UNIO - *EU Law Journal*. Vol. 4, No. 2, Julho 2018, pp 103-112.

Identificação eletrónica, assinatura e serviço de confiança

Francisco C.P. Andrade*

SUMÁRIO: A generalização do uso de comunicações eletrónicas em todas as esferas das atividades humanas traz a necessidade de uma nova perspetiva legal. Esta necessidade é particularmente sentida a nível da União Europeia com o objetivo assumido de construir um mercado digital único e fiável. O Regulamento 910/2014 foi estabelecido como o principal quadro jurídico europeu destinado a harmonizar o entendimento de instrumentos como identificação eletrónica, autenticação eletrónica, serviços eletrónicos e também outros serviços de confiança da sociedade de informação, como selos eletrónicos, carimbos, serviços de entrega registrada eletrónica e autenticação de sites. No seu conjunto, o Regulamento 910/2014 visa estabelecer um quadro jurídico comum que permitisse aos cidadãos europeus tirarem pleno partido dos serviços digitais num ambiente técnica e juridicamente seguro.

PALAVRAS-CHAVE: identificação eletrónica – assinatura eletrónica – serviço de confiança eletrónica.

* Professor da Escola de Direito da Universidade do Minho. Diretor do Mestrado em Direito e Informática da Universidade do Minho.

I. Introdução

A generalização progressiva de procedimentos eletrónicos, processamento, comunicação e arquivamento de mensagens trouxe uma urgente necessidade de uma nova abordagem, tanto sob uma perspetiva técnica quanto legal, sobre uma nova série de questões relacionadas com a identificação dos intervenientes numa comunicação eletrónica. A questão da identificação do usuário[1] de um sistema informático é essencial nos processos de comunicação eletrónica, principalmente se considerarmos a comunicação escrita a partir de um terminal numa rede aberta.[2] É preciso saber quem está do outro lado da rede, em um processo comunicacional no qual as partes (geralmente) não estarão frente a frente e não terão a visão uma da outra.[3] É claro que é tecnicamente possível proceder a uma identificação "lógica" do usuário em uma rede – através dos respetivos endereços IP, endereço de correio eletrónico ou nome de domínio.[4] Mas tal processo de identificação não é seguro nem fiável. A mera identificação lógica pode apenas estabelecer uma presunção de correspondência com um determinado equipamento ou com um determinado grupo de usuários.[5] O problema é que o uso de tais endereços pode, muito facilmente, ser abusivamente realizado por outra pessoa que não seja a detentora legítima do direito de uso. E essa questão se torna mais problemática porque, nas transações eletrónicas, os participantes não estão se encontrando frente a frente e se comunicam por meio da linguagem binária.[6] A identificação do autor da mensagem e sua autenticação tornam-se assim um requisito imprescindível para a viabilidade do comércio eletrónico e do governo eletrónico.

O Regulamento 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, refere-se à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e revoga a antiga Diretiva 1999/93/CE.[7] O regulamento procura "reforçar a confiança nas transacções electrónicas no mercado interno criando uma base comum para a realização de interações electrónicas

---

[1] "O destinatário tem muito poucas possibilidades de ter uma certeza sobre a identidade do remetente", cfr. Miguel Pupo Correia, "Assinatura electrónica e certificação digital", *Direito da Sociedade da Informação*, vol. VI (Coimbra: Coimbra Editora, 2006), 277.

[2] As questões relativas à segurança e confidencialidade das mensagens nos ambientes de comércio eletrónico, especialmente quando operando em redes abertas, levaram ao surgimento de protocolos especiais que garantem uma maior confiabilidade das transações comerciais. Exemplos destes são os protocolos securitários SET (*Secure Electronic Transaction*) e SSL (*Secure Sockets Layer*). Cfr. Erica Brandini Barbagalo, *Contratos eletrônicos* (São Paulo: Editora Saraiva, 2001), 46.

[3] "A comunicação eletrônica é direta e imediata, mas torna-se impessoal quando não implica a transmissão da imagem ou voz dos participantes". Cfr. Miguel Pupo Correia, *Assinatura electrónica*…, 277.

[4] Erica Brandini Barbagalo, *Contratos eletrônicos*…, 41.

[5] Erica Brandini Barbagalo, *Contratos eletrônicos*…, 41.

[6] "Проблема идентификации субъекта в сети Интернет возникает в связи с тем, что участники электронной торговли обычно не вступают друг с другом в личный контакт - их"общение" происходит в рамках электронной сети", Филиппов А. П. "Подтверждение подлинности авторства (источника) информации, передаваемой с помощью средств Интернет". Tradução livre: "O problema da identificação da pessoa na Internet surge porque os participantes do comércio eletrónico geralmente não têm contato pessoal - sua comunicação surge dentro da rede eletrónica", cfr. A.P. Filipov, "Confirmation of the authenticity of authorship (source) of the information transmitted through the Internet", *Legal Aspects of the use of the Internet technologies* (Moscovo: Knijni Mir, 2002): 106.

[7] Recorda-se que a antiga diretiva foi transposta para o ordenamento jurídico português pelo DL 62/2003 de 3 de abril. Este DL alterou o DL 290-d /99 anteriormente existente sobre o uso de assinaturas digitais, tornando-o compatível com a Diretiva. Entretanto, o DL 290-D/99 sofreu várias alterações, sendo a última a do DL 88/2009 de 9 de abril.

seguras entre cidadãos, empresas e autoridades públicas" (ponto 2 do Preâmbulo do Regulamento), constituindo assim um pilar importante na construção do mercado único digital europeu.[8]

II. Identificação pessoal

Como referimos supra, a questão da identificação de um usuário[9] de um sistema de informática é crucial em qualquer processo de comunicação eletrónica, principalmente em casos de comunicação escrita oriunda de um terminal em rede aberta.[10] É preciso saber quem está do outro lado da rede, num processo comunicacional em que as partes não estarão frente a frente.[11]

O artigo 3.º n.º 1 do Regulamento 910/2014 apresenta uma definição do que deve ser entendido como "o processo de utilização dos dados de identificação pessoal em formato eletrónico que representam de modo único uma pessoa singular ou coletiva ou uma pessoa singular que represente uma pessoa coletiva". Mas tal definição não impede o fato de haver uma diversidade de meios diferentes de identificação eletrónica e que diferentes meios podem ser usados para construir a confiança do cidadão em relação às comunicações e transações eletrónicas. E certamente é possível identificar alguém através de algo que apenas a pessoa conhece (como é o caso das senhas ou números de identificação pessoal) ou algo que só a pessoa possui (como cartões ATM ou cartões inteligentes) ou ainda através de algo que somente a pessoa é ou que somente a pessoa é capaz de fazer ou, pelo menos, de fazer de maneira única (como o tom da voz ou da impressão digital, a imagem do olho ou a maneira como alguém escreve em um teclado ou com uma caneta).[12]

Entretanto, é preciso reconhecer que o conceito (e meios) de identificação eletrónica é muito mais amplo do que o conceito de assinatura eletrónica. E, entre as diferentes tecnologias disponíveis, apenas duas delas poderão ser consideradas como verdadeiros meios de assinatura: *i*) as assinaturas digitais, que operam através de um complexo sistema de emissão de chaves criptográficas e procedimentos de certificação, usualmente denominado "Infraestrutura de Chaves Públicas", garantindo a identificação através de algo que apenas a pessoa conhece ou possui (código de acesso, chave secreta ou cartão inteligente – *smart card*) e *ii*) uma nova tecnologia construída sobre o uso de tecnologias biométricas, capazes de converter características físicas de seres vivos em dados digitais,[13] com base em características

[8] Como se refere no ponto 4 do preâmbulo do Regulamento, quando é referido que "A comunicação da Comissão, de 26 de agosto de 2010, intitulada 'Agenda Digital para a Europa', apontou a fragmentação do mercado digital, a falta de interoperabilidade e o aumento da cibercriminalidade como os principais obstáculos ao ciclo virtuoso da economia digital. No seu Relatório de 2010 sobre a Cidadania da União, com o título "Eliminar os obstáculos ao exercício dos direitos dos cidadãos da UE", a Comissão sublinhou ainda a necessidade de resolver os principais problemas que impedem os cidadãos da União de colher os benefícios do mercado único digital e dos serviços digitais transfronteiriços".

[9] "O destinatário tem pouca possibilidade de se certificar da identidade do remetente", Miguel Pupo Correia, *Assinatura electrónica e certificação digital*…, 277.

[10] Erica Brandini Barbagalo, *Contratos eletrônicos*…, 46.

[11] "A comunicação telemática é muito directa e imediata, mas torna-se impessoal quando não implica a transmissão de voz e/ou imagem dos participantes", cfr. Miguel Pupo Correia, *Assinatura electrónica e certificação digital*…, 277.

[12] Cfr. Arizona Electronic Signature Infrastructure, *Signature Dynamics Electronic Signatures*, disponível em: http://www.sos.state.az.us/pa/SigDynamicsCP.pdf.

[13] "…[T]echnologies for converting physical characteristics of living things into digital data streams", Sean O'Connor, "Collected, tagged, & archived: the burgeoning use of biometrics in personal identification",

pessoais ou relativas a algo que somente a pessoa é capaz de fazer.[14] Estamos nos referindo às assinaturas dinâmicas baseadas na conversão digital do comportamento biométrico da assinatura escrita.

O fato de termos diferentes métodos de identificação para diferentes comunicações e diferentes propósitos levou o legislador europeu a identificar claramente dois níveis principais de mecanismos de identificação associados aos conceitos de autenticação e assinatura eletrónica. O artigo 3.º, n.º 5 nos dá o significado de autenticação como sendo "o processo eletrónico que permite a identificação eletrónica de uma pessoa singular ou coletiva ou da origem e integridade de um dado em formato eletrónico a confirmar". Um conceito diferente é o da assinatura eletrónica, agora definida como "dados em formato electrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar" (artigo 3.º, n.º 10).[15]

Um bom exemplo de um método de autenticação que não é considerado assinatura eletrónica é o mecanismo de autenticação português designado "Chaves Móveis Digitais".[16] É um método alternativo e voluntário para a autenticação de cidadãos nos portais e *sites* da Internet da administração pública. Este método consiste principalmente na associação de um número de identificação civil (ou número de passaporte para estrangeiros) a um número de celular ou endereço de *e-mail*. É um método de autenticação seguro e que traz consigo uma presunção de autoria: presume-se que os atos associados ao cidadão nos portais ou sites da administração pública foram praticados por ele.

III. Assinatura eletrónica no Regulamento 910/2014

O conceito de assinatura não está definido na legislação portuguesa. Em termos gerais, a assinatura é uma maneira de identificar alguém e de mostrar sua concordância com um fato, um objeto ou conteúdo. A assinatura, portanto, aparece como um símbolo que alguém usa com a intenção real de autenticar um documento escrito.[17] Na doutrina jurídica clássica é um sinal distintivo, próprio do autor da assinatura, pelo qual a pessoa se torna conhecida em relação aos outros. Assim sendo, a admissibilidade de uma assinatura não escrita deve levar em consideração uma análise funcional da assinatura.[18] Isso significa que uma assinatura deve ser um

---

Bender's Immigration Bulletin 1245 (1998): 3; e Francisco Carneiro Pacheco Andrade *Consideração jurídica das assinaturas dinâmicas no ordenamento jurídico português,* Atas do XVI Congresso IberoAmericano de Derecho e Informática, Tomo II (Quito: Ministerio de Justicia, Derechos Humanos y Cultos, 2012), 57.

[14] A maioria das tecnologias biométricas (reconhecimento de impressões digitais, reconhecimento da íris e assim por diante) não alcança, apesar de sua confiabilidade muito alta, a garantia das funções associadas ao conceito de assinatura. Miguel Pupo Correia, na obra citada, afirma que as tecnologias biométricas "não asseguram por si mesmas a função de manifestação da vontade do autor, que só pode ser alcançada por outro processo associado à referida tecnologia".

[15] Com o esclarecimento expresso, do n.º 9 do mesmo artigo, de que signatário significa "a pessoa singular que cria uma assinatura eletrónica". Com isso, esclarece-se que, embora a autenticação possa dizer respeito tanto a pessoas coletivas quanto a pessoas singulares, somente as últimas são capazes de assinar eletronicamente.

[16] Lei 37/2014 de 26 de junho.

[17] "Uma assinatura tradicional deve ser (1) um símbolo; (2) executado ou adotado; (3) por uma parte; (4) com intenção atual; (5) para autenticar; (6) uma escrita", cfr. John P. Fischer, "Computers as agents: a proposed approach to revised U.C.C. article 2", *Indiana Law Journal*, vol. 72, No. 2 (Nova York: Spring 1997): 567.

[18] "Важно обеспечить так называемый"функционально-эквивалентный" подход к бумажной

sinal estritamente pessoal e distintivo que possa certificar, sem margem de dúvida, a vontade da pessoa que assina.[19] Vincent Gautrais[20] a esse respeito nos diz que uma assinatura contém essencialmente duas funções principais: a identificação do signatário e a manifestação de sua vontade.[21]

O legislador europeu manteve o foco num conceito tecnologicamente neutro[22] de assinatura eletrónica,[23] entendendo-o como um método usado pelo signatário para assinar um documento eletrónico de tal forma que permite identificar o autor. Sobre as assinaturas eletrónicas, a doutrina jurídica reconhece a necessidade de uma consideração funcional dos métodos tecnológicos para cumprir as duas funções primordiais de uma assinatura: a identificação da pessoa que assina e a sua manifestação de vontade. Contudo, também é reconhecido que as assinaturas eletrónicas devem obedecer a outras funções principais: uma função de autenticação e verificação da origem de uma mensagem ou documento; uma função de integridade ou a verificação de que a mensagem ou documento não foi alterado após a assinatura; uma função de não-repúdio da mensagem ou documento; e, eventualmente, uma função de confidencialidade. De entre as possíveis tecnologias utilizadas para a assinatura eletrónica, duas serão atualmente consideradas: a assinatura digital, baseada em algo que só o signatário possui (chave secreta ou *smart card*) ou sabe (um código especial) e a assinatura dinâmica, baseada em algo que somente o signatário pode fazer de uma certa maneira.[24]

As assinaturas digitais usam métodos criptográficos. E baseiam-se no facto de o usuário ter duas chaves diferentes, uma chave privada (somente conhecida por ele) e uma chave pública que os terceiros conhecem ou podem conhecer.[25] A chave pública pode ser comunicada diretamente ao terceiro ou por meio de terceiros confiáveis.[26] A

и безбумажной документации", Вершинин А П, "Электронный документ: правовая форма и доказательство в суде". Tradução livre: "É importante garantir a chamada equivalência funcional à documentação em e sem papel", cfr. P.A. Vershinin, *Electronic document: legal validity and proof value in Court* (Gorodiets, Moscow: 2000), 31.

[19] Alain Bensoussan, *Les telecommunications et le droit* (Paris: Memento-Guide Alain Bensoussan, Hermés, 1992), 183.

[20] Vincent Gautrais, "La formation des contrats en ligne", in *Guide juridique du commerçant électronique*, dir. Daniel Poulain *et.al.* (Montreal: Themis, 2003), 143-164.

[21] Vincent Gautrais, *La formation des contrats*…

[22] A neutralidade da tecnologia é expressamente declarada no Considerando 27 do Regulamento: "O presente regulamento deverá ser tecnologicamente neutro. Os efeitos legais que o presente regulamento produz deverão poder ser obtidos por qualquer meio técnico, desde que os requisitos do regulamento sejam cumpridos".

[23] Se o conceito amplo de assinatura eletrónica se refere a qualquer método usado para identificar o signatário, o conceito de assinatura digital é muito mais restrito: ele se refere ao uso de técnicas criptográficas para a transmissão de dados e para a identificação do autor da mensagem e para a verificação de sua integridade.

[24] Assinatura dinâmica é um método derivado da técnica do comportamento biométrico. Essa assinatura biométrica reproduz não apenas a geometria da assinatura de alguém, mas também as características dinâmicas do processo de assinatura manuscrita, como a velocidade, a aceleração, a sequência de riscos, tornando assim todo o conjunto de dados único.

[25] Lorenc Hughet Rotger e Guillermo Alcover Garau, "Seguridad en la transmisión electrónica: validez jurídica", *Encuentros sobre Informática y Derecho 1994-1995* (Pamplona: Aranzadi Editorial, 1995), 131-136.

[26] Lorenc Hughet Rotger e Guillermo Alcover Garau, "*Seguridad en la transmisión*", Colegios Notariales de España – Consejo General del Notariado (Madrid: CNE, 2000), 131-136. Ver também s/a, *Notariado y contratación electrónica*, Colegios Notariales de España – Consejo General del Notariado (Madrid: CNE, 2000).

mensagem é encriptada com a chave privada do emissor e desencriptada com a chave pública, e os terceiros não têm nenhuma possibilidade de reverter as funções de criptografia. Além disso, a assinatura digital é criada através do uso de um algoritmo específico chamado *hash* que permite transformar a mensagem num determinado resultado matemático, em uma sequência única de *bits*[27] Uma vez recebida a mensagem, o destinatário usa a chave pública para a desencriptar e obter a sequência de *bits* gerada pelo "algoritmo *hash*".[28] E, ao enviar a mensagem para o mesmo algoritmo de *hash*, ele pode ter certeza de que a mensagem manteve sua integridade desde que foi assinada. Assim, é possível garantir não apenas que a mensagem foi originada realmente pelo remetente (e não por um qualquer *hacker*), mas também que a mensagem foi recebida exatamente como foi enviada, sem qualquer modificação adicional. As assinaturas digitais podem, assim, cumprir todos os requisitos de uma assinatura verdadeira, oferecendo um nível de segurança que dificulta bastante as falsificações.[29]

A assinatura dinâmica é baseada em tecnologias biométricas e usa as características comportamentais da assinatura manuscrita. Esta assinatura usa um sistema digital e periférico, como caneta digital e tela sensível.[30] Essa assinatura é, portanto, única e identifica a pessoa que assina. A partir do momento em que a assinatura é introduzida no sistema, ela não pode mais ser alterada ou copiada.[31] Mas o sistema não captura apenas a imagem digital da assinatura, também captura as medidas estatísticas relativas ao modo de assinar, significando assim as características comportamentais únicas do signatário no momento preciso da assinatura.[32] Este sofisticado sistema torna-se assim substancialmente seguro.[33] Para ter sucesso num ataque, um *hacker* teria que ter acesso não apenas aos códigos-fonte, mas também ao amplo conjunto de informações sobre o modo de assinar do autor da assinatura, o que seria uma tarefa quase impossível.[34] Além disso, existe ainda outra vantagem relacionada às assinaturas dinâmicas: sempre seria possível para um Tribunal ter acesso ao Sistema de Verificação de Assinatura e, com a assistência de um especialista, apresentar evidências de que a assinatura teria sido (ou não) produzida pelo suposto autor ou se o documento associado à assinatura seria (ou não) o documento utilizado no momento da assinatura ou se terá sido (ou não) sujeito a qualquer modificação adicional. Assim sendo, pode-se dizer que uma assinatura dinâmica terá, pelo menos, o mesmo nível de certeza de uma assinatura *man uscrita.*[35]

Embora os dois métodos de assinatura eletrónica identificados sejam bastante confiáveis e possam potenciar relações jurídicas seguras, é óbvio que nem toda mensagem ou documento requer uma assinatura eletrónica. Assim sendo, os métodos de autenticação eletrónica e os métodos de assinatura eletrónica devem coexistir,

---

[27] Erica Brandini Barbagalo, *Contratos eletrônicos*…, 43-44.

[28] Christophe Sorge, *Softwareagenten – Vertragsschluss, Vertragsstraffe, Reugeld*, (Karlsruhe: Universitätsverlag Karlsruhe, 2006), 15.

[29] Chris Reed, *Computer law* (Londres: Blackstone Press Limited, 1990), 271; e Alain Bensoussan, *L'échange de donnés informatise*…, 33.

[30] Marc Gaudreau, "On the distinction between biometrics and digital signatures", *CIC Enterprise Solutions*, 1999, disponível em http://www.penop.com/enterprise/whitepapers/whitepaper5.asp.

[31] Francisco Andrade, *Consideração jurídica das assinaturas dinâmicas no ordenamento jurídico português*…

[32] Benjamin Wright, "Signing tax returns with a digital pen", *ACM SIGSAC Review – special issues on electronic commerce*, vol. 14, No. 4 (1996):17-20.

[33] Benjamin Wright, *Signing tax returns...*

[34] Benjamin Wright, *Signing tax returns*…

[35] Benjamin Wright, *Signing tax returns*…

garantindo simultaneamente diferentes níveis de segurança e diferentes funções.[36] Mas também no que diz respeito às assinaturas eletrónicas, deve considerar-se níveis diferentes de segurança e confiança, e é por essa razão que o Regulamento estabelece uma distinção entre assinatura eletrónica[37] avançada e assinatura eletrónica qualificada.[38]

A assinatura eletrónica avançada deve atender aos requisitos do artigo 26.º do Regulamento, quais sejam:

- Estar associada de modo único ao signatário;
- Permitir identificar o signatário;
- Ser criada utilizando dados para a criação de assinatura eletrónica que o signatário pode, com um elevado nível de confiança, utilizar sob o seu controlo exclusivo;
- Estar ligada aos dados por ela assinados de tal modo que seja detetável qualquer alteração posterior de dados.

A assinatura eletrónica qualificada é 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 3.º, n.º 12).[39] Assim sendo, são necessários dois requisitos complementares para que a assinatura eletrónica seja considerada qualificada: os requisitos estabelecidos no anexo II do Regulamento para os dispositivos de criação de assinaturas eletrónicas (artigo 29.º) e os requisitos estabelecidos no anexo I do Regulamento para certificados qualificados de assinaturas eletrónicas.

O Regulamento prevê uma abordagem tecnologicamente neutra da utilização de diferentes métodos de assinatura eletrónica, entendida num sentido lato. Permitindo assim tanto o uso de assinaturas digitais como de assinaturas dinâmicas. A assinatura dinâmica é o resultado de um processamento eletrónico de dados usando as mesmas características comportamentais da assinatura manuscrita, permitindo assim identificar inequivocamente o signatário de um documento. A aposição de uma assinatura dinâmica em um documento é um verdadeiro ato de assinatura, um ato pelo qual o autor de um documento se identifica e manifesta concordância com o conteúdo declarativo. Os requisitos da "assinatura eletrónica avançada" (artigo 26.º)[40] não apresentam dificuldades especiais quanto à consideração de assinaturas digitais e dinâmicas.

De qualquer forma, assinaturas eletrónicas avançadas e assinaturas eletrónicas

---

[36] Embora alguns autores questionem se "a noção da assinatura ainda é relevante na relação de confiança da sociedade atual nos processos de informação eletrónica", cfr. Jos Dumortier e Niels Vandezande, *Critical observations on the proposed Regulation for electronic identification and trust services for electronic transactions in the internal Market* (Leuven: Interdisciplinary Center for Law and ICT, 2013).

[37] Assinatura eletrónica avançada – artigo 3º., n.º 11.

[38] Assinatura eletrónica qualificada – artigo 3º., n.º 12.

[39] De acordo com o número 14 do artigo 3.º do Regulamento, um certificado de assinatura eletrónica é um atestado eletrónico que associa os dados de validação da assinatura eletrónica a uma pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo. Além disso, o certificado qualificado de assinatura eletrónica deve ser emitido pelo prestador de serviços de confiança que preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela entidade supervisora (artigo 3.º, n.º 20).

[40] Estar associada de modo único ao signatário; permitir identificar o signatário; ser criada utilizando dados para a criação de uma assinatura eletrónica que o signatário pode, com um elevado nível de confiança, utilizar sob o seu controlo exclusivo; e estar ligada aos dados por ela assinados de tal modo que seja detetável qualquer alteração posterior dos dados.

qualificadas representam dois níveis de segurança diferentes no fornecimento de assinaturas eletrónicas e serviços de certificação eletrónica. E como o órgão de supervisão é muito importante na concessão do status de qualificado, é importante dizer que, em Portugal, o órgão supervisor é o GNS (Gabinete Nacional de Segurança).[41]

Um importante esclarecimento do Regulamento diz respeito à ideia de que a assinatura é de facto uma marca ou sinal pessoal utilizado para identificar a pessoa que assina e para averiguar se está de acordo com o que é assinado. A assinatura deve, portanto, ser um sinal pessoal para uma pessoa singular. Isto é muito claro no artigo 3.º nºs. 9 e 10, onde se afirma que a assinatura eletrónica é "utilizada pelo signatário para assinar", sendo o signatário necessariamente uma pessoa singular (n.º 9 do artigo 3.º). Este é um esclarecimento bastante importante, uma vez que a lei portuguesa[42] anterior ao Regulamento estabelecia a possibilidade de uma pessoa coletiva ser detentora de uma assinatura eletrónica.[43] Agora, com o regulamento, é evidente que os titulares de assinaturas eletrónicas são apenas pessoas singulares.[44]

Mas a principal clarificação do Regulamento diz respeito aos efeitos jurídicos e ao valor de prova das assinaturas eletrónicas. O artigo 25.º do Regulamento é bastante claro quanto a esses aspetos. Em primeiro lugar, afirma que "não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial a uma assinatura eletrónica pelo simples facto de se apresentar em formato eletrónico ou de não cumprir os requisitos exigidos para as assinaturas eletrónicas qualificadas". Isso quer dizer que tanto as assinaturas eletrónicas avançadas quanto as qualificadas são admissíveis como prova no Tribunal e não lhes podem ser negados efeitos legais. Embora, como já mencionámos, diferentes níveis de segurança correspondam a assinaturas eletrónicas avançadas e qualificadas e essa diferença terá consequências jurídicas, o que o legislador europeu expressamente confirma no n.º 2 do artigo 25.º: "a assinatura eletrónica qualificada tem um efeito legal equivalente ao de uma assinatura manuscrita". Embora alguns possam ver essa norma como um acompanhamento dos regimes nacionais anteriores relativos a assinaturas eletrónicas qualificadas, a verdade é que essa norma traz consigo um esclarecimento muito importante, tanto no que diz respeito ao conceito de assinatura eletrónica qualificada quanto a seus efeitos legais. Principalmente, põe termo à distinção estabelecida na legislação portuguesa[45] entre assinaturas eletrónicas qualificadas e assinaturas eletrónicas qualificadas certificadas por entidades certificadoras acreditadas. Agora o conceito de assinatura eletrónica qualificada é igualmente estabelecido em todos os Estados-Membros, e torna-se claro que todas as assinaturas eletrónicas qualificadas têm os mesmos efeitos jurídicos. Além disso, as assinaturas eletrónicas qualificadas "baseadas em certificados qualificados emitidos num Estado-Membro são reconhecidas como

[41] DL 116-A / 2006. A GNS é um serviço central da Administração do Estado, administrativamente autónomo, na dependência do Primeiro-Ministro ou de um membro do Governo designado pelo Primeiro-Ministro.

[42] DL 290-D/99 de acordo com a última revisão do DL 88/2009.

[43] Artigo 7.º, n.º 2 do DL 290-D/99 refere-se expressamente "a titular legal da Corporação da assinatura eletrônica qualificada".

[44] Embora os "certificados qualificados de assinaturas eletrónicas podem incluir características específicas adicionais não obrigatórias" (artigo 28.º, n.º 3 do Regulamento).

[45] Artigo 3.º, n.º 2 do DL 290-D/99: "quando lhe seja aposta uma assinatura digital certificada por uma entidade credenciada e com os requisitos previstos neste diploma, o documento […] tem a força probatória de documento particular assinado…".

assinatura eletrónica qualificada em todos os outros Estados-Membros".[46] O que é muito importante no que diz respeito à interoperabilidade das assinaturas eletrónicas em toda a União e um fator crucial para a construção efetiva de um mercado único digital.

IV. Outros serviços de confiança

O Regulamento 910/2014 não trata apenas da identificação eletrónica e assinaturas eletrónicas: tem um âmbito mais vasto ao mesmo tempo que considera a necessidade de serviços de confiança para transações eletrónicas no mercado interno. E, a fim de reforçar estes serviços confiáveis em todos os Estados-Membros, o Regulamento apresenta um conjunto de serviços bastante relevantes e um quadro jurídico para a prestação de tais serviços no mercado interno. Ao reservar a assinatura eletrónica para pessoas singulares, como já vimos, o Regulamento traz consigo um novo instrumento e bastante relevante para instituições privadas e públicas: o selo eletrónico, ou seja, "os dados em formato eletrónico apensos ou logicamente associados a outros dados em formato eletrónico para garantir a origem e a integridade destes últimos".[47] Este selo eletrónico, similarmente ao que acontece com as assinaturas eletrónicas, também pode ser considerado como um selo eletrónico avançado[48] ou um selo eletrónico qualificado de acordo com o certificado associado ao selo. Servindo de instrumento de particular relevância para a certeza das relações jurídicas – particularmente no caso de contratação eletrónica de pessoas coletivas e de comunicação entre os cidadãos e a administração pública – funcionam como os carimbos eletrónicos.[49] Com vista a fazer uma equivalência funcional ao serviço e instrumento baseado no papel, o legislador europeu introduziu no Regulamento a disponibilidade de serviços de entrega eletrónica registada[50] e até os serviços de autenticação de *sites*, visando assim tornar o ato de navegar na Internet muito mais seguro, pelo menos nos *sites* autenticados associados a certificados qualificados.[51] Todos estes novos instrumentos devem agora ser utilizados, com segurança técnica e jurídica, por operadores privados e públicos, a fim de construir uma rede de serviços fiáveis, permitindo aos cidadãos interações garantidamente seguras e fiáveis no mercado digital europeu.

V. Considerações finais

O Regulamento 910/2014 revogou a Diretiva 1999/93/CE visando estabelecer

[46] Artigo 25.º, n.º 3 do Regulamento.
[47] Artigo 3.º, n.º 25.
[48] Artigos 36.º e 38.º do Regulamento.
[49] Artigo 41.º e 42.º do Regulamento. Quanto aos carimbos, ver também http://www.antwerpen.be/david/website/teksten/Rapporten/Rapport6.pdf (em holandês, visitado em 28 de fevereiro de 2005), nota de rodapé 7: "*Tijdsstempeldiensten kunnen aan de hand van een tijdsstempel de datum en zelfs het uur van een elektronische transactie vaststellen, of de datum of het uur van het bestaan van bepaalde elektronische informatie, zoals een digitale handtekening*". Tradução livre: "O serviço de carimbo permite estabelecer, através do selo, a data e a hora em que uma determinada operação eletrónica ocorreu, ou a data e a hora da existência de uma determinada informação eletrónica, como um dispositivo da assinatura digital. Sendo assim, a data e a hora da formação, transmissão e receção de um documento informatizado tornam-se certas e podem, portanto, ser opostas a terceiros", cfr. Alessandra Villeco Bettelli, *L'Efficacia delle prove informatiche* (Milano: Giuffrè, 2004), 112.
[50] Artigos 43.º e 44.º do Regulamento.
[51] Artigo 45.º do Regulamento.

um quadro jurídico comum, aplicado diretamente em todos os Estados-Membros, relativo às questões de identificação eletrónica, autenticação eletrónica, assinaturas eletrónicas e outros serviços de confiança da sociedade de informação. O Regulamento apresenta esclarecimentos sobre as diferentes formas de identificação das pessoas singulares e coletivas na sociedade em rede, mas também sobre quem pode ser titular de assinaturas eletrónicas. Foi também estabelecido um quadro comum de documentos e assinaturas eletrónicas admissíveis pelo Tribunal, bem como um novo conjunto de instrumentos jurídicos, adaptados às possibilidades tecnológicas atuais, destinado a garantir a segurança e fiabilidade das comunicações e transações eletrónicas. Um aspeto importante do Regulamento é a opção assumida pelo legislador europeu (em conformidade com o espírito do antigo quadro jurídico europeu derivado da agora revogada Diretiva 1999/93/CE) por uma abordagem tecnologicamente neutra. Assim sendo, independentemente do facto de as assinaturas digitais ainda corresponderem a maior parte do atual sistema europeu de certificação eletrónica, é importante notar a possibilidade de diferentes tecnologias e métodos serem considerados, como as assinaturas digitais e as assinaturas dinâmicas. Pode-se dizer também que a neutralidade tecnológica e a equivalência funcional são dois fatores importantes na construção de um mercado digital europeu inovador, confiável e seguro, do qual o Regulamento 910/2014 será, sem dúvida, o instrumento jurídico principal e comum.