aos interesses do declarante; mas neste caso a declaração é indivisível, nos termos prescritos para a prova por confissão"* – artigo 376.º, n.º 2 e 360.º do Código Civil[9].
d) Não sendo alegada a falsidade do conteúdo do documento (declaração escrita), este beneficia de *"prova plena quanto às declarações atribuídas ao seu autor"*, a não ser que existam notas marginais, palavras entrelinhadas, rasuras, emendas ou outros vícios externos, sem a devida ressalva, caso em que cabe ao julgador fixar livremente a medida em que esses vícios excluem

[8] Atente-se no entanto no artigo 26.º, n.º 4 do Código do Registo Predial, nos termos do qual se estabelece que os documentos arquivados em suporte electrónico referidos no número anterior (que fundamentaram o registo) têm a força probatória dos originais, numa equiparação do suporte papel ao suporte electrónico, desde que exista despacho nesse sentido do Senhor Presidente do IRN – Instituto dos Registos e do Notariado I.P. – mais exemplos análogos se podem encontrar em diferentes sistemas da AP – Administração Pública.

[9] Artigo 360.º
(Indivisibilidade da confissão)
Se a declaração confessória, judicial ou extrajudicial, for acompanhada da narração de outros factos ou circunstâncias tendentes a infirmar a eficácia do facto confessado ou a modificar ou extinguir os seus efeitos, a parte que dela quiser aproveitar-se como prova plena tem de aceitar também como verdadeiros os outros factos ou circunstâncias, salvo se provar a sua inexactidão

ou reduzem a força probatória do documento – artigo 376.º, n.º 3 e artigo 366.º do Código Civil.

Quanto aos outros tipos de representação de dados informáticos, que também devem ser considerados "documentos electrónicos", mas que não revistam a forma escrita, ***tipicamente as imagens, vídeos e os ficheiros de áudio***, caso lhes seja aposta uma assinatura electrónica qualificada certificada por uma entidade certificadora, têm o seguinte valor probatório:

a) Caso a parte contra quem são apresentados não impugnar a representação dos factos ou de coisas que representam "*fazem prova plena desses factos*", nos termos do disposto no artigo 368.º do Código Civil.
b) Caso a parte contra quem são apresentados impugnar a representação dos factos ou de coisas que representam, cabe à parte que apresenta os documentos fazer prova de que os mesmos são verdadeiros, nos termos do disposto no artigo 342.º do Código Civil.

De referir, que *a " prova legal plena só pode ser contrariada por meio de prova que mostre não ser verdadeiro o facto que dela for objecto, sem prejuízo de outras restrições especialmente determinadas na lei"*, nos termos do disposto no artigo 347.º do Código Civil.

Verificamos, assim, que ao viajarmos pelo regime jurídico aplicável aos documentos electrónicos e às assinaturas digitais que este tem como referência o regime do Código Civil, raciocinando no âmbito de uma realidade física, designadamente em suporte papel, o que desde logo se afigura redutor, designadamente com a utilização das novas tecnologias associadas aos SIC – Sistemas de Informação e Comunicação, ao *cloud computing*, em que lidamos com dados/códigos informáticos e respectivas formas de representação.

De notar, que a informação electrónica caracteriza-se pela essencialmente pela sua volatilidade e instabilidade, e os bits são a sua forma original, querendo-se significar que o *original do documento*, os bits, não são susceptíveis de ser devidamente interpretados em suporte papel.

Acresce que se alguém colocar em causa a autenticidade de determinados dados é necessário recorrer a perícias informáticas forenses, no sentido de determinar a sua autenticidade ou falsidade, o que não sucede em suporte papel, em que outros são admissíveis genericamente outros meios de prova.

Um DAE – Documento de Arquivo Electrónico é assim uma realidade mais complexa do que um mero documento físico.

De acordo com a letra da lei, e a título de exemplo, verificamos que, perante um documento electrónico que tenha uma parte susceptível de ser interpretada sob a forma de escrita e outra parte susceptível de ser interpretada através de uma imagem, a parte escrita de um documento assinada electronicamente, mediante a *aposição* de assinatura electrónica qualificada certificada por uma entidade certificadora, pode ter um valor probatório diferente da imagem contida nesse documento, o que, em termos práticos, exige o recurso a meios e pessoas especialmente especializadas, no sentido de detectar que parte dos "*dados"* foi alterada.

Finalmente, prevê-se ainda, que o valor probatório dos documentos electrónicos relativamente *aos quais não seja aposta* uma assinatura electrónica qualificada certificada por entidade certificadora credenciada é apreciado nos termos gerais de direito – artigo 3.º, n.º 5 do Decreto-Lei n.º 290-D/99, de 2 de Agosto e artigo 366.º do Código Civil.

Documentos em suporte papel/Código Civil: **Prova documental** é a que resulta de documento; diz-se documento qualquer objecto elaborado pelo homem com o fim de reproduzir ou representar uma pessoa, coisa ou facto – artigo 362.º do Código Civil.	***Documentos electrónico***s: satisfaz o requisito legal de forma escrita quando o seu conteúdo seja susceptível de representação como declaração escrita (eg.: através do MSWord) – artigo 3.º, n.º 1.
Documentos autênticos: - os ***exarados****, com as formalidades legais, pelas autoridades públicas;* *- nos limites da sua competência ou,* *- dentro do círculo de actividades que lhe é atribuído pelo notário ou outro oficial público*	***Documentos autênticos:*** - ***não existem****, nos termos desta legislação,* ***documentos autênticos*** *stricto sensu****;*** - ***Documentos com*** assinatura electrónica qualificada certificada por entidade certificadora credenciada **(equiparados a documentos particulares do Código Civil)**: -Caso a parte contra quem é apresentada o

provido de fé pública, *- Os documentos particulares são havidos por autenticados, quando confirmados pelas partes, perante notário, nos termos prescritos nas leis notariais.* *– artigo 363.º do Código Civil*	documento, impugnar a autoria da assinatura, incumbe à parte que apresentar o documento a prova da sua veracidade, - Não sendo impugnada a autoria da letra ou assinatura, o documento "*faz prova plena quanto às declarações atribuídas ao seu autor*", - Caso a parte contra quem é apresentada o documento alegar a sua falsidade do seu conteúdo (declaração escrita), estatui-se que os "factos *compreendidos na declaração consideram-se provados na medida em que forem contrários aos interesses do declarante; mas neste caso a declaração é indivisível, nos termos prescritos para a prova por confissão"* – artigo 376.º, n.º 2 e 360.º do Código Civil. - Não sendo alegada a falsidade do conteúdo do documento (declaração escrita), este beneficia de *"prova plena quanto às declarações atribuídas ao seu autor"*, a não ser que existam notas marginais, palavras entrelinhadas, rasuras, emendas ou outros vícios externos, sem a devida ressalva, caso em que cabe ao julgador fixar livremente a medida em que esses vícios excluem *- nos outros tipos de documentos electrónicos (ficheiros áudio, imagens, entre outros) quando lhes for aposta uma assinatura electrónica qualificada por uma entidade certificadora credenciada, fazem prova plena dos factos que representam, se a parte contra quem forem apresentados não impugnar a sua exactidão.*
Documentos particulares: *todos os outros – artigo 363.º do Código Civil.*	***Outros documentos electrónicos:*** *apreciados nos termos gerais de direito*

Fig. 1 – quadro comparativo valor probatório suporte papel e suporte electrónico

III. A PRESERVAÇÃO DIGITAL – INQUÉRITO CRIME

3.1. Enquadramento

A preservação digital pode ser definida como o conjunto de actividades ou processos responsáveis por garantir o acesso continuado a longo prazo à informação existente em suportes digitais.

Consiste na capacidade de garantir que a informação digital permanece acessível, com capacidade probatória, de modo a ser interpretada no futuro, recorrendo, por exemplo, a uma plataforma tecnológica diferente da utilizada no momento da sua criação, assegurando a manutenção do conteúdo intelectual, forma, estilo, aparência e funcionalidade dos dados[10].

No âmbito dos SI da Justiça verifica-se que a informação tem sido produzida com carácter de *utilização imediata* sem serem consideradas necessidades sobre a disponibilização desses dados a médio ou longo prazo[11].

Embora existam no mercado bastantes aplicações para a gestão de documentos electrónicos, ao nível a produção, da circulação ou do seu armazenamento, não são previstas capacidades conducentes à preservação da informação em períodos de tempo prolongados, de acordo com o seu valor administrativo, legal, ou outro.

Com o objectivo da *virtualização* da informação no âmbito do inquérito crime, pelas razões já apontadas, a temática a preservação digital constitui-se como requisito a considerar no âmbito da Segurança da Informação, em termos de confidencialidade, integridade, autenticidade e disponibilidade.

A **confidencialidade** traduz-se na implementação de uma política de gestão de perfis de acesso, nos termos da qual só acede à informação de um inquérito crime quem tem legitimidade e necessidade em termos organizacionais e funcionais.

A **integridade** assegura que o conteúdo da informação produzida não foi alterado de forma propositada ou acidental.

[10] Conselho Nacional de Justiça, *Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário Brasileiro* – Moreq-Jus, Versão 1.0., Brasília, Agosto de 2009. Disponível em URL: http://www.cnj.jus.br/images/stories/docs_cnj/resolucao/manualmoreq.pdf. Acedido em: 14 de Outubro de 2011

[11] São públicas a referência ao desaparecimento de despachos proferidos por Magistrados e a necessidade de repetição de julgamentos por ininteligibilidade do áudio gravado relativo à audição de testemunhas, por obsolescência do *software* de gravação.

A **disponibilidade** assegura o acesso à informação produzida sempre que necessário, idealmente através da definição de um PPD – Plano de Preservação Digital, que permita eliminar em tempo útil a informação que já não é necessária às investigações, designadamente pelo decurso do tempo.

A **autenticidade** da informação electrónica produzida permite identificar inequivocamente o responsável pela sua produção, o propósito e em que termos esta foi produzida e o controlo exclusivo por parte do possuidor ou possuidores dessa informação.

Consta-se, assim, que o armazenamento de documentos de arquivo electrónicos requer uma planificação adicional e a definição de estratégias que previnam a sua perda, implementando designadamente:

a) Sistemas de salvaguarda de dados (backup) que se traduzem num método de copiar documentos electrónicos, de valor idêntico aos originais, que previne a sua perda em caso de falhas do sistema. É conveniente que estes sistemas incluam um plano que preveja a execução regular de cópias, a realização de cópias múltiplas em diferentes suportes, o armazenamento disperso das cópias obtidas e a garantia do acesso rotineiro e urgente às cópias;
b) Procedimentos de manutenção para prevenir danos físicos no suporte – os documentos podem necessitar ser copiados para versões mais recentes do mesmo suporte (ou para outros novos suportes) no sentido de prevenir a corrupção dos dados – de notar, que a desactualização do hardware e software pode afectar a capacidade de interpretar os documentos electrónicos.[12]

A DGARQ – Direcção Geral de Arquivos preconiza uma classificação através da definição de critérios para a construção de uma tabela de selecção, no âmbito de um PPD – Plano de Preservação Digital, com o objectivo de enunciar o resultado do processo de avaliação documental e fixar, consoante o tipo de informação identificada, os respectivos prazos de conservação e destino final da informação digital: a *conservação permanente ou a eliminação*.

[12] (2005) NP – Norma Portuguesa 4438, *Informação e documentação, Gestão de Documentos de Arquivo, Parte 2: Recomendações de Aplicação,* IPQ – Instituto Português da Qualidade, Almada, Portugal.

A tabela de selecção permite, assim, determinar os prazos de retenção e acções de eliminação ou de transferência de informação de arquivo electrónico.

3.2. Enquadramento – o caso do Ministério Público em particular - área crime

O MP - Ministério Público no exercício das funções que lhe estão legalmente atribuídas é a entidade responsável pelo exercício da acção penal, dirigindo as investigações criminais com o objectivo de determinar a existência de um crime, para o que conta com a necessária colaboração Órgãos de Polícia Criminal, que actuam na sua dependência funcional, exemplos da PJ – Polícia Judiciária, da GNR – Guarda Nacional Republicana, da PSP – Polícia de Segurança Pública e de outros Órgãos de Polícia Criminal.

Existindo decisão de acusação por parte do MP será o arguido submetido a julgamento, perante um Tribunal.

Perspectivando-se construir um sistema de informação que trate centralmente a documentação e os dados electrónicos relativos às diligências de prova recolhidas no âmbito do inquérito - crime, com o desiderato de implementar o denominado *inquérito electrónico*, torna-se indispensável assegurar que esses dados se mantêm verdadeiros, integrais, inteligíveis e operacionais ao longo do tempo, de modo a conferir confiança e segurança aos operadores judiciários, aos cidadãos em geral e sobretudo aos visados pelas investigações, planeando estratégias de *preservação digital*[13], descritas num PPD.

Neste âmbito é assim necessário abordar a questão da preservação digital no âmbito do *inquérito electrónico,* designadamente o prazo de obsolescência tecnológica, que consiste na perda que o valor de um bem sofre em resultado do progresso técnico ou da evolução - eg.: perda de valor do MS Word 2000 , também conhecido como Word 9 face ao MS Word 2007 - , os prazos de conservação da informação no inquérito - crime, analisar as estratégias de preservação da informação actualmente existentes, propor uma

[13] Conjunto de actividades ou processos responsáveis por garantir o acesso continuado a longo prazo à informação existente em suportes digitais. Consiste na capacidade de garantir que a informação digital permanece acessível, com capacidade probatória, de modo a ser interpretada no futuro, recorrendo, por exemplo, a uma plataforma tecnológica diferente da utilizada no momento da sua criação, assegurando a manutenção do conteúdo intelectual, forma, estilo, aparência e funcionalidade dos dados.

metodologia de preservação, debater a problemática específica da preservação das assinaturas electrónicas, formulando, de seguida, propostas de recomendação.

3.3. Prazos de conservação dos dados dos inquéritos-crime

Os prazos de conservação provisória dos processos criminais em Portugal estão ligados à gravidade dos crimes, variando entre 1 (um) ano e 22,5 (vinte anos e seis meses), ressalvadas situações particulares em que o prazo fica suspenso, por vicissitudes legais determináveis, em fase de Instrução e Julgamento - *cfr. Portaria n.º 1003/99, de 10 de Novembro que regula o arquivo de processos judiciais em suporte papel.*

São dados **de conservação permanente**, ou seja que se não podem eliminar, os dados constantes do registo de processos criminais – Eg.: Tribunal/serviço do MP responsável, número do processo, tipo de infracção criminal, data do registo, data da distribuição, identificação do queixoso e do acusado, das testemunhas e dos objectos apreendidos.

Têm, igualmente, como destino a conservação permanente, 5 (cinco) processos, objecto de selecção anual, por cada Tribunal ou Serviço do Ministério Público, que revistam interesse histórico ou cultural - *o caso do incêndio do Chiado, ocorrido em 25 de Agosto de 1988, que correu termos no DIAP de Lisboa, foi destinado à conservação permanente, por interesse histórico.*

3.4. Obsolescência tecnológica

A rápida taxa de obsolescência tecnológica, inerente à indústria informática, levanta problemas críticos de preservação de informação, operacionalmente indispensável ao Sistema Justiça, e ao MP em particular. O prazo de obsolescência, de acordo com recomendações da DGARQ, no exercido das suas funções de autoridade nacional dos arquivos, estima-se em sete (7) anos (2010, Barbedo et alia, página 14).

Explicitando brevemente alguns conceitos temos que:

- Um Sistema de Informação (SI) é uma estrutura aplicacional especializada;

- o Documento de Arquivo Electrónico (DAE) é a entidade lógica que possui conteúdo, contexto e estrutura de forma a ter um significado específico;

- o Objecto Digital (OD) é a componente física do DAE ou do SI, normalmente equivalente a ficheiros.

Um DAE ou um SI são sempre compostos por, pelo menos, um OD, podendo ser compostos por vários OD (2010, Barbedo).

Por exemplo, um despacho de acusação proferido por um Magistrado do Ministério Público pode ser composto por um ficheiro de texto (MS Word), um ficheiro de imagem (JPEG) e um ficheiro tabular (Excel), estando todos integrados para a representação completa do documento. O mesmo raciocínio se aplica a documentos estruturados, como bases de dados (simples ou de suporte a sistemas de informação complexos) ou ainda documentos multimédia.

Do ponto de vista legal[14] os prazos de conservação previstos para os dados do Inquérito Crime, em suporte papel, são os seguintes:

a) registo de processos criminais - *conservação permanente;*

b) processos criminais - *1 ano salvaguardado o prazo de prescrição do procedimento criminal.*

Os processos criminais, como em muitas das organizações, constituem-se electronicamente como um *dossier virtual* onde se encontram todos os dados relativos à investigação em causa corporizados em DAE – Documentos de Arquivo Electrónico[15].

[14] A Portaria n.º 1003/99, de 10 de Novembro aprovou o *Regulamento de Conservação Arquivística dos Tribunais Judiciais*, em suporte papel, o que demanda desde logo a necessidade de alteração legislativa, que defina os prazos de conservação dos dados digitais do sistema de justiça.

[15] Eg.: denúncia ou participação criminal e toda a informação relativa a diligências efectuadas - autos de busca e apreensão, de interrogatório de arguido, de perícia, fotografias, vídeos, entre outros

No caso de processos criminais que tenham sido objecto de despacho de arquivamento pelo MP verifica-se ser possível a sua reabertura se surgirem novos elementos de prova, conquanto os factos sob investigação não tenham sido atingidos pela *prescrição do procedimento criminal*[16].

No caso de dados de conservação permanente de processos – crimes, cuja tipologia indicaremos adiante, deveria ponderar-se a sua integração no RODA – Repositório de Objectos Digitais Autênticos da DGARQ[17].

A tabela de selecção, parte integrante de um PPD, permite determinar os prazos de retenção e acções de eliminação ou de transferência de informação do arquivo electrónico (2010, Barbedo et alia). Os prazos de conservação provisória dos inquéritos - crime objecto de despacho de arquivamento estão ligados à gravidade dos crimes e são os seguintes:

Pena de Prisão	*Prazo mínimo*	*prazo máximo*
+ 10 anos	15 anos	22,5 anos
+/= 5anos	10 anos	15 anos
+=1ano/-5anos	5 anos	7,5
- 1 ano	2 anos	3 anos

Fig. 2 - Prazos Conservação Provisória

São dados de conservação permanente, ou seja que se não podem eliminar do SI, os dados constantes de registo de processos criminais[18], *a que acrescem 5 (cinco) processos, objecto de selecção anual, por cada Serviço do Ministério Público, que*

[16] Momento a partir do qual já não é possível exercer a acção penal - artigo 279.º do Código de Processo Penal e artigos 118.º a 121.º do Código Penal.
[17] Por paralelismo de situações, os termos do disposto no artigo 7.º da Portaria n.º 1003/99, de 10 de Dezembro, com integração dos processos em papel nos Arquivos Distritais.
[18] O registo dos processos criminais abrange os dados identificativos do respectivo processo, designadamente: comarca/serviço do MP responsável, número do processo, tipo de infracção criminal, data do registo, data da distribuição, identificação do queixoso, do ofendido e ou do participante, identificação do denunciado ou do arguido, magistrado titular, secção/oficiais de justiça de apoio, identificação de testemunhas, tipo de decisão, objectos apreendidos, destino dos objectos, decisão final e data da eliminação.

revistam interesse histórico/cultural. No ano de 2009 foram objecto de despacho de arquivamento no MP, 469.324 inquéritos, pelo que a definição dos dados a eliminar do sistema, com a adequada segurança jurídica, vai influenciar, além do mais, o desempenho, eficiência e rapidez na operação do Sistema de Informação que tratar este tipo de dados.

Distrito Judicial	*Arquivados*	*S. Provisória Processo*[19]
Coimbra	61.080	1.328
Évora	55.855	1.079
Lisboa	158.958	4.169
Porto	137.469	1.672
Total Nacional/2009	413.362	8.248

Fig. 3 – Processos Arquivados e Suspensos Provisoriamente- Fonte: Relatório PGR 2009

Verificamos que findaram nos serviços do MP para conservação, no ano de 2009, 421.610 processos-crime em papel, o que demanda especiais inteligências em termos de preservação digital, tendo em conta os prazos impostos para a conservação da informação e a eficiência do SI em causa. Um dado relevante, constante do relatório da PGR relativo ao ano de 2009, é o de que *46,3% dos processos do Distrito de Lisboa correspondem a processos-crime em que é desconhecido o agente do crime*.[20]

3.5. Estratégias de preservação digital

As estratégias de preservação digital mais comuns são as seguintes:

a) *preservação de tecnologia* – implica a conservação e manutenção de todo o software e hardware necessários à correcta apresentação dos OD;

[19] Tipo de decisão do MP que, na maioria dos casos, demanda prolação de despacho de arquivamento, decorrido determinado período de tempo, desde que o arguido cumpra com as injunções impostas

[20] No caso de inquéritos contra desconhecidos, que demandam trabalho meramente administrativa seria de prever um prazo máximo de conservação em linha de 2 anos após o despacho final. Este tipo de processos, na maioria dos casos, é constituído por 4 tipos de ficheiros em Word: capa do processo (conservação permanente), participação inicial, despacho de arquivamento, notificação e respectivo comprovativo. Apenas 10% destes processos são objecto de reabertura após despacho de arquivamento, normalmente nos dois subsequentes à data do início do processo. Seria assim de ponderar a colocação deste tipo de dados fora de linha (*off-line),* decorrido aquele prazo de 2 anos. Apenas os dados da capa do processo permaneceriam em linha (online) – Fonte: DIAP de Lisboa.

b) *emulação* – corresponde à utilização de um software – o *emulador* – capaz de reproduzir o comportamento de uma plataforma que, à partida, seria incompatível;
c) *Monitorização de suportes e formatos* – prevê processos de verificação automática, manual e semiautomática dos OD;
d) *Encapsulamento* – consiste em preservar, juntamente com o objecto digital, toda a informação necessária e suficiente para permitir o futuro desenvolvimento de conversores, visualizadores ou emuladores (por exemplo, a descrição formal e detalhada do objecto preservado);
e) *Transposição de formatos e suportes (Migração e transferência de suportes)* – refere-se à transferência de documentos contidos num determinado suporte ou formato para outro suporte ou formato mais actualizado. O principal objectivo desta estratégia é evitar a obsolescência tecnológica, mantendo os OD compatíveis com tecnologias actuais, de forma a permitir a sua interpretação sem necessidade de recorrer a técnicas não convencionais (2010, Barbedo et alia].

Apesar de se encontrarem referenciadas algumas desvantagens quanto à *Migração e transferência de suportes*, por questões de segurança, deve-se optar por esta metodologia de preservação digital, por ser a mais aplicada até à data e a única que tem vindo a dar provas da sua eficácia (2010, Barbedo et alia].

3.6. A preservação digital e a assinatura digital

A assinatura digital do ponto de vista de preservação em ambiente electrónico oferece dificuldades acrescidas, pois constitui uma camada suplementar de *software* que tem de ser preservado.

Sucede que a obsolescência tecnológica provoca no âmbito de uma estratégia de preservação digital a periódica migração da informação para formatos actualizados, normalizados e mais estáveis, com a inerente perda de capacidade probatória do objecto da assinatura digital, uma vez que esta *detecta qualquer alteração no nível físico ocorrida no documento assinado*, como sucede nas operações de preservação (8, Barbedo).

Efectivamente, a assinatura digital foi pensada para ser utilizada de forma imediata descurando obviamente a necessidade mediata de conservação de um documento cuja força probatória deve ser preservada por períodos alargados de tempo[21].

O artigo artº 34º al. a) do Decreto Regulamentar n.º 25/2004 de 15 de Julho revela preocupação do legislador sobre este problema apontando como solução a reassinatura do documento*"…nos casos em que estes sejam necessários, na forma assinada, por um período de tempo superior à validade dos algoritmos e parâmetros associados utilizados na geração e verificação da assinatura*".O artigo 35º do mesmo diploma especifica ainda que: *"A nova assinatura referida na alínea a) do artigo anterior deve ser gerada com os algoritmos e parâmetros associados adequados e incluir as assinaturas anteriores, assim como validação cronológica."*

A solução prevista é incompatível do ponto de vista funcional e jurídico, uma vez que os documentos objecto de reassinatura perdem a característica de integridade e autenticidade no mundo jurídico por um lado e, por outro, se não vislumbra que os produtores de dados no sistema de informação que tratar os inquéritos (eg.: Magistrados do Ministério Público), consintam em voltar a assinar documentos em formato electrónico. (8, Barbedo)[22]

Nesse sentido, é necessário que o repositório dos dados das investigações criminais, assegure a *conservação permanente* dos dados associados a todas as assinaturas digitais dos produtores de dados e a todos os dados/documentos produzidos, assim se assegurando a autenticidade da informação armazenada, apesar da caducidade do certificado digital,[23] o que se afigura uma solução de difícil execução e que com implicações em termos de desempenho do Sistema de Informação

Em alternativa, poderão ser observadas como referência as melhores práticas internacionais, designadamente as contidas no *"TRAC - Trustworthy Repositories Audit*

[21] Verifica-se, assim, que no caso de caducidade do prazo de validade de um certificado digital atribuído a um Magistrado não vai ser possível verificar por essa via a autoria do documento, uma vez que esse Magistrado passou a ter atribuído novo certificado digital, com diferente algoritmo de assinatura.
[22] Esta preocupação é especialmente relevante no caso de arguidos em prisão preventiva ou objecto de restrições ao nível dos direitos, liberdades e garantias dos visados pelas investigações.
[23] Os dados das assinaturas digitais estariam associados à meta-informação do DAE e constituir-se-iam como de dados conservação permanente.

& Certification"[24], que consiste numa ferramenta de avaliação para determinar o compromisso das organizações para assumir responsabilidades de preservação a longo prazo, a nível organizacional e técnico e, bem assim, as regras técnicas previstas para a segurança da informação, actualmente contidas nas normas *ISO/IEC 27001:2005*[25].

No âmbito da legislação interna é necessário proceder a alteração legislativa no sentido de prever a atribuição competências a uma entidade ou entidades que certifiquem na qualidade a observância dos referidos requisitos.

A ANS – Autoridade Nacional de Segurança e a DGARQ poderiam exercer essas competências, nas respectivas áreas de atribuição

É ainda necessário prever no PPD, um *plano de continuidade do negócio*, inserido na estratégia de preservação digital, designadamente sistemas de salvaguarda de dados (backup) e procedimentos de manutenção para prevenir danos físicos no suporte.

IV. CONCLUSÕES

É objectivo da Justiça Portuguesa implementar o *processo electrónico*, querendo significar que se pretende que toda a informação inerente às investigações criminais seja tratada em suporte digital, em substituição do *papel*. Constata-se ser obrigatório, atento o prazo de 7 (sete) anos previsto para a obsolescência tecnológica de *software* e *hardware* - podendo configurar-se prazos mais estreitos - que todos os sistemas que incluam informação em suporte digital por período superior a 7 (sete) anos, como é o caso dos processos criminais, tenham associado um PPD, que inclua, além do mais, um plano de *continuidade de negócio.*

[24]Cfr.URL: http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf (TRAC). Acedido em 13 de Janeiro de 2010. O TRAC consiste numa lista de de requisitos desenvolvidos pelo programa OCLC/RLG - "Online Computer Library Center"/"Research Libraries Group" - e o NARRA - "National Archives and Records Administrarion". A lista de requisitos é neste momento gerida pelo CRL - Center for Research Libraries

[25] A observância destes requisitos e respectiva certificação na qualidade, confere ao repositório digital características de fidedignidade, credibilidade e confiança na preservação da informação, assim se ultrapassando as dificuldades inerentes à perda da validade das assinaturas digitais, querendo-se significar que a organização produtora de informação digital, atentas as regras que implementou, é fidedigna na informação que produz – mesmo que as assinaturas digitais dos produtores de informação não sejam já válidas.

A elaboração de um PPD constitui-se como necessidade essencial ao sucesso da transição do papel para o digital, devendo optar-se pela estratégia de *Migração e Transferência de Suportes*, assim se assegurando que os dados digitais se mantêm verdadeiros, integrais, inteligíveis, disponíveis, operacionais e dotados de capacidade probatória a longo termo.

Consta-se, que a assinatura digital foi pensada para ser utilizada de forma imediata descurando obviamente a necessidade mediata de conservação de um documento/dados cuja força probatória deve ser preservada por períodos alargados de tempo, colocando-se assim em causa a validação cronológica dos certificados digitais, com a previsão legal de reassinatura dos documentos electrónicos, em caso de caducidade da validade do certificado digital – cfr. artigo artº 34º al. a) do D. Reg. 25/2004 de 15 de Julho.

Sucede, que a solução prevista é incompatível do ponto de vista funcional e jurídico, nos casos de ser necessário preservar informação por longos períodos de tempo, uma vez que os documentos objecto de reassinatura perdem a característica de integridade e autenticidade no mundo jurídico por um lado e, por outro, se não vislumbra que os produtores de dados no sistema de informação que tratar os inquéritos (eg.: Magistrados do Ministério Público, Advogados, Oficiais de Justiça, Peritos), consintam em voltar a assinar documentos em formato electrónico.

Assim, no que respeita à preservação das assinaturas digitais pode seguir-se como referência os requisitos contidos no *"TRAC - Trustworthy Repositories Audit & Certification" - ferramenta de avaliação que permite determinar o compromisso e capacidade efectiva das organizações para assumirem responsabilidades de preservação a longo prazo* – ***numa perspectiva de certificação global do SI***, como alternativa à utilização de certificados electrónicos individuais, para a autenticação da informação produzida.

Assim, os SI seriam certificados e auditados regularmente, em termos tais que fossem considerados fontes fidedignas produtoras de informação, reservando-se as assinaturas electrónicas para utilização no âmbito imediato do e-comerce, propósito inicial da legislação sobre esta matéria, e como método seguro de autenticação e acesso a um determinado SI, seguindo-se assim as melhores práticas da indústria.

Caso estes aspectos não sejam acautelados no âmbito dos SI da Justiça prevê-se perda definitiva de informação, com a inerente perda de confiança dos utilizadores e destinatários da informação produzida, quanto à validade, credibilidade e autenticidade da informação produzida em suporte digital, com prejuízo sério para os direitos, liberdades e garantias dos visados pelas investigações e para a sociedade em geral.

*

Manuel Eduardo Aires Magriço, Magistrado do Ministério Público, DIAP de Lisboa

Campus de Justiça de Lisboa
Av. D. João II, 1.08.01
1990-097 LISBOA
Tel. +(351) 213182200 +(351) 213188600

e-mail: lisboa.diap@tribunais.org.pt

REFERÊNCIAS BIBLIOGRÁFICAS:

1. Decreto-Lei n.º 290-D/99, de 2 Agosto, com as alterações introduzidas pelo Decreto-Lei n.º 165/2004, de 6 de Julho e o Decreto-Lei n.º 116-A/2006, com a última alteração introduzida pelo Decreto-Lei n.º 88/2009, de 9 de Abril - *Regime Jurídico Aplicável aos Documentos Electrónicos e Assinatura Digital*. Disponível em URL: http://www.gns.gov.pt/NR/rdonlyres/8149D82F-D20B-4C4B-BE82-EA5335E5E3F9/0/DL882009.pdf. Acedido em 14 de Outubro de 2011.

2. Decreto-Regulamentar n.º 25/2004, de 15 de Julho. Disponível em URL: http://dre.pt/pdf1sdip/2004/07/165B00/42694278.pdf. Acedido em 14 de Outubro de 2011.

3. Acórdão do Tribunal da Relação de Lisboa, de 21.06.2011, Processo n.º 10693/10.5YYLSB.L1-1 [Des. Graça Araújo]. Disponível em URL: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/8e497d46d599c183802578e80054cc79?OpenDocument&Highlight=0,documento,aut%C3%AAntico. Acedido em 14 de Outubro de 2011.

4. (2004) M. Enza La Torre**,** *Contributo Alla Teoria Giuridica Del Documento*, Giuffrè, Milano, pág. 272.

5. *Electronic Signatures in Global and National Commerce Act*, de 30.06.2000. Disponível em URL: http://www.fca.gov/download/public%20law%20106-229%20e-sign.pdf. Acedido em 14 de Julho de 2011.

6. (2010) Barbedo, Francisco; Corujo, Luís; Sant´Ana, Arquivos, Direcção Geral de Arquivos, *Recomendações para a Produção de Planos de Preservação Digital*. Disponível em URL: http://dgarq.gov.pt/files/2008/10/PlanoPreservacaoDigital_V2-02.pdf. Acedido em: 14 de Outubro de 2011.

7. (2005) NP – Norma Portuguesa 4438, *Informação e documentação, Gestão de Documentos de Arquivo, Parte 2: Recomendações de Aplicação*, IPQ – Instituto Português da Qualidade, Almada, Portugal

8. Barbedo, Francisco, *A Preservação Digital na AP – O Papel do Órgão de Gestão da Política Arquivística Nacional*. Disponível em URL: http://www.scribd.com/doc/12891965/arquivos-judiciais-epreservacao-digital. Acedido em: 14 de Outubro de 2011.

9. (2007) TRAC – Trustworthy Repositories Audit & Certification. Disponível em URL: http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

10. Conselho Nacional de Justiça, *Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário Brasileiro* – Moreq-Jus, Versão 1.0., Brasília, Agosto de 2009. Disponível em URL: http://www.cnj.jus.br/images/stories/docs_cnj/resolucao/manualmoreq.pdf. Acedido em: 14 de Outubro de 2011.

11. Relatório Procuradoria-Geral da República 2009. Disponível em URL:http://www.pgr.pt/pub/relatorio/2009/Relatorio%202009.pdf. Acedido em: 14 de Julho de 2011.