OS SERVIÇOS DE CERTIFICAÇÃO ELETRÓNICA FACE AO DL 12/2021

Francisco ACP Andrade[1]
https://doi.org/10.21814/uminho.ed.148.13

Resumo: A entrada em vigor do DL 12/2021, visando assegurar a execução na ordem jurídica interna do Regulamento 910/2014 (Regulamento eIDAS), trouxe consigo importantes esclarecimentos relativamente ao regime jurídico da identificação eletrónica, mas também criou confusão sobretudo devido a um precipitada revogação em bloco do anterior DL 290-D/99[2], sem que estivessem assegurados aspectos essenciais do regime jurídico e de segurança relativos à identificação eletrónica, serviços de assinatura eletrónica e de certificação eletrónica em geral. Está em causa a prestação de serviços de confiança pelos prestadores de serviços de certificação eletrónica, bem como os direitos e deveres das partes na relação de certificação eletrónicas e, em última análise, a própria segurança da utilização dos serviços de identificação eletrónica em geral.

Palavras chave: Identificação eletrónica, assinatura eletrónica, certificação eletrónica, serviços de confiança.

---

[1] Membro integrado do JUSGOV – Centro de Investigação em Justiça e Governação, da Escola de Direito da Universidade do Minho; Membro colaborador do Centro Algoritmi, da Escola de Engenharia da Universidade do Minho

[2] Com última alteração pelo DL 88/2009 de 9 de Abril, e entretanto revogado pelo DL 12/2021 de 9 de Fevereiro, aqui referido como ARJDEAE – Antigo Regime Jurídico do Documento Eletrónico e Assinatura Eletrónica

1. Introdução

O Regulamento Europeu 910/2014 é relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno. Este Regulamento revogou a Diretiva 1999/99/CE.

Há uma necessidade de criar confiança nas transações eletrónicas em linha, no mercado interno, atendendo a uma realidade técnica em mutação com a introdução de novos serviços da sociedade da informação potenciadores da confiança dos utilizadores. Por outro lado, sente-se a necessidade de uma harmonização de regimes, eliminando obstáculos à utilização transnacional dos meios de identificação eletrónica.

Está em causa a utilização dos serviços de identificação eletrónica: "processo de utilização dos dados de identificação pessoal em formato eletrónico que representem de modo único uma pessoa singular ou coletiva, ou uma pessoa singular que represente uma pessoa coletiva (art. 3º nº 1 Regulamento 910/2014).

A entrada em vigor do DL 12/2021 que visa assegurar a execução na ordem jurídica interna do Regulamento 910/2014, trouxe consigo aspetos esclarecedores mas também um conjunto de aspetos muito negativos, nomeadamente pela precipitada revogação em bloco do anterior DL 290-D/99.

1.1. Assinatura electrónica e prestadores de serviços de confiança

A mera existência de assinaturas eletrónicas[3] não é suficiente para garantir a autenticidade e integridade dos dados intercambiados, tornando-se necessária a intervenção de entidades terceiras de confiança[4]. É que a identificação do titular e a autenticidade da chave são elementos essenciais

[3] "Assinatura eletrónica: os dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar", art. 3º nr. 10 Reg. 910/2014. Cfr Dumortier, Jos, Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation) (July 1, 2016). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2855484 (consultado em 10 Julho 2023). SSRN: https://ssrn.com/abstract=2855484 or http://dx.doi.org/10.2139/ssrn.2855484 page 18.

[4] Cfr. Jorge Sinde Monteiro, "Assinatura Electrónica e Certificação", "Direito da Sociedade da Informação", Coimbra Editora, 1999, vol. III, pág. 114: "Para prevenir o perigo de que alguém divulgue uma chave pública sob falso nome é necessário que todos os utilizadores se identifiquem perante um ou vários "terceiros de confiança", tarefa que,

do próprio funcionamento, com um nível satisfatório de segurança, do mecanismo da assinatura eletrónica (ou pelo menos da assinatura digital)[5]. Para estabelecer a autenticidade (e a ligação entre os dados e o titular dos mesmos) e o serviço utilizado (por exemplo, assinatura digital), é necessária a intervenção de autoridades terceiras de confiança[6]. Todo o atual sistema de identificação eletrónica assenta na utilização de entidades certificadoras ou "entidades prestadoras de serviços de confiança".

O sistema de assinatura eletrónica[7] está assim assente na existência de "Prestadores de serviços de confiança"[8], entendidos como entidades, pessoas singulares ou coletivas, que "... emite(m) certificados[9] ou presta(m) outros serviços relacionados com assinaturas eletrónicas"[10]. Um certificado de assinatura eletrónica[11] deve ser entendido como "um atestado eletrónico que associa os dados de validação da assinatura eletrónica a uma pessoa

em conjunto com outras, como a própria criação e atribuição de pares de chaves públicas, poderá ser entregue a "prestadores de serviços de certificação"".

[5] "However the utility of an electronic signature as an authenticating tool is limited by the ability of the recipient to ensure the authenticity of the key used to verify the message digest", cfr. Steffen Hindenlang, "No remedy for disappointed trust – the liability regime for Certification Authorities towards third parties outwith the EC Directive in England and Germany compared", Journal of Information, Law and Technology (JILT) 2002 (1) in http://elj.warwick.ac.uk/jilt/02-1/hindenlang.html (visitado 21-2-2003), ponto 2.1.3. Certication Infrastructure

[6] "Traditionally, Public Key Infrastructures (PKI) have been used for this purpose. The core element of a PKI is a so- called certification authority (CA) also referred to as certification service providers ", Christophe Sorge, "The legal classification of identity based signatures" in Computer Law and Security Review, 30 (2014) 126-136

[7] Cfr. Miguel Pupo Correia, "Assinatura electrónica e certificação digital", in « Direito da Sociedade da Informação », Vol. VI, Coimbra Editora, 2006, pág. 314, que refere que "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". Parece-nos no entanto que este Autor terá ido longe de mais na sua apreciação. É que se a validade da assinatura depende efectivamente da existência de uma entidade certificadora, já nos parece que o facto de tal entidade estar ou não credenciada já terá mais que ver com o efectivo valor probatório associado a tal assinatura do que com a sua validade ou invalidade.

[8] "A certification authority is a body, either public or private, that seeks to fill the need for trusted third parties in electronic commerce by issuing electronic certificates, signed electronically, that attest to some fact about the subject of the certificate", cfr. Steffen Hindenlang, op. citada.

[9] A entidade de certificação (CA) "A CA certifies the mapping between a public key and its owner by digitally signing a certificate, i.e. a data structure that contains both the identity and the public key.", Christophe Sorge, "The legal classification of identity-based signatures", in "Computer law & security review" 30 (2014) pág.126.

[10] A doutrina costuma referir a essencialidade do papel desempenhado por terceiros de confiança ou, na terminologia anglo-saxónica, "Trusted Third Parties". Cfr. a propósito do papel destes terceiros de confiança, na doutrina norte-americana, A. Michael Froomkin, "The Essential Role of Trusted Third Parties in Electronic Commerce", 75 Oregon Law Review, 49 (1996).

[11] Cfr. Joel Timóteo Ramos Pereira, "Compêndio Jurídico da Sociedade da Informação", Quid Iuris, 2004, pág. 200 in fine: "Na prática, o certificado de assinatura constitui a versão electrónica do "bilhete de identidade" ou "cartão de pessoa colectiva", devendo conter as informações previstas no art. 29º (nome e outros elementos de identificação, país de certificação, chave pública, número de série, validade) podendo ser apresentado electronicamente como prova de identidade". Cfr. ainda Miguel Pupo Correia, "Assinatura electrónica e certificação digital", citado, pág. 314.

singular e confirma, pelo menos, o seu nome ou pseudónimo;"[12] (Regulamento 910/2014 art. 3º nr. 14). Os certificados de assinatura eletrónica podem ser, ou não, qualificados. (art. 3º nrs. 14 e 15). Os certificados qualificados de assinatura eletrónica são os que satisfazem os requisitos estabelecidos no Anexo I do Regulamento e deverão conter necessariamente:

- a indicação de que o certificado foi emitido como certificado qualificado;
- os dados de identificação do prestador qualificado de serviços de confiança
- o nome ou pseudónimo do signatário
- os dados de validação da assinatura correspondentes aos dados de criação de assinatura
- indicação de início e termo de validade do certificado
- código de identidade do certificado
- assinatura eletrónica ou selo eletrónico do prestador qualificado de serviços de confiança emitente do certificado
- o local em que está disponível (a título gratuito) o certificado
- a localização dos serviços aos quais se pode recorrer para inquirir da validade do certificado

"Prestador de serviços de confiança"[13], de acordo com o mesmo regulamento (art. 3º nr. 19, é a "a pessoa singular ou coletiva que preste um ou

[12] "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", Miguel Pupo Correia, "Assinatura electrónica e certificação digital", citado, pág. 314.

[13] A doutrina anglo-saxónica refere a existência de "Infraestruturas de chaves públicas" ou "PKI Infrastructure", pois que, na verdade, são estas entidades que gerem e divulgam as chaves públicas necessárias à utilização de sistemas de assinatura digital. Mas também em relação ao funcionamento e às competências destas entidades se vão observando críticas, algumas das quais pertinentes. Cfr., a propósito, relativamente à doutrina anglo-saxónica, o artigo de Carl Ellison e Bruce Schneier, "Ten risks of PKI: what you're not being told about Public Key Infrastructure", Computer Security Journal, volume XVI, Number 1, 2000. Estes autores identificam dez riscos principais na utilização de certificados de assinatura digital emitidos por infraestruturas de chaves públicas: "Risk 1: who do we trust, and for what?"; Risk 2: who is using my key?; Risk 3: how secure is the verifying computer?; Risk 4: Which John Robinson is he?; Risk 5: is the CA (certification authority) an authority?; Risk 6: is the user part of the security design? ; Risk 7: Was it one CA or a CA plus a Registration Authority?; Risk 8: How did the CA identify the certificate holder? Risk 9: How secure are the certificate practices? Risk 10: why are we using the CA process anyway?". Em relação à questão da identificação do titular das chaves de assinatura, nomeadamente no que respeita ao Risco 4º identificado por Ellison e Schneier ("Which John Robinson is he?"), não posso deixar de fazer aqui uma

mais do que um serviço de confiança[14] quer como prestador qualificado quer como prestador não qualificado de serviços de confiança".

Os prestadores de serviços de confiança podem ser ou não qualificados (art. 3º nrs. 19 e 20 do Regulamento 910/2014). Prestador de serviços de confiança qualificado é o prestador de serviços que "preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela entidade supervisora". (art. 3º nrº 20 Regulamento 910/2014),

1.2. Funções das entidades certificadoras

A doutrina vem estabelecendo uma distinção fundamental, a respeito destas entidades, no que à assinatura eletrónica respeita, ao separar duas importantes funções das mesmas, a função de criação de códigos e de registo de assinatura ou de ligação dos códigos de assinatura a um determinado titular, por um lado, e a função de identificação da pessoa que se vai tornar titular da mesma assinatura, por outro lado[15]. Podemos assim estabelecer uma distinção entre as duas importantes funções: funções de Identificação[16] e funções de Registo. Claro que as acimas referidas funções[17] poderão, ou não, coexistir numa mesma entidade. Mas a distinção continua a ser operativa em termos

especial referência ao modo de atribuição de nomes e apelidos usual em Portugal e, em alguns países, considerado algo complicado. Na verdade, o facto de cada um de nós, cidadãos portugueses, poder ter dois nomes próprios, acrescidos de dois apelidos maternos e dois apelidos paternos, faz com que o conjunto de nomes que identificam um cidadão em Portugal constitua um conjunto potencialmente único e perfeitamente identificador da pessoa em causa, pelo que o risco enunciado por Ellison e Schneier ("Which John Robinson is he?") estará muitíssimo atenuado em Portugal. Afinal, parece que o complicado sistema de atribuição de nomes em Portugal se encontra perfeitamente adaptado às necessidades da sociedade tecno-digital.

[14] Sobre serviços de confiança cfr. Zaccaria, Schmidt-Kessel, Schulze, Gambino "EU eIDAS Regulation – Article by article commentary", 2020, Beck Hart Nomos, 23-24.

[15] "... if Alice and Bob had no previous dealings, are strangers, then no electronic signature will reliably identify them to each other without assistance of some outside source to provide a link between their identities and their public keys", cfr. Steffen Hindenlang, op. citada, ponto 2.1.3. Certication Infrastructure.

[16] "... l'accertamento dell'identità personale del sottoscrittore, risponde all'esigenza di accertare che effettivamente il soggetto che risulta titolare della chiave ai sensi della certificazione posta in essere dal soggetto certificatore, sia effetivamente quel soggetto. ", cfr. Alessandra Villeco Bettelli, "L'Efficacia delle prove informatiche", Giufré, Milano, 2004 págs. 107/108.. Para este Autora, a instituição da figura do Notário Electrónico ou"Cybernotary" como nova figura profissional na área dos serviços da Sociedade da Informação "funzionerebbe come una garanzia di effettività dei diritti coinvolti e della loro tutela".

[17] Giusella Finocchiaro, "Firma digitale e firme elettroniche – profili privatistici", Giuffré Editore, Milano, 2003, pág. 80, refere as funções de "identificazione (registration service)" e "certificazione (certification service)"

teóricos e pode até determinar aspetos importantes do regime jurídico das atividades de certificação eletrónica.

De todo o modo, poderemos considerar também a possibilidade de a entidade certificadora poder criar ela própria os códigos de assinatura[18], ou antes optar por fornecer ao cliente os meios para este criar, ele próprio, os seus próprios códigos de assinatura. Ou seja, no caso da assinatura digital, o par de chaves pode ser emitido pela entidade certificadora ou ser criado pelo próprio interessado. No entanto, em qualquer dos casos, o certificado de assinatura é necessariamente emitido pela entidade certificadora.

A entidade certificadora deve verificar a identidade[19] do requerente do certificado[20] e, nos casos aplicáveis, os poderes de representação do requerente – não podendo aqui deixar de ser salientada uma atribuição a entidades certificadoras privadas de competências que normalmente competiam às entidades notariais.... Esta cláusula deve ser compreendida no âmbito do processo de "privatização" do notariado e da atribuição de competências "notariais" a outras entidades que não os notários (por exemplo, advogados e até funcionários dos CTT). Claro que esta atribuição de funções é feita a favor de entidades privadas que se presumem idóneas. E, no caso dos prestadores de serviços de confiança, estes estão sujeitos a fiscalização da entidade supervisora (art. 3º nr. 20 do Regulamento 910/2014). A questão poderá, no entanto, revelar-se mais delicada a respeito de entidades certificadoras não considerados como prestadores qualificados.

Prestadores qualificados de serviços de confiança

O Regulamento eIDAS estabeleceu a distinção entre Prestador de Serviços de Confiança e Prestador Qualificado de Serviços de Confiança, com implicações na distinção entre os diferentes modelos de assinatura eletrónica:

[18] "...a central authority is introduced that generates private keys on behalf of the users. This authority is referred to as Private Key Gener- ator (PKG)", Christophe Sorge, ""Softwareagenten – Vertragsschluss, Vertragsstraffe, Reugeld", Universitatsverlag Karlsruhe, 2006, pág. 127.

[19] Cfr. Giusella Finicchiaro, op. citada, pág. 81: "La prima funzione del certificatore è quella di identificare il soggetto che richiede la certificazione, al fine di garantire la corrispondenza fra il titolare del dispositivo di firma e la persona fisica che lo utilizza".

[20] Cfr. Miguel Pupo Correia, "Assinatura electrónica e certificação digital", citado, pág. 315.

assinatura eletrónica (simples)[21], assinatura eletrónica avançada[22] e assinatura eletrónica qualificada[23]. A assinatura eletrónica qualificada implica necessariamente a existência de um certificado qualificado de assinatura eletrónica[24].

O Regulamento 910/2014 veio ainda estabelecer um regime único para os certificados qualificados de assinatura eletrónica, terminando assim com o regime dual que existia em Portugal na vigência do DL 290-D/99[25]. De acordo com o nº 3 do artigo 3º daquele diploma, estabelecia-se uma distinção entre assinatura eletrónica qualificada certificada por entidade certificadora credenciada e assinatura eletrónica qualificada certificada por entidade certificadora não credenciada. Esta era uma distinção desnecessária e motivadora de confusão. Felizmente, o Regulamento 910/2014 veio unificar o conceito de assinatura eletrónica qualificada (pelo menos em Portugal) e a sua equivalência a assinatura manuscrita, bem como deixando claro que só a assinatura eletrónica qualificada confere a um documento eletrónico o valor de documento particular assinado (artigo 25º nº 2 Regulamento eIDAS) !!![26]

No entanto, com a aprovação e entrada em vigot do DL 12/2021 de 9 de Fevereiro, que visa assegurar a execução do Regulamento 910/2014 na ordem jurídica portuguesa, suscita-se um conjunto de questões decorrentes da precipitada e desastrada revogação na íntegra (art. 36 do DL 12/2021) do regime constante do DL 290-D/99 (na redação que resultou do DL 88/2009), sem regular ex-novo as matérias da suspensão e revogação dos certificados qualificados e dos deveres e obrigações dos titulares dos certificados. O que terá consequências em termos de validade de assinaturas e até relativamente a questões de responsabilidade.

---

[21] "Os dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar" (art. 3º nº 10 Regulamento 910/2014;

[22] «Assinatura eletrónica avançada»: uma assinatura eletrónica que obedeça aos requisitos estabelecidos no artigo 26" (artigo 3º nº 11 Regulamento 910/2014)

[23] "Assinatura eletrónica qualificada»: uma assinatura eletrónica avançada criada por um dispositivo qualificado de criação de assinaturas eletrónicas e que se baseie num certificado qualificado de assinatura eletrónica" (artigo 3º nº 12 Regulamento 910/2014)

[24] Um certificado "emitido por um prestador de serviços de confiança" e que satisfaça os requisitos estabelecidos no Anexo I do Regulamento (Regulamento 910/2014, artigo nº 3 nº 15)

[25] Artigo 3º DL 290-D/99, nº 3: "Quando lhe seja aposta uma assinatura electrónica qualificada certificada por uma entidade certificadora credenciada, o documento electrónico com o conteúdo referido no número anterior tem a força probatória de documento particular assinado, nos termos do artigo 376.º do Código Civil".

[26] O que leva Jorge Sinde Monteiro, op. citada, pág. 117, a referir que "Ao longo do diploma ficaram diversos resquícios de um sistema de autorização prévia".

Isto, para além de também terem sido revogadas, sem previsão de nova regulação, as normas relativas aos deveres das entidades certificadoras que constavam do artigo 24º do DL 290-D/99. Estão nomeadamente em causa as normas relativas aos deveres de "proceder à publicação imediata da revogação ou suspensão dos certificados (art. 24º al. p):

- Assegurar que a data e hora da emissão, suspensão e revogação dos certificados possam ser determinadas através de validação cronológica (art. 24º al. q); ;
- Conservar os certificados emitidos, por um período não inferior a 20 anos (art. 24º al. r);
- Capital social mínimo de 200.000 euros (art. 14º);
- Manter contrato de seguro de responsabilidade civil válido (art. 24º al. d);
- Verificar rigorosamente a identidade dos requerentes titulares dos certificados (art. 24º al. i) DL 290-D/99 e art. 24º nº 1 Regulamento eIDAS);
- Verificar rigorosamente os poderes de representação dos representantes de pessoas colectivas (art. 24º al. i) DL 290-D/99;
- Assegurar o funcionamento de um serviço que permita a consulta "de forma célere e segura do registo informático dos certificados emitidos, revogados, suspensos ou caducados" (art. 24º al. o) DL 290-D/99;
- Proceder à publicação imediata da revogação ou suspensão dos certificados (art. 24º al. p) DL 290-D/99;
- Garantir uma absoluta integridade e independência no exercício da actividade de certificação (art. 24º al. b) DL 290-D/99;
- Assegurar todos os necessários requisitos de integridade e independência no exercício da actividade (art. 24º al. b) DL 290-D/99);
- Assegurar a fiabilidade técnica, segurança e eficácia dos sistemas e a eficácia e idoneidade dos recursos humanos (art. 24º als. c), e), f), g), h DL 290-D/99).

Há que ter sempre em atenção que, se a entidade certificadora oferecer aos titulares de certificados serviços de gestão de chaves, a entidade certificadora não deveria armazenar ou copiar dados de criação de assinaturas do titular (art. 24º al. n) ARJDEAE) – ou seja, a entidade certificadora não deveria, ao abrigo do regime ora revogado, armazenar ou copiar a chave privada... Acresce que,

- No exercício da suas competências, a entidade certificadora deveria assegurar ainda o funcionamento de um serviço que garantisse:
- A revogação e suspensão, "de forma imediata e segura", dos certificados (art. 24º al. o) ii) DL 290-D/99;
- A consulta (não só pelo titular, mas sobretudo pelos terceiros) "..de forma célere e segura", do registo informático dos certificados emitidos, revogados, suspenso e caducados "(art. 24º al. o) i) DL 290-D/99;
- A entidade certificadora teria ainda que garantir a possibilidade de determinação da data e hora da emissão, suspensão e revogação dos certificados (art. 24º al. q) DL 290-D/99;
- As entidades certificadoras teriam a obrigação de conservar as informações referentes aos certificados durante um prazo não inferior a 20 anos "... a contar da suspensão ou revogação de cada certificado..." (art. 30º nº 6 DL 290-D/99 e art. 17º nº 6 Dec. Reg. 25/2004 de 15 de Julho, também revogado pelo DL 12/2021.

Há que recordar ainda que, nos termos do DL 290-D/99, o titular de um certificado era responsável pela sua utilização, devendo em consequência tomar todas as medidas necessárias à preservação da confidencialidade dos dados constantes do certificado e a evitar danos a terceiros (art. 31º nº 1 DL 290-D/99), devendo tomar todas as medidas necessárias para preservar a confidencialidade da chave privada[27].

[27] Miguel Pupo Correia"Assinatura electrónica e certificação digital", citado, pág. 315.

O titular de um certificado era responsável pela sua utilização, devendo tomar todas as medidas necessárias à preservação da confidencialidade dos dados constantes do certificado e a evitar danos a terceiros (art. 31º nº 1 ARJDEAE).

Já a iniciativa de suspensão do certificado por parte da própria entidade certificadora (art. 30º nº 1 b) ARJDEAE), se justificava (e continua a justificar) amplamente nos casos enunciados no artigo ora revogado:

- Quando houvesse fundadas razões para crer que o certificado tinha sido emitido com base em informações erróneas ou falsas;
- Quando houvesse fundadas razões para crer que as informações contidas no certificado haviam deixado de ser conformes com a realidade;
- Quando houvesse fundadas razões para crer que a confidencialidade dos dados de criação de assinatura não estava mais assegurada.

Em casos extremos, podia naturalmente a entidade certificadora proceder à revogação do certificado (art. 30º nº 3 RJDEAE):

- Quando após suspensão se confirmasse que o certificado havia sido emitido com base em informações erróneas ou falsas;
- Quando após suspensão se confirmasse que as informações contidas no certificado haviam deixado de ser conformes com a realidade;
- Quando após suspensão se confirmasse que a confidencialidade dos dados de criação de assinatura não estava assegurada;
- Quando a entidade certificadora cessasse as suas actividades sem ter transmitido a sua documentação a outra entidade certificadora;
- Quando por motivo fundamentado e decorrente da lei a entidade certificadora devesse ordenar a revogação do certificado;
- Quando a entidade certificadora tomasse conhecimento do falecimento, interdição ou inabilitação do titular pessoa singular;

- Quando a entidade certificadora tomasse conhecimento da extinção da pessoa colectiva titular do certificado[28];
- A suspensão ou revogação do certificado deveria indicar a data e hora a partir das quais produziriam efeitos (art. 30º nº 6 ARJDEAE) e a suspensão e a revogação eram oponíveis a terceiros a partir da sua inscrição no registo respectivo (art. 30º nº 5 ARJDEAE). Este registo, dos certificados válidos, suspensos e revogados, deveria obviamente, estar disponível e acessível a todos os interessados.

Estas matérias não estão expressamente reguladas no Regulamento eIDAS e foram revogadas pelo DL 12/2021 sem que o legislador tivesse o cuidado de prever normas que pudessem substituir as que foram revogadas.

O quer nos diz o Regulamento eIDAS que possa ser aproveitável para esta situação?

Apenas a disposição do art. 28º nº 4 que estipula que "os certificados qualificados de assinaturas eletrónicas que tenham sido revogados após a ativação inicial perdem validade a partir do momento da revogação, não podendo o seu estatuto ser revertido, em nenhuma circunstância".

É verdade que o art. 28º nº 5 do Reg. eIDAS se refere à possibilidade de os Estados Membros estabelecerem regras sobre a suspensão temporária dos certificados qualificados...

Mas no caso de Portugal, o Estado Membro que tinha regras relativas à suspensão dos certificados.... revogou-as... Intencionalmente ou talvez não....

Também foi revogada a norma (art. 31º DL 290-D/99) que referia os deveres do titular de certificado, nomeadamente "em caso de dúvida quanto à perda de confidencialidade dos dados de criação de assinatura, o titular deve pedir a suspensão do certificado e, se a perda for confirmada, a sua revogação"...

[28] Embora esta norma tivesse que ser considerada como revogada face à entrada em vigor do Regulamento 910/2014, diretamente aplicável em todo o território da União Europeia e que expressamente prevê que signatário de assinatura eletrónica será necessariamente uma pessoa singular, desaparecendo assim os certificados passados a pessoa coletiva que estavam previstos no DL 290-D/99.

Ou seja, o legislador revogou as únicas normas que previam as obrigações do titular dos certificados e as situações de suspensão ou revogação dos certificados (enquanto deveres quer do titular do certificado quer da entidade certificadora)

Também há que assinalar a revogação da norma que estipulava que "a suspensão e revogação do certificado eram oponíveis a terceiros a partir da inscrição no respetivo registo" (art. 30º nº 5 do DL 290-D/99), bem como a norma que estipulava que "A partir da suspensão ou revogação de um certificado..." era proibida a emissão de certificado referente aos mesmos dados de criação de assinatura pela mesma ou outra entidade certificadora...

A entidade certificadora é, obviamente, civilmente responsável pelos danos sofridos pelos titulares dos certificados e por terceiros em consequência do incumprimento dos deveres que lhe incumbem "...excepto se provar que não actuou de forma dolosa ou negligente ". (art. 26º nº 1 ARJDEAE)[29], sendo nulas as convenções de exoneração e limitação de responsabilidade (art. 26º nº 2)[30].

No anterior regime de credenciação (entretanto revogado), as entidades certificadoras tinham ainda que preencher determinados requisitos (art. 12º ARJDEAE):

- estar dotadas de meios financeiros adequados, sendo o capital mínimo obrigatório, para entidades credenciadas pessoas colectivas, de €200.000, integralmente realizado à data da credenciação (art. 2º nº 1 a), art. 14º e 24º ARJDEAE)[31];
- dar garantias de integridade (idoneidade) e independência (arts. 12º nº 1 b), art. 15º e art. 24º ARJDEAE);

[29] Cfr. A.G. Lourenço Martins, J.A. Garcia Marques e Pedro Simões Dias, "Cyberlaw em Portugal – O Direito das Tecnologias da Informação e Comunicação", Edições Centro Atlântico, 2004, op. citada, referem a este propósito, a inclusão, neste ponto, dos "actos praticados pela entidade certificadora com negligência leve, o que no domínio informático deve ser considerado como uma excessiva extensão da imputação objectiva".

[30] Isto, não obstante o art. 29º nº 1 al. h) prever a possibilidade de, no certificado, serem estabelecidas "limitações convencionais da responsabilidade da entidade certificadora, sem prejuízo do disposto no nº 2 do artigo 26º".

[31] Para entidades credenciadas pessoas singulares, o ARJDEAE estipulava uma obrigatoriedade de estas terem e manterem "durante toda a sua actividade, um património, livre de quaisquer ónus, de valor equivalente a € 200.000 (art. 14º nº 3 ARJDEAE).

– dispor de recursos técnicos e humanos que assegurassem padrões mínimos de segurança e eficácia (art. 12º nº 1 c) e art. 39º ARJDEAE);
– manter um seguro de responsabilidade civil (art. 12º nº 1 d) e art. 16º ARJDEAE)[32];

E, claro está, a entidade certificadora era civilmente responsável pelos danos sofridos pelos titulares dos certificados e por terceiros em consequência do incumprimento dos deveres que lhe incumbem "...excepto se provar que não actuou de forma dolosa ou negligente " (art. 26º ARJDEAE).

1.4. Deveres das entidades certificadoras

O DL 290-D/99 apontava ainda um conjunto de deveres que impendiam sobre as entidades certificadoras (art. 24º ARJDEAE):

– Estar dotada dos requisitos patrimoniais do art. 14º ARJDEAE (art. 24º ARJDEAE al. a));
– Capital social mínimo de €200.000, integralmente realizado (sociedades comerciais) ou substrato patrimonial equivalente (art. 14º ARJDEAE);
– Manter contrato de seguro de responsabilidade civil válido (art. 24º al. d) ARJDEAE);
– Verificar rigorosamente a identidade dos requerentes titulares dos certificados (art. 24º al. i) ARJDEAE);
– Verificar rigorosamente os poderes de representação dos representantes de pessoas colectivas (art. 24º al. i) ARJDEAE);
– Assegurar o funcionamento de um serviço que permita a consulta "de forma célere e segura do registo informático dos certificados emitidos, revogados, suspensos ou caducados" (art. 24º al. o) ARJDEAE);

[32] Este seguro devia ser celebrado por prazo certo, nunca inferior a um ano, e renovável e com um capital mínimo anual de €125.000 (Portaria 1370/2000 de 12 de Setembro);

– Proceder à publicação imediata da revogação ou suspensão dos certificados (art. 24º al. p) ARJDEAE);
– Assegurar que a data e hora de emissão, suspensão e revogação dos certificados possam ser (precisamente) "determinados através de validação cronológica" ((art. 24º al. q) ARJDEAE)[33];
– Conservar os certificados que emitir por um período não inferior a 20 anos (art. 24º al. r) ARJDEAE) – pode haver necessidade de comprovar uma assinatura electrónica em qualquer momento, durante esse período, até mesmo em Tribunal ou noutra instância de resolução de conflitos;
– Garantir uma absoluta integridade e independência no exercício da actividade de certificação (art. 24º al. b) ARJDEAE);
– Assegurar todos os necessários requisitos de integridade e independência no exercício da actividade (art. 24º al. b) ARJDEAE);
– Assegurar a fiabilidade técnica, segurança e eficácia dos sistemas e a eficácia e idoneidade dos recursos humanos (art. 24º als. c), e), f), g), h) ARJDEAE).

Havia ainda que ter em atenção que, se a entidade certificadora oferecesse aos titulares de certificados serviços de gestão de chaves, a entidade certificadora não deveria armazenar ou copiar dados de criação de assinaturas do titular (art. 24º al. n) ARJDEAE) – ou seja, a entidade certificadora não devia armazenar ou copiar a chave privada.... Esta devia permanecer sempre sob o controlo exclusivo do titular do certificado!

No exercício da suas competências, a entidade certificadora deveria assegurar ainda o funcionamento de um serviço que garantisse:

– A revogação e suspensão, "de forma imediata e segura", dos certificados (art. 24º al. o) ii) ARJDEAE);
– A consulta (não só pelo titular, mas sobretudo pelos terceiros) "... de forma célere e segura", do registo informático dos certificados emitidos, revogados, suspenso e caducados "(art. 24º al. o) i) ARJDEAE).

[33] Determinação da hora tem que ser precisa. Por outro lado, parece que também deveria ser feita referência à indicação do exacto momento – data e hora – em que caduca cada certificado.

A entidade certificadora tinha que garantir a possibilidade de determinação da data e hora da emissão, suspensão e revogação dos certificados (art. 24º al. q) ARJDEAE).

As entidades certificadoras tinham a obrigação de conservarem as informações referentes aos certificados durante um prazo não inferior a 20 anos "... a contar da suspensão ou revogação de cada certificado..." (art. 30º nº 6 ARJDEAE e art. 17º nº 6 Dec. Reg. 25/2004 de 15 de Julho). Parece que aqui deveria também ter sido feita uma referência à data da caducidade. Pode ser fundamental, em determinado momento em que se coloca a questão de utilização de um determinado certificado entretanto caducado, determinar-se se, na data em que o documento electrónico foi assinado, o certificado estava ou não caducado. É que poderá haver necessidade de fazer prova, já depois do momento da caducidade do certificado, da aposição de uma assinatura electrónica, aposta ainda em período em que o certificado [34](logo, a assinatura) era válido (a).

De todo o modo, a lei estabelecia como dever das entidades certificadoras "... Conservar os certificados que emitir, por período não inferior a 20 anos" (art. 24º al. r) ARJDEAE.)

As entidades certificadoras tinham ainda um dever de prestação de informação à entidade "credenciadora": "As entidades certificadoras fornecem à autoridade credenciadora, de modo pronto e exaustivo, todas as informações que ela lhe solicite para fins de fiscalização da sua actividade..." (art. 32º nº 1 ARJDEAE). O que, à primeira vista, se afigura como perfeitamente natural, já que a entidade credenciadora tinha competências de fiscalização da actividade das entidades certificadoras. Com a entrada em vigor do Regulamento eIDAS, esta deverá ser entendida como referência à "entidade supervisora".

[34] Claro está que, se a assinatura electrónica foi aposta em momento ulterior à data de caducidade do certificado, o documento, para todos os efeitos legais, ter-se-à por não assinado. Mas aqui desempenhará um papel de primordial importância a aposição do selo temporal que poderá, até, garantir a validade da assinatura electrónica aposta, apesar de uma ulterior revogação do certificado. Cfr. Alessandra Villeco Bettelli, op. citada, pág. 111: "...la marca temporale svolge un'altra funzione molto importante: prolunga la"validità" del documento oltre la scadenza del certificato relativo alle chiavi di sottoscrizione, e la mantiene anche nel caso di compromissione della chiave privata, purché la marca stessa sia stata generata prima dell'evento cha ha compromesso la chiave privata".

1.5. Suspensão e revogação de certificados

Existia também a possibilidade de suspensão e revogação do certificado, seja a pedido do próprio titular (art. 30º nº 1 al. a) e nº 3 al. a) ARJDEAE) – por exemplo em caso em que este tem sérias razões para pensar que a segurança dos códigos de assinatura se encontra seriamente comprometida –, quer por iniciativa da própria entidade certificadora.

Em caso de dúvida do titular quanto à perda de confidencialidade dos dados de criação de assinatura, impendia mesmo sobre o titular um dever de pedir a suspensão do certificado e, se a perda fosse confirmada, a sua revogação (art. 31º nº 2 ARJDEAE).

É que o titular de um certificado era entendido como responsável pela sua utilização, devendo tomar todas as medidas necessárias à preservação da confidencialidade dos dados constantes do certificado[35] e a evitar danos a terceiros (art. 31º nº 1 ARJDEAE).

Já a iniciativa de suspensão do certificado por parte da própria entidade certificadora (art. 30º nº 1 b) ARJDEAE), se justificava amplamente nos casos enunciados no artigo:

- Quando houvesse fundadas razões para crer que o certificado foi emitido com base em informações erróneas ou falsas;
- Quando houvesse fundadas razões para crer que as informações contidas no certificado deixaram de ser conformes com a realidade;
- Quando houvesse fundadas razões para crer que a confidencialidade dos dados de criação de assinatura não estava assegurada.

Em casos extremos, podia naturalmente a entidade certificadora proceder à revogação do certificado (art. 30º nº 3 ARJDEAE):

- Quando após suspensão se confirmasse que o certificado fora emitido com base em informações erróneas ou falsas;

[35] "Ele deve tomar todas as medidas necessárias para preservar a confidencialidade da chave privada", Miguel Pupo Correia"Assinatura electrónica e certificação digital", citado, pág.315

– Quando após suspensão se confirmasse que as informações contidas no certificado haviam deixado de ser conformes com a realidade;
– Quando após suspensão se confirmasse que a confidencialidade dos dados de criação de assinatura não estava assegurada;
– Quando a entidade certificadora cessasse as suas actividades sem ter transmitido a sua documentação a outra entidade certificadora;
– Quando por motivo fundamentado e decorrente da lei a entidade certificadora devesse ordenar a revogação do certificado;
– Quando a entidade certificadora tomasse conhecimento do falecimento, interdição ou inabilitação do titular pessoa singular;

A suspensão ou revogação do certificado deveria indicar a data e hora a partir das quais produziriam efeitos (art. 30º nº 6 ARJDEAE) e a suspensão e a revogação seriam oponíveis a terceiros a partir da sua inscrição no registo respectivo (art. 30º nº 5 ARJDEAE). Este registo, dos certificados válidos, suspensos e revogados, deveria, obviamente, estar disponível e acessível a todos os interessados.

Conclusões

A entrada em vigor do DL 12/2021 que visa assegurar a execução na ordem jurídica interna do Regulamento 910/2014, veio introduzir alguns relevantes esclarecimentos mas também algumas escusadas perturbações no regime jurídico da identificação eletrónica e do funcionamento do sistema de certificação eletrónica.

Estão em causa o regime jurídico dos próprios prestadores de serviços de certificação eletrónica, desde aspetos essenciais da sua constituição e dissolução, incluindo a necessidade de capital social reforçado e os particulares deveres dos prestadores de serviços face aos clientes e à emissão dos certificados relativos à prestação de serviços de confiança para as transações eletrónicas. Mas também estão em causa os deveres e direitos dos próprios clientes, utilizadores dos serviços. De particular relevo são as consequências ao nível do

sistema de suspensão e revogação de certificados que, após a revogação em bloco do DL 290-D/99, se encontram numa insuportável situação de incerteza. Há que questionar a revogação em bloco, e a possibilidade de termos que entender que algumas normas se deverão manter em vigor, por uma questão de coerência e segurança do próprio sistemas jurídico relativamente à utilização dos serviços de confiança nas relações digitais.