

# As Distinções Jurídicas dos Procedimentos de Assinatura<sup>1</sup>

Alexander Roßnagel\*

A lei de assinatura eletrônica distingue três procedimentos de assinaturas. Como conseqüência, aquele que desejar criar, implantar ou utilizar um procedimento de assinatura deverá tomar uma decisão. Isso se aplica também ao legislador que quiser estabelecer as assinaturas eletrônicas para determinada aplicação. Para essa tomada de decisão, devem ser observadas, acima de tudo, além de outros critérios, as distinções jurídicas entre os diferentes procedimentos de assinatura. Essas distinções serão descritas na parte II. Anteriormente, porém, na parte I, são apresentados os três procedimentos de assinatura com regulamentação legal. Finalmente, na parte III, são expostas algumas conclusões sobre as diferenças jurídicas identificadas para a decisão de escolha de um dos procedimentos.

---

<sup>1</sup> O presente texto foi traduzido por Fabiano Menke, tendo sido publicado originariamente na Revista *Multimedia und Recht*, ano V (2002), vol. IV, páginas 215-222. Refere-se basicamente às características fundamentais dos procedimentos de aposição de assinatura eletrônica consoante a lei alemã de assinaturas (Signaturgesetz de 2001) e consoante o respectivo regulamento (Signaturverordnung de 2001). Entre outros motivos, o tema ganha sua importância tendo em vista o reconhecimento, pela reforma do BGB de 2001, no seu §126a, da forma eletrônica: "no caso de a forma escrita legalmente prevista ser substituída pela forma eletrônica, o declarante deverá apor o seu nome na declaração e assinar o documento eletrônico com uma assinatura eletrônica qualificada, de acordo com a lei de assinaturas". Assim, o texto trata das características e efeitos dos procedimentos possíveis para "assinar" no espaço virtual. Para os textos da lei e do decreto, tanto em alemão quanto em inglês, acessar [www.regtp.de](http://www.regtp.de), clicando em elektronische Signatur.

\* O Prof. Dr. Alexander Roßnagel é professor de direito público na Universidade de Kassel, lá ele dirige o Projektgruppe verfassungsverträgliche Technikgestaltung (provet) e é diretor do Instituto Europeu de Direito da Informática de Saarbrücken.

## I. A decisão por um procedimento de assinatura

A lei de assinatura eletrônica prevê tão-somente uma estrutura para procedimentos de assinatura, cujos resultados – assinaturas eletrônicas – deverão obter relevância jurídica. Os procedimentos de assinatura oferecidos no mercado dividem-se em três classes, que são identificadas por uma estrutura jurídica e por conseqüências jurídicas diversas. Assim, oferece-se aos interessados a possibilidade de escolher, de acordo com o emprego específico e com a adequação do risco, entre determinados procedimentos de assinatura classificados em níveis: procedimentos ordinários, procedimento de assinatura qualificado (nível intermediário) e procedimento de assinatura credenciado (nível mais alto). A mesma escolha deve ser feita pelo legislador quando ele cria normas que possibilitem transações jurídicas eletrônicas para determinados campos do direito.

### 1. Três procedimentos de assinatura juridicamente diferenciados

As normas estruturais da lei de assinatura eletrônica devem ser compreendidas como uma oferta ao mercado. Elas não prevêm qualquer procedimento de assinatura específico, mas apenas oferecem uma moldura jurídica a qual o prestador de serviços de certificação poderá voluntariamente se subordinar. Por isso, de acordo com o § 1º, alínea 2 da lei de assinatura, são também permitidos procedimentos de assinatura que não preenchem os requisitos da lei.<sup>2</sup> Para os prestadores de serviços de certificação que quiserem se subordinar à lei existem duas alternativas. Eles podem ser auditados previamente ao início de suas atividades conforme o disposto no § 15º da lei de assinatura. Mas eles também podem, sem auditoria prévia, iniciar os seus trabalhos com a mera notificação à autoridade competente (RegTP), consoante o § 4º da lei de assinatura. Com isso, a lei de assinatura diferencia três procedimentos de assinatura, cujos graus qualitativos são marcados pela variação dos níveis de segurança, de prova e de controle.

- no nível mais alto encontram-se os procedimentos de assinatura “credenciados” de que trata o § 15º da lei de assinatura.<sup>3</sup> Para estes aplicam-se os deveres materiais compreendidos do § 4º ao 14º da lei. O cumprimento

<sup>2</sup> A isso correspondem as exigências da lei de assinatura de 1997. Vide Roßnagel em *Recht der Telekommunikation*, comentários à *Telekommunikationsgesetz* e à *MDStV*, 1999, § 1 *SigG*, Rn. 58 ff.

<sup>3</sup> Ao invés de conferir a esses procedimentos um nome plausível, as frações de coalizão – em que pese as múltiplas exigências – inseriram na recomendação da comissão relativa ao § 15, alínea 1, sentença 4 da lei de assinatura apenas a complicada expressão entre aspas “(assinatura eletrônica qualificada com credenciamento do fornecedor)”. Essa denominação não faz com que as diferenças com relação aos procedimentos qualificados fiquem suficientemente claras, e, na prática, é substituída pela denominação “assinatura credenciada”, em que pese a assinatura não seja credenciada, mas sim os procedimentos do fornecedor.

dessas obrigações deve ser provado, todavia, por meio de uma auditoria prévia. Todos os componentes implementados devem observar as exigências do § 17º da lei de assinatura. Isso também deve ser confirmado na auditoria prévia.<sup>4</sup>

- no nível intermediário encontram-se os procedimentos “qualificados”, conforme o § 4º da lei de assinatura. Eles também têm de observar os deveres compreendidos do § 4º ao 14º da lei.<sup>5</sup> Para este procedimento é suficiente que o prestador de serviços de certificação notifique a RegTP antes de começar a desempenhar as suas atividades. Acerca dos componentes técnicos, só é necessário que aqueles relacionados à criação de assinaturas sejam vistoriados, antes de sua utilização, por um órgão independente.<sup>6</sup>
- no nível mais baixo localizam-se os procedimentos de assinatura ordinários, de acordo com a alínea 2 do § 1º da lei de assinatura. Eles são definidos, no § 1º alíneas 1 e 2 da lei de assinatura como “eletrônicos” ou como “assinatura eletrônica avançada”, mas sua regulamentação legal não vai além disso. Eles não são assinaturas conforme a lei e não são associados a qualquer consequência jurídica específica.

## 2. A necessidade de uma decisão

Até o início do ano de 2002, 15 prestadores de serviços de certificação credenciados e mais um não-credenciado (que, todavia, nesse meio tempo obteve o seu credenciamento), além de vários outros prestadores de serviços de certificação, anunciavam os seus serviços e produtos ao mercado.<sup>7</sup> Nesse mercado de serviços de certificação digital o interessado deve decidir entre as ofertas.

Aquele que quiser adquirir procedimentos de assinatura e estabelecer as condições para a sua utilização deverá considerar na sua decisão de escolha se o procedimento de assinatura eleito lhe oferece a segurança e as consequências jurídicas, bem assim as condições estruturais que são necessárias para a aplicação desejada. Uma decisão equivocada poderá levar a uma impossibilidade de utilização da aplicação para o fim desejado ou resultar em dificuldades de reconhecimento e de aceitação de seu valor jurídico.

---

<sup>4</sup> Vide Roßnagel, NJW 2001, 1721F

<sup>5</sup> Veja as respectivas exigências da diretiva europeia. Quanto a isso, veja em detalhes em Roßnagel, MMR 1999, 264, e também na MMR 2000, 458.

<sup>6</sup> Vide Roßnagel, NJW 2001, 1720F.

<sup>7</sup> Vide os números atuais na homepage da RegTP, no endereço [www.regtp.de](http://www.regtp.de).

Também aqueles que só quiserem utilizar os procedimentos de assinatura deverão atentar para as condições e conseqüências do emprego de seus diversos métodos. Aquele que cria assinaturas deve saber quais as conseqüências jurídicas que elas poderão produzir, durante qual espaço de tempo elas poderão ser verificadas e quais as desvantagens jurídicas a que estará sujeito no caso de má-utilização, ou de uma disputa judicial. Os que recebem e verificam assinaturas eletrônicas, ou aqueles que confiam em assinaturas de terceiros, devem saber qual segurança jurídica os diferentes procedimentos lhes oferecem, em que medida e por qual período estarão dependentes do serviço de terceiros<sup>8</sup> e ainda se poderão ou não confiar nesses serviços.

Partindo do pressuposto de que o legislador queira estabelecer regras para transações eletrônicas, ele terá de decidir qual o procedimento de assinatura para a declaração de vontade específica a ser tratada na previsão legal. Quanto a isso, também deverá considerar quais as condições adicionais e conseqüências jurídicas que a legislação sobre assinaturas eletrônicas dispõe sobre os procedimentos de assinatura.

## II. Diferenças legais

Somente na prática pode-se verificar o nível de segurança dos procedimentos de assinatura.<sup>9</sup> Com relação ao aspecto jurídico - no que tange aos pressupostos e conseqüências da oferta de serviços e produtos concernentes às assinaturas eletrônicas - os procedimentos de assinatura apresentam nítidas distinções, muitas vezes desconhecidas, que podem influenciar as respectivas aplicações.<sup>10</sup> Tais distinções encontram-se predominantemente nos aspectos discriminados nos itens seguintes.<sup>11</sup>

### 1. Prova de segurança organizacional

Os prestadores de serviços de certificação credenciados são auditados, antes de iniciarem seus serviços, por órgãos de validação e de testes bem como pela

<sup>8</sup> Vide, quanto a isso, em detalhes em Ondarza, *Digitale Signaturen und die staatliche Kontrolle von "Fremdleistungen"*.

<sup>9</sup> Bröhl/Tettenborn, no *Das neue Recht der elektronischen Signaturen*, 2001, p. 91, salientam que os procedimentos de assinatura credenciados apresentam um nível de segurança elevado.

<sup>10</sup> Correta é a indicação de Bröhl/Tettenborn (Fn.8), p. 92, que as assinaturas produzidas por procedimentos credenciados e as produzidas por procedimentos apenas qualificados, com relação à forma escrita e a facilitação probatória do § 292a do Código de Processo Civil, apresentam as mesmas conseqüências jurídicas. É incabível, todavia, a afirmação de que os procedimentos de assinatura credenciados só se diferenciariam dos não credenciados pelo selo de qualidade do credenciamento, e que não haveria distinções no plano jurídico. As distinções jurídicas relevantes serão demonstradas a seguir.

<sup>11</sup> Sobre esse ponto com relação a aplicações de e-government, veja também Roßnagel, do mesmo editor, *A assinatura eletrônica na administração pública*, 2002, página 9.

autoridade de regulação (RegTP). A auditoria verifica se as exigências da lei de assinatura são integralmente cumpridas.<sup>12</sup> Em condições normais, e de acordo com o § 11º, item 2, alínea 2 do decreto de assinatura, os prestadores de serviços de certificação credenciados se submetem a uma nova auditoria, no mais tardar, a cada três anos.<sup>13</sup> Como consequência, e conforme o § 15º, item 1, alínea 4 da lei de assinatura, eles têm a faculdade de apresentar a qualquer momento “a prova testada e aprovada da segurança” e podem utilizar o selo de qualidade referido no § 15º, item 1, alínea 3 da lei, a fim de deixar claro no âmbito comercial o nível superior de segurança de suas assinaturas qualificadas.<sup>14</sup>

Os procedimentos de assinatura qualificados devem preencher, basicamente, as mesmas exigências dos procedimentos credenciados. O cumprimento delas, todavia, não é verificado previamente. Em realidade, os prestadores de serviços de certificação precisam apenas notificar a RegTP acerca do início de suas atividades. Ao mesmo tempo, eles devem demonstrar na forma apropriada que preenchem as condições de funcionamento. Eles também estão sob a supervisão da RegTP, que todavia, em consideração ao disposto no art. 10 da diretiva européia, não poderá controlá-los sistematicamente.<sup>15</sup> Na falta de um controle sistemático, não se pode garantir que todos os prestadores de serviços de certificação estejam adequados aos requisitos legais. Os procedimentos de assinatura qualificados gozam apenas de uma segurança organizacional declarada e não de uma segurança organizacional comprovada.

Os procedimentos de assinatura ordinários não estão subordinados a quaisquer exigências legais. Eles não são testados antecipadamente nem de alguma maneira controlados. As partes envolvidas em transações jurídicas eletrônicas que utilizam essas assinaturas não dispõem de indicações totalmente confiáveis sobre as declarações dos prestadores de serviços de certificação e sobre a segurança de seus procedimentos. De qualquer modo, essa confiança pode ser construída por longa experiência com a credibilidade de tais procedimentos ou de medidas acessórias dos prestadores de serviços de certificação.<sup>16</sup>

## **2. Verificação da segurança técnica**

Os procedimentos de assinatura credenciados dispõem também do atestado de segurança. Segundo o § 15º, alínea 7 da lei de assinatura, todos os componentes

---

<sup>12</sup> Acerca do significado da auditoria prévia, veja, por exemplo, Ondarza, (Fn. 7), p. 61 e ss.

<sup>13</sup> Veja Roßnagel, BB 2002, 262.

<sup>14</sup> Veja BT-Drs. 14/4662,27.

<sup>15</sup> Uma supervisão operacional previne até mesmo eventual apresentação insuficiente dos relatórios da RegTP.

<sup>16</sup> Sobre isso, vide Fuhrmann, *Vertrauen im Electronic Commerce*, 2001, p. 40, 61, 238.

técnicos introduzidos nos procedimentos de assinatura devem ser testados previamente. Os testes e as confirmações devem, consoante dispõe o § 11, alínea 3 do decreto de assinatura, observar os requisitos do item primeiro do anexo I do decreto<sup>17</sup> e satisfazer o estado da ciência e da técnica, conforme o § 15º, item 7 da lei de assinatura. A segurança atestada é confirmada pela RegTP, de acordo com o § 16º, item 3, por meio de um certificado específico.<sup>18</sup> A verificação dessa segurança também pode ser reconhecida com a ajuda do certificado também nos procedimentos automatizados.

Para os procedimentos de assinatura qualificados o § 17º, alínea 4 da lei de assinatura exige uma testagem prévia apenas para os equipamentos de criação de assinaturas dos prestadores de serviços de certificação, sem levar em conta o estado da ciência e da técnica. Para o teste dos componentes dos procedimentos de assinatura qualificados vigem, consoante o § 15º, item 5, alínea 2, do decreto, os requisitos da segunda parte do anexo I. Eventualmente, e na falta de indicações sobre o estado da ciência e da técnica do § 17º, alínea quatro, da lei, podem haver variações em casos isolados. Para esses componentes, idealizados para a inserção nos procedimentos qualificados, não são emitidos pela RegTP os certificados para verificação automática de segurança de que trata o § 16º, alínea 3, da lei de assinatura.

Enquanto que no direito alemão relativo a componentes técnicos são exigidos essencialmente os mesmos requisitos materiais no tocante aos procedimentos credenciados e qualificados, pode ocorrer que as normas européias sobre produtos para assinaturas eletrônicas qualificadas requeiram níveis mais baixos de segurança.

Para os procedimentos de assinatura eletrônica qualificados não é exigida qualquer testagem prévia dos componentes de verificação de assinaturas e dos componentes de utilização de assinaturas<sup>19</sup>, nem dos componentes técnicos de serviços de listas de certificados revogados e de serviços de “time-stamping”. Para esses componentes técnicos é suficiente a declaração do fabricante confirmando o cumprimento das exigências legais.<sup>20</sup> De acordo com esse quadro legislativo, não se pode ter a certeza de que foram efetivamente inseridos componentes suficientemente seguros nos procedimentos de assinatura qualificados.

Conforme o § 17º, alínea 2, da lei de assinatura eletrônica, no tocante aos componentes de verificação de assinaturas e de emprego de assinaturas é deixado a cargo do usuário a obrigação de utilização dos componentes lá descritos.

---

<sup>17</sup> Quanto às exigências veja os pormenores de conteúdo em Roßnagel/Pordesch, in: Roßnagel (Fn.1), § 17SigV Rn. 33-94.

<sup>18</sup> Isso se aplica apenas para componentes técnicos previamente testados de procedimentos credenciados – veja BT-Drs. 14/4662, 27.

<sup>19</sup> Vide, relacionado a isso, Bovenschulte/Eifert, DuD 2002, 76.

<sup>20</sup> Relativo ao seu conteúdo, veja o § 15, alínea 5 do decreto de assinatura.

Portanto, os procedimentos de assinatura qualificados proporcionam somente uma segurança técnica declarada, mas não uma segurança técnica comprovada.

Os procedimentos de assinatura ordinários podem empregar qualquer outro componente técnico. Com relação aos componentes seguros de criação de assinaturas e aos componentes de utilização, é permitida a escolha do titular da chave de assinatura, mas isso já não se mostra possível quanto aos componentes utilizados pelo prestador de serviços de certificação. Os receptores da assinatura eletrônica e terceiros também não têm influência sobre a segurança do procedimento de assinatura no qual eles devem confiar nem têm possibilidades de avaliar essa segurança.

### 3. A estrutura de certificação

Segundo dispõe o § 16º, alínea 1, da lei de assinatura, somente os prestadores de serviços de certificação credenciados recebem da autoridade competente um certificado raiz, o que assegura a confiabilidade da cadeia de certificados. Com isso, de um lado é fixado o caminho de certificação ligando à RegTP – instância certificadora raiz e âncora de confiança. De outro lado, todos os certificados dos prestadores de serviços de certificação credenciados encontram-se na mesma estrutura de certificados e em vista disso podem ser facilmente verificados também pelos programas de verificação de outros prestadores de serviços de certificação.

Diferentemente, o caminho de certificação não é determinado no caso dos procedimentos de assinatura ordinários e dos procedimentos de assinatura qualificados. Quanto a eles, a RegTP não pode assumir a função de autoridade de certificação raiz.

Os prestadores de serviços de certificação também são livres para criarem suas próprias infra-estruturas de certificação, mas não dispõem de estrutura de certificação em comum com outros prestadores de serviços de certificação. Para esses, pode existir apenas um certificado auto-assinado<sup>21</sup>, e, portanto, nenhuma âncora de confiança independente. Com base em certificados auto-assinados, não se pode, todavia, verificar confiavelmente se os certificados foram efetivamente emitidos pelo prestador de serviços de certificação identificado<sup>22</sup>, quando esse certificado não for conhecido do terceiro que nele deva confiar ou não seja confirmado por uma terceira autoridade.

---

<sup>21</sup> Quanto a esse assunto, veja Brandner/Pordesch/Roßnagel/Schachermayer, DuD 2002, 107.

<sup>22</sup> Com isso também é possível a simulação de uma identidade eletrônica por meio da criação de um cadeia de certificados incluindo o certificado autoassinado do prestador de serviços de certificação.

Essas confirmações, que possibilitam principalmente a interoperabilidade, podem ocorrer com a certificação cruzada de outros prestadores de serviços de certificação.<sup>23</sup> Pelo fato de carecerem de um certificado raiz em comum, os prestadores de serviços de certificação não credenciados devem providenciar o reconhecimento mútuo de seus certificados. Ao invés de buscar um único certificado raiz, cada prestador de serviços de certificação deverá pesquisar os certificados cruzados de todos os outros.<sup>24</sup> Como decorrência, a estrutura de certificação é de precária visibilidade para os que recebem documentos assinados eletronicamente.<sup>25</sup>

#### 4. Substituição da forma escrita

Os procedimentos de assinatura credenciados preenchem os requisitos do § 126a do Código Civil e do § 3a do VwVfG-E, relativos, respectivamente, à forma eletrônica no direito privado e no direito administrativo. Tendo em vista que o cumprimento dessas exigências foi previamente verificado no processo de credenciamento, os titulares de chaves de assinatura, os que confiam nas assinaturas e os terceiros podem ficar seguros que a assinatura eletrônica é conforme a lei, e, portanto, tem eficácia jurídica.

As assinaturas eletrônicas qualificadas também preenchem os requisitos do § 126a do Código Civil e do § 3a do VwVfG-E. Todavia, em face da ausência de auditoria prévia dos procedimentos, pode-se considerar insegura a adequação aos requisitos legais – até que se faça uma verificação detalhada pela RegTP ou se proceda a um esclarecimento judicial. Se eventualmente, após alguns anos, venha a ser colocado em evidência que um pressuposto de uma assinatura qualificada não foi cumprido, haverá de se considerar não adequadas à lei todas as assinaturas criadas com esse procedimento. Assim, serão inválidas todas as declarações de vontade que dependerem de forma prescrita. Não é somente o titular de chave de assinatura que corre esse risco, ou seja, não é somente aquele que poderia precariamente valorar e escolher os serviços de certificação qualificados. Aqueles que recebem as assinaturas eletrônicas e terceiros que acreditam que se tratam de manifestações de vontade com validade jurídica também passam a sofrer essa ameaça.

Quanto aos procedimentos ordinários, não se podem dispor quaisquer formas de regulação por meio de lei em face da carência de informações sobre a sua

---

<sup>23</sup> Quanto a isso, veja Hammer, DuD 2001, 65.

<sup>24</sup> Isso eventualmente pode ser facilitado por meio de distintos modelos de certificação “bridge”. Quanto a isso, veja, por exemplo, Esslinger/Barcklow/Bartosch, DuD 2001, 519; Fell, DuD 2001, 536; Reif, DuD 2001, 553. Para todos os modelos de certificação-bridge discutidos até o momento faltam ainda prescrições legais que garantam a aptidão probatória duradoura dos certificados.

<sup>25</sup> Veja, por exemplo, Thiel, DuD 2000, 523.

qualidade. Esses procedimentos não são substitutos da forma escrita legalmente prevista. Entretanto, de acordo com o § 127, alínea 3, do Código Civil, basta para a forma eletrônica particular - na falta de uma declaração assinada - que seja obtida por meio de “outra” assinatura conforme o § 1º, alínea 2 da lei de assinatura. Se uma dita assinatura precisar ser utilizada, poderá ser exigido, para a segurança da força probatória do documento, que a manifestação de vontade seja posteriormente declarada com o emprego de uma assinatura eletrônica qualificada. Se o respectivo equipamento não estiver à disposição, poderá ser exigida, ao invés dessa assinatura, uma declaração escrita de próprio punho pelo subscritor do documento ou uma declaração notarial, conforme dispõe o § 126 do Código Civil.<sup>26</sup>

## 5. A aptidão probatória

A aptidão probatória das assinaturas dos procedimentos credenciados é baseada em **duas** presunções. Aquele que desejar carrear provas com essas assinaturas poderá considerar, de um lado, a presunção probatória do § 292a do Código de Processo Civil.<sup>27</sup> De acordo com ela, a aparência de autenticidade de uma manifestação de vontade veiculada na forma eletrônica do § 126a do Código Civil (assinatura eletrônica qualificada), que se apresente na forma da lei de assinatura<sup>28</sup>, só poderá ser afastada no caso de fatos que fundamentem sérias dúvidas de que a declaração de vontade tenha sido realmente fornecida pelo titular da chave de assinatura.<sup>29</sup>

De outro lado, o destinatário da prova poderá considerar a presunção de segurança técnico-organizacional do § 15º, alínea 1, inciso 4 da lei de assinatura, que se refere à prova ampla de segurança técnico-administrativa das assinaturas eletrônicas.<sup>30</sup>

Na prática, a presunção probatória do § 292a do Código de Processo Civil, de que se trata precisamente de uma assinatura qualificada conforme o § 2º, alínea 3 da lei de assinatura, freqüentemente só poderá ser provada com o auxílio da presunção

---

<sup>26</sup> Veja BT-Drs. 14/4987, 21; veja por exemplo também Müglich, MMR 2000, 7; Vehslage, DB 2000, 1802; Scheffler/Dressel, CR 2000, 378; Irrgang, Grundeigentum 2000, 720; Gesellschaft für Informatik, DuD 2001, 38; Sieber/Nöding, ZUM 2001, 199; Eichler, DSWR 2001, 56; Oertel, MMR 2001, 419; Boente/Riehm, JURA 2001, 797.

<sup>27</sup> BT-Drs. 14/4987, 23; veja Roßnagel, NJW 1998, 3312, sobre a presunção de segurança conforme o § primeiro, alínea 1 da lei de assinatura de 1997.

<sup>28</sup> Veja, sobre isso, Hammer, DuD 2000, 96; Spitz, DuD 2001, 459.

<sup>29</sup> Veja o posicionamento crítico quanto a esse preceito, por exemplo, Bundesrat, BT-Drs. 14/4987, 36f.; Roßnagel, MMR 2000, 459 ff.; NJW 2001, 1826; Malzer, em: Geis(editor), Die digitale Signatur – eine Sicherheitstechnik für die Informationsgesellschaft, 2000, S. 180f.; Gesellschaft für Informatik, DuD 2001, 39f.

<sup>30</sup> Veja, quanto a essa presunção de segurança do § primeiro, alínea 1 da lei de assinatura, Roßnagel, NJW 1998, 3312.

decorrente do § 15º, alínea 1, sentença 4 da lei de assinatura.<sup>31</sup> Com base nessa presunção, a parte que produzir a prova já poderá referir as alegações de verificação prévia da segurança dos serviços de certificação e dos componentes técnicos realizada por órgãos de testagem e homologação, e pela RegTP. Por meio da aprovação prévia das respectivas práticas organizacionais e técnicas, a parte que produzir a prova poderá provar os seguintes aspectos: a associação inequívoca entre a assinatura e o titular da chave de assinatura, o controle exclusivo deste sobre sua chave de assinatura, a utilização de um dispositivo seguro de criação de assinatura, a existência de um certificado qualificado, a identificação segura do emissor do certificado e o emprego de algoritmos com os seus respectivos parâmetros, e, finalmente, a impossibilidade de uma posterior alteração dos dados.

No que toca às assinaturas de procedimentos qualificados, vige, contrariamente, apenas uma presunção probatória, especificamente aquela do § 292a do Código de Processo Civil. Para que ela possa ser argüida, a parte que produz a prova não poderá provar, todavia, sem um suporte mais robusto de outra presunção, que a assinatura utilizada preenche todos os seis requisitos de uma assinatura qualificada de que trata o § 2º, alíneas 2 e 3 da lei de assinatura, e que, ainda, essa assinatura possa ser verificada consoante as disposições da lei de assinatura. Se isso ocorrer à parte, ela, na realidade, não poderá mais contar com a presunção de autenticidade do § 292a do Código de Processo Civil. No caso de não ter se submetido à prévia verificação da segurança organizacional e técnica de seus procedimentos, o emissor da assinatura poderá explorar essas fraquezas da assinatura qualificada e poderá até mesmo negar a criação da assinatura com uma perspectiva de êxito. Para refutar isso, o receptor da assinatura necessitará de informações sobre os procedimentos de assinatura empregados e sobre os componentes técnicos, dados essas que não dispõe.<sup>32</sup> Com base na reforma do Código de Processo Civil de 2002, poderá ele, depois do ajuizamento da ação, requerer ao juiz que o emissor da assinatura, com base no § 144 do Código de Processo Civil, apresente em juízo o dispositivo de criação de assinaturas e que o prestador de serviços de certificação apresente toda sua documentação, com base no § 142 do referido código.

Essas novas regras poderiam mitigar, em alguns casos – todavia com os riscos das custas processuais – o ônus probatório da parte que pretenda produzir provas aproveitando-se do benefício do artigo 292a do Código de Processo Civil. Tais dispositivos não o auxiliam quando o certificado não se encontra<sup>33</sup> mais no

---

<sup>31</sup> Nota do tradutor: a presunção referida nesse dispositivo diz que o selo de qualidade recebido pelos prestadores de serviços de certificação credenciados visa a expressar a comprovação de segurança técnico-administrativa dessas entidades.

<sup>32</sup> Sobre a reforma do Código de Processo Civil, veja Rossnagel, NJW 2001, 1826.

<sup>33</sup> Quanto a isso veja o nº 6 *infra*.

serviço de repositório *on-line* do prestador de serviços de certificação ou se esse serviço tiver sido totalmente cancelado.<sup>34</sup>

As assinaturas dos procedimentos ordinários não apresentam qualquer presunção probatória. Elas não podem se beneficiar de facilitações no tocante à produção de prova tendo em vista a falta de informações relacionadas a sua qualidade. Dependerá da parte que queira produzir a prova a demonstração pormenorizada da integridade, autenticidade e autorização da declaração assinada eletronicamente, quando o réu, bem instruído, suscitar impugnações relativas a esses aspectos.<sup>35</sup> De regra, faltarão a ela as informações necessárias sobre técnica e organização dos procedimentos de assinatura empregados. Essas informações também poderão ser obtidas, de forma restrita, por meio do arriscado caminho dos §§ 142 e 144 do Código de Processo Civil. Portanto, em virtude desses aspectos, a aptidão probatória dos métodos de assinatura ordinários é modesta.

## 6. Aptidão probatória ao longo do tempo

Os certificados emitidos por prestadores de serviços de certificação credenciados devem se distinguir dos certificados qualificados, entre outros aspectos, por poderem ser verificados durante um longo período.<sup>36</sup> Deve ser possível, conforme dispõe o § 4º, alínea 2, do decreto de assinaturas, a verificação *on-line* ou o *download* das informações desses certificados, pelo prazo mínimo de 30 anos a contar do momento em que a validade do certificado expirar. Caso um prestador de serviços de certificação credenciado encerre as suas atividades, os certificados por ele emitidos passarão ao controle da RegTP. Com isso é garantido que todos os certificados das entidades credenciadas poderão ser verificados *on-line* durante o período de 30 a 35 anos.<sup>37</sup>

No que toca aos procedimentos de assinatura qualificados, os certificados devem ser conservados e mantidos com possibilidade de serem verificados ou “baixados” durante um período relativamente curto – mais precisamente, pelo tempo de sua validade, mais cinco anos.<sup>38</sup> Após esse tempo, eles podem ser apagados. A

<sup>34</sup> Quanto a isso, veja *infra* n° 8.

<sup>35</sup> Veja, quanto às possíveis manipulações que possam ser praticadas, Die Simulationsstudie Rechtspflege, Eine neue Methode zur Technikgestaltung für Telekooperation, S. 124 ff.; Pordesch, DuD 1993, 561; ders., DuD 2000, 89.

<sup>36</sup> Veja, BT-Drs. 14/4662, 28.

<sup>37</sup> Sobre isso, veja Roßnagel, NJW 2001, 1822f.

<sup>38</sup> A conformidade desta regra ao direito europeu é duvidosa porque ela cria um obstáculo aos serviços de certificação. Os prestadores de serviços de certificação em outros estados da União Européia não devem observar essas condições. Não é suficiente o indicativo da exposição de motivos de que a diretiva não conteria nem instruções relativas ao tempo de conservação de certificados nem qualquer tipo de restrições relativas a esse tema para justificar esse entrave adicional do sistema nacional.

partir dessa realidade, as assinaturas qualificadas não apresentam qualquer garantia de possibilidade de verificação duradoura. Como previsto pela lei de assinatura, se elas não forem mais verificáveis *on-line*, elas não preencherão as prescrições formais e serão imprestáveis como meio de prova. Elas não preencherão mais o pressuposto de presunção probatória do § 292a do Código de Processo Civil, uma vez que a autenticidade da assinatura deve resultar da “verificação conforme a lei de assinatura”. Essa verificação tem lugar por meio dos respectivos componentes de utilização de assinaturas, que, conforme o §17 da lei de assinatura, entre outros dispositivos, devem deixar fixados: a qual resultado a verificação do certificado conduz; a confirmação da associação entre uma chave de verificação com uma pessoa identificada; que a qualquer momento a verificação poderá ser efetuada através de meios de comunicação de acesso público consoante o §5, alínea 1, sentença 2 da lei de assinatura.<sup>39</sup> Quanto aos procedimentos qualificados, a atuação de um terceiro também é decisiva para determinar se e quando os documentos eletrônicos das partes perdem o valor.

No caso dos procedimentos de assinatura ordinários, não existem requisitos para a possibilidade de verificação duradoura dos certificados. Coloca-se ao livre arbítrio do prestador de serviços de certificação a faculdade de colocar ou não, em seu repositório, e por qual período, os certificados emitidos e revogados. Com a utilização desses procedimentos, não há segurança jurídica de que as assinaturas ainda serão verificáveis num momento futuro.

## 7. Documentação de longo prazo

Os prestadores de serviços de certificação credenciados devem conservar sua documentação, por no mínimo 30 anos, a contar do término do ano no qual a validade do certificado respectivo expirou, conforme dispõe, o §8, alínea 3 do decreto de assinatura, que se refere ao §4 do mesmo diploma legal.<sup>40</sup> A disponibilidade e a eventual revogação de certificados também podem ser verificadas, bem como medidas de segurança ou alegadas irregularidades, em até 35 anos após a aposição da assinatura. No caso de estar pendente um processo judicial - antes do transcurso desse prazo - no qual a prova de certificação seja de importância, a documentação deverá ser conservada ainda além desse prazo até que se tenha uma solução definitiva do processo. Após o término do prazo legal de conservação de documentação, não é mais exigível um posterior armazenamento da documentação. Assim, os dados podem ser apagados. O processamento de dados acima dos prazos legais só é permitido com o consentimento do interessado, ou em virtude de autorização legal.<sup>41</sup>

---

<sup>39</sup> Veja, sobre isso também Nissel, *Neue Formvorschriften bei Rechtsgeschäften. Elektronische Form im Privatrechtsverkehr*, 2001, p. 90.

<sup>40</sup> Acerca da responsabilidade da guarda da documentação após o encerramento das atividades, veja infra n° 8.

<sup>41</sup> Informações sobre a finalidade do arquivamento de acordo com as leis de arquivo, veja Schneider, em Roßnagel (editor), *Handbuch des Datenschutzrechts*, 2002, capítulos 8 e 9.

Os fornecedores de certificados qualificados, que comunicarem o início de suas operações conforme o § 4, alínea 3 da lei de assinatura, devem conservar a sua documentação apenas por cinco anos após o ano em que terminar a validade do certificado. Assim, eles devem inutilizar a documentação quando o titular da chave de assinatura não tenha consentido com uma conservação mais longa.<sup>42</sup> Para essa documentação, conforme o §8, alínea 3 do decreto de assinatura, também vige a necessidade da conservação prolongada no caso de um processo judicial pender de decisão. A documentação relativa aos certificados qualificados, conseqüentemente, é conservada por um período entre cinco e dez anos após a utilização da assinatura. Após esse lapso temporal não poderão mais ser esclarecidas as investigações referentes a questionamentos da certificação.

Para os procedimentos “ordinários” de assinatura não existem exigências legais relativas à documentação da disponibilidade e da revogação de certificados. Já que não se apresentam dispositivos legais no tocante à responsabilidade dos prestadores de serviços de certificação e de facilidades para a prova da ausência de culpa; falta um incentivo legal para que os prestadores de serviços de certificação gerenciem a documentação. Fica ao seu livre talante o período de tempo pelo qual será conservada determinada documentação. É totalmente incerto se tal documentação poderá ser recuperada no caso de uma contenda jurídica.

## **8. A “sobrevida” dos certificados à paralisação das atividades do prestador de serviços de certificação**

Se um prestador de serviços de certificação credenciado quiser ou precisar encerrar suas atividades, ele deverá providenciar, conforme o mandamento do §13, alínea 1, sentença 2, da lei de assinatura, que quando da paralisação de suas operações, a documentação disponível e os certificados alocados no seu serviço de repositório sejam assumidos por um outro prestador de serviços de certificação credenciado. Ao mesmo tempo, a RegTP deverá garantir, consoante a previsão do §15, alínea 6, sentença 1, da lei de assinatura, que as atividades terão prosseguimento com um outro prestador de serviços de certificação credenciado. Não basta apenas encontrar um fornecedor que aceite assumir os certificados e a documentação, a RegTP deverá garantir também que os contratos em vigor com os titulares de chaves de assinatura sejam cumpridos.<sup>43</sup> Nesse caso, os prestadores de serviços de certificação deverão

---

<sup>42</sup> Veja Roßnagel, na mesma obra, capítulo 7.7.

<sup>43</sup> A responsabilidade de assumir as atividades não se resume exclusivamente aos certificados válidos. Indo além, a RegTP, de acordo com o § 15, alínea 6, sentença 1 da lei de assinatura, deverá providenciar a assunção de todas as atividades do prestador de serviços de certificação credenciado. E nisso está compreendido também a manutenção da possibilidade de comprovação dos certificados revogados – quanto a isso veja também Blum, DuD 2001, 74.

revogar os certificados ainda válidos, a teor do §13, alínea 1, sentença 2, da lei de assinatura, bem como encaminhá-los, juntamente com toda a documentação, para a RegTP. Isso permite a conservação da documentação e dos certificados emitidos pelo prazo de 30 anos a contar do término de sua validade, de modo que eles sejam verificáveis a qualquer momento (conforme preceituam o §15, alínea 6, sentença 1, e §10, alínea 1, sentença 1 da lei de assinatura).<sup>44</sup> Na prática, somente os certificados dos prestadores de serviços de certificação credenciados ainda serão verificáveis, após a assunção da documentação pela RegTP.

De forma diversa, para os prestadores de serviços de certificação não credenciados que tenham apenas notificado a RegTP do início de suas atividades, e que venham a encerrar as operações, não existirá o dever de continuidade da RegTP. Observado o que diz o §13, alínea 1, sentença 2, da lei de assinatura, esse prestador de serviço de certificação deverá providenciar por si próprio que a sua documentação e que os certificados qualificados ainda válidos sejam assumidos por uma outra entidade. Este, por seu turno, será obrigado a continuar gerenciando apenas o certificados válidos no momento em que assumiu as atividades<sup>45</sup> bem como aqueles que se encontram no repositório de certificados, mas não os certificados revogados.<sup>46</sup> Com isso, falta aos certificados revogados a possibilidade de sua verificação desde o momento preciso em que foram revogados. Outrossim, carecem também de indicativos acerca das causas da revogação<sup>47</sup>, desde quando isso ocorreu, bem assim de eventuais restrições então existentes, ou de atributos constantes do certificado.<sup>48</sup> Em que pese a realidade de que até mesmo antes do momento de sua revogação esses certificados possibilitem declarações de vontade com efeitos jurídicos, todas as assinaturas qualificadas criadas anteriormente perderão o seu valor probatório com o encerramento das atividades do respectivo prestador de serviços de certificação.<sup>49</sup> Com relação à documentação a ser assumida e aos certificados ainda válidos, o prestador de serviços de certificação substituto absorve os deveres do prestador de serviços de certificação substituído. Ele deverá dar prosseguimento à lista de certificados e à guarda da documentação, consoante o § 4, alínea 3, do decreto de assinatura, pelo mesmo período que incumbiria ao antigo prestador de serviços de certificação.

---

<sup>44</sup> Arquivos das Comissões internas do parlamento, BT-Drs. 14/5324, 25: § 15, alínea 6 da lei de assinatura deverá “garantir a possibilidade de verificação posterior das assinaturas eletrônicas qualificadas com prestador de serviços de certificação credenciados.”

<sup>45</sup> Contrariamente Blum, DuD 2001, 74: compreensivelmente, também pertencem aos certificados válidos os certificados somente verificáveis nos repositórios de certificados.

<sup>46</sup> Veja em pormenor Blum, DuD 2001, 74; Bertsch/Fleisch/Michels, DuD 2002, 71.

<sup>47</sup> Veja Roßnagel (Fn.40), Rn. 105.

<sup>48</sup> Veja em pormenor Blum, DuD 2001, 74.

<sup>49</sup> Veja quanto à supressão da presunção probatória do § 292a do Código de Processo Civil, o item n° 6, acima.

Esse dever de cuidado<sup>50</sup> do prestador de serviços de certificação não credenciado também é coberto, conforme o §24, alínea 1, sentença 10, da lei de assinatura, com uma multa pecuniária. Com efeito, na prática, só é possível punir a inexistência de esforços; raramente, todavia, a eventual tomada de medidas práticas de baixa qualidade. Caso não seja possível ao prestador de serviços de certificação encontrar um substituto que assuma os seus certificados, quando do encerramento das atividades, ele deverá revogar os certificados de acordo com o que dispõe o §13, alínea 1, sentença 2, da lei de assinatura. Neste caso, ele deverá apenas entregar a documentação à RegTP, sendo que esta deverá conservá-la pelo mesmo tempo que o prestador de serviços de certificação teria de fazê-lo (conforme preceituam o §10, alínea 3, sentenças 1 e 4 da lei de assinatura e §3 do decreto de assinatura). Diversamente dos procedimentos credenciados, e consoante dispõe o §13, alínea 2, sentença 3 da lei de assinatura, a RegTP somente fornecerá informações<sup>51</sup> no caso de existir um interesse legítimo e ainda assim, apenas se isso for possível sem grandes esforços técnicos. Tendo em vista as limitações estruturais e de pessoal do departamento responsável da RegTP, isso dificilmente ocorrerá.<sup>52</sup> Tendo em vista que o serviço de listas de verificação não prosseguirá, os certificados não poderão mais ser checados. Já que também poucas informações da documentação poderão ser obtidas, todas as assinaturas criadas no passado por meio de procedimentos qualificados perderão a sua aptidão probatória com o encerramento das operações do prestador de serviços de certificação não credenciado. Daí, nem sua integridade ou autenticidade, ou a sua adequação formal poderão ser comprovadas.<sup>53</sup>

Para os procedimentos de assinatura ordinários não existe qualquer regra protetora dos titulares de chave de assinatura ou de terceiros que determine o que ocorrerá no caso do encerramento das atividades de um prestador de serviços de certificação. O prestador de serviços de certificação provavelmente destruirá ou venderá a sua documentação, contanto que ele a possua, e requererá falência. Neste caso, todas as assinaturas criadas no passado não poderão ser verificadas e não terão valor como prova de declaração de vontade.

---

<sup>50</sup> Contrariamente Blum, DuD 2001, 74, que entende tratar-se não apenas de um dever de cuidado, mas sim de um dever jurídico.

<sup>51</sup> Veja quanto a isso também; Bertsch/Fleisch/Michels, DuD 2002, 72.

<sup>52</sup> Veja quanto à justificativa dessa diferença os arquivos das comissões internas do parlamento, BT-Drs. 14/5324, 25.

<sup>53</sup> Na hipótese de que a parte a apresentar a prova tenha corretamente arquivado todas as informações relevantes do status da assinatura – veja Brandner/Pordesch/Roßnagel/Schachermayer, DuD 2002, 97 ff. Ainda nesse caso a falta de uma âncora de confiança na corrente de certificação continua sendo um ponto fraco dos procedimentos qualificados dos prestadores de certificação na credenciados.

## 9. Reconhecimento de assinaturas e produtos estrangeiros

Para a valoração do nível de segurança técnico e organizacional dos diversos procedimentos de assinatura também deverá ser considerado, se e como o nível de segurança de produtos e procedimentos de assinatura estrangeiros - eventualmente sujeitos a outros critérios de detalhamento ou procedimentos probatórios - são equiparados aos procedimentos e produtos de assinaturas nacionais.

As assinaturas eletrônicas estrangeiras, conforme §23, alínea 2, da lei de assinatura, só serão equiparadas às assinaturas de um procedimento de assinatura credenciado quando uma segurança equivalente tenha sido previamente comprovada. Para assinaturas estrangeiras, a RegTP somente determinará essa equiparação de segurança com as assinaturas credenciadas, na linha do previsto no §18, alínea 2, do decreto de assinatura. Ou seja, quando: as exigências de segurança dos prestadores de serviços de certificação e dos produtos, as modalidades de testagem destes últimos, as exigências quanto aos órgãos de testes e homologação bem como os sistemas de credenciamento e de supervisão oferecerem uma segurança equivalente. Similarmente, os produtos estrangeiros com componentes testados para procedimentos de assinatura credenciados, conforme o §15, alínea 8, da lei de assinatura, serão equiparados somente quando uma segurança equivalente tenha sido comprovada também para eles. Para esta prova servem, pelo teor do §18, alínea 3, do decreto, os mesmos princípios aplicáveis à verificação de equiparação de valor das assinaturas. Neste caso também é exigida uma declaração afirmativa homologatória da RegTP.

De modo diverso, todas as assinaturas criadas a partir de certificados da União Européia ou de outro Estado associado do tratado sobre o espaço econômico europeu, que satisfaçam as exigências do art. 5º, § 1º da diretiva, são equiparadas às assinaturas eletrônicas qualificadas automaticamente, ou seja, sem necessidade de verificação de equiparação do valor das assinaturas. Para estes procedimentos de assinatura qualificada europeus, não deveria existir qualquer sistema de supervisão similar ao previsto nos §§ 4º e 19º da lei de assinatura. Em menor grau, ainda poderá ser aceita uma segurança de valor equiparado, quando, conforme o §23, alínea 1, sentença 2, da lei de assinatura, as assinaturas forem baseadas em certificados de outros países. Por isso que as assinaturas eletrônicas qualificadas devem ser equiparadas, e também porque o prestador de serviços de certificação estabelecido na União Européia responde pelos certificados de seu parceiro internacional. Em realidade, um prestador de serviços de certificação alemão não credenciado, conforme o §18, alínea 1 do decreto, deverá notificar a RegTP e também providenciar que as assinaturas e certificados estrangeiros obedeçam as exigências da lei de assinatura e do decreto de assinatura, e que as informações exigidas para a notificação de que trata o §18, alínea 1, do decreto estejam disponíveis.<sup>54</sup> Essas diretrizes não existem para os prestadores de serviços

---

<sup>54</sup> Veja Rossnagel, BB 2002, 64.

de certificação que se responsabilizem por prestadores de serviços de certificação de fora da União Europeia. Neste caso, o dever de responsabilização estabelece apenas um responsável solidário, mas não uma prova de segurança suficiente.

Pelo que prevê o §23, alínea 3, da lei de assinatura, quando em outro estado membro da União Europeia ou em outro estado associado do tratado sobre o espaço económico europeu tenha sido determinada a observância das exigências da diretiva, os produtos para assinaturas eletrónicas devem ser reconhecidos como suficientes para os procedimentos de assinaturas qualificados (isto especialmente para os componentes de criação de assinatura, porque apenas estes, de acordo com o arr. 3º da diretiva europeia, devem ser previamente testados). A extensão e a profundidade da testagem não são nem conhecidas nem influenciáveis.

Os procedimentos de assinatura ordinários não apresentam distinções jurídicas entre os procedimentos nacionais e estrangeiros, uma vez que os próprios procedimentos nacionais não estão vinculados a quaisquer consequências jurídicas específicas.

## 10. A Responsabilidade dos prestadores de serviços de certificação

Quanto a todos os três procedimentos de assinatura a responsabilidade contratual entre os prestadores de serviços de certificação e os titulares de chaves de assinatura se direciona, na mesma medida, para os princípios gerais. Em face de terceiros, todavia, apenas no que toca aos procedimentos credenciados e qualificados é que existe uma responsabilidade<sup>55</sup> específica dos prestadores de serviços de certificação.<sup>56</sup> Consoante o §11, alínea 1, da lei de assinatura, se um prestador de serviços de certificação infringir as exigências da lei ou do decreto, ou se outros componentes técnicos de segurança falharem, ele responderá perante um terceiro<sup>57</sup> pelos prejuízos que este venha a sofrer por ter confiado nas indicações de um certificado qualificado, ou num “time-stamp” qualificado ou ainda na informação do serviço de repositório.<sup>58</sup> Esta responsabilidade é garantida por meio de uma provisão de cobertura (seguro), conforme dispõe o §12, da lei de assinatura e o § 9 do decreto de assinatura.<sup>59</sup>

---

<sup>55</sup> Esta ocorre ao lado de previsões legais de responsabilidade extracontratual – veja, por exemplo, Blum, DuD 2001, 75.

<sup>56</sup> BT-Drs. 14/4662,24.

<sup>57</sup> De acordo com Blum, DuD 2001, 75, o terceiro, cujas informações estejam contidas no certificado, deve estar protegido por um contrato em favor de terceiros e não pelo § 11 da lei de assinatura.

<sup>58</sup> Sobre esse assunto veja em pormenores, Thomale: Die Haftung des Zertifizierungsdiensteanbieters, Baden-Baden 2002, i.E.

<sup>59</sup> Veja em Roßnagel, BB 2002, 262.

Quanto aos procedimentos ordinários de assinatura, perdura para o prestador de serviços de certificação perante terceiros apenas uma responsabilidade extracontratual, conforme o §823, alínea 1, do Código Civil, quando um bem jurídico tenha sido incontestavelmente lesado. Isso raramente ocorre. À míngua de uma outra regulamentação legal - com a exceção de um tipo penal como o de fraude - não haveria infringência a qualquer lei protetiva, a teor do §823, alínea 2, do Código Civil. Um terceiro que confie numa assinatura advinda desses procedimentos ordinários, que venha a sofrer um prejuízo patrimonial, provavelmente não receberá uma indenização.<sup>60</sup>

### III. Condições estruturais para a escolha

Estas diferenças entre os procedimentos de assinatura devem ser observadas por todos aqueles que tenham que tomar decisões de escolha.

#### 1. A decisão do legislador

O legislador que pretenda permitir a utilização de assinaturas eletrônicas na esfera de atuação pública deverá, na escolha dos procedimentos de assinatura eletrônicas credenciadas, seguir também as exigências do artigo 3, alínea 7 da diretiva europeia. Este preceito determina: “Os estados membros podem submeter a utilização de assinaturas eletrônicas no setor público a eventuais requisitos adicionais. Esses requisitos devem ser objetivos, transparentes, proporcionais e não discriminatórios e dizer apenas respeito às características específicas da utilização em causa. Esses requisitos não devem constituir para o cidadão um obstáculo aos serviços transfronteiriços.” Este comando legal tem por consequência que em regra as assinaturas dos cidadãos devem ser providas por procedimentos de assinatura qualificados, mas que para as assinaturas de repartições públicas devem ser exigidos procedimentos de assinatura credenciados.<sup>61</sup>

#### 2. A decisão do usuário

Os usuários de procedimentos de assinatura são, todavia, amplamente livres na sua decisão de escolha. Ela só é restringida nos casos em que uma determinação legal exija expressamente procedimentos qualificados ou credenciados ou nos casos

---

<sup>60</sup> Vide: Bundesrat, BR-Drs. 966/96 (Beschluss), 21f.; BR-Drs. 420/97 (Beschluss); Roßnagel, em: Tauss/Koillbeck/Mönikes (Hrsg.), Deutschlands Weg in die Informationsgesellschaft, 1996, S. 669f.; ders., DuD 1997, 79; Bömer, ZUM 1997, 246; Timm, DuD 1997, 525; Neuser, MMR 1999, 67.

<sup>61</sup> Veja Roßnagel, DÖV 2001, 225f.

em que a assinatura eletrônica deva substituir a forma escrita. Mas os usuários sempre terão liberdade de aplicar um procedimento de valor superior, ainda que um outro procedimento seja exigido ou permitido.

Para as declarações de vontade que, em caso de necessidade tenham de ser utilizadas como meio de prova perante os tribunais, poderão ser necessários em muitas aplicações o nível de segurança e a segurança de verificação dos procedimentos de assinatura credenciados, que propiciam a observância das formas, a segurança probatória, bem como a segura possibilidade de verificação ao longo do tempo dos documentos assinados eletronicamente. Somente quando estas assinaturas forem empregadas é possível prevenir também com segurança pretensões de responsabilização das repartições públicas ou eventuais pretensões de indenização decorrentes de lesões a direitos de crédito ou de culpa no momento da contratação. Esta responsabilização pode ocorrer quando forem empregados procedimentos de assinatura cujas medidas de segurança não testadas possibilitem manipulações, ou quando as respectivas assinaturas, depois de um determinado tempo, não sejam mais verificáveis.

Da mesma forma, são exigidos desde o começo, procedimentos de assinatura credenciados em todas as aplicações nas quais não seja descartado que após cinco anos seja necessário conferir os dados assinados. É que somente nesses procedimentos é garantida a possibilidade de verificação de forma duradoura dos certificados e da documentação de todos os registros de certificação relevantes, até mesmo após eventual falência do prestador de serviços de certificação. Apenas com os procedimentos de assinatura credenciados pode-se também resolver<sup>62</sup> de maneira satisfatória o problema do arquivamento duradouro e com segurança probatória dos dados assinados eletronicamente, conforme o § 17 do decreto de assinatura.<sup>63</sup>

Aquele que utiliza os procedimentos ordinários de assinatura deve atentar para o fato de que a sua assinatura: não garante um nível de segurança homologado pela autoridade competente nem mesmo previsto em lei; não preenche os requisitos da lei; não produz meios de prova passíveis de serem alegados em juízo; se perde quando de eventual encerramento das atividades do prestador de serviços de certificação; não garante qualquer possibilidade de verificação duradoura e não oferece a terceiros qualquer pretensão jurídica de responsabilização.

Portanto, esses procedimentos sequer podem ser considerados para as transações comerciais que demandem vinculação jurídica. Isso também vale para as

---

<sup>62</sup> Veja o § 18 do decreto de assinatura de 1997 e Roßnagel/Hammer, em: Roßnagel (Fn. 1), § 18 do decreto de assinatura, Rn. 19 ff.

<sup>63</sup> Veja em detalhes Brandner/Pordesch/Roßnagel/Schacermayer, DuD 2002, 97.

soluções provisórias com limitações temporais. O governo federal considera utilizar soluções transitórias sem cartões inteligentes e leitoras de cartão no seu plano de implantação da iniciativa de e-gov “BundOnline 2005”<sup>64</sup> para os processos administrativos com exigências de forma escrita. Porém, a utilização temporária de soluções de software causaria a duplicação dos custos e exigiria a dupla criação de procedimentos de assinatura. Entrementes os padrões equivocados seriam estabelecidos e poucas experiências aproveitáveis seriam geradas.<sup>65</sup> Afora isso – já durante a precária implantação – a utilização de procedimentos inseguros aumentaria o risco de que para a introdução de procedimentos de assinaturas seguros fosse ameaçada a necessária confiança do sistema por meio de um ataque excessivo da mídia aos pontos fracos de tais procedimentos de assinatura inseguros transitoriamente permitidos.

Se for feito uso dos procedimentos ordinários de assinatura, deve-se atentar outrossim, que nas formas escritas particulares o receptor poderá exigir a qualquer momento, para a garantia da força probatória do documento, que a manifestação de vontade seja também veiculada por meio de uma assinatura eletrônica qualificada (de acordo com o §127, alínea 3, do Código Civil). Se o respectivo aparelhamento não estiver disponível, poderá ser exigido, ao invés disso, o documento previsto no § 126 do Código Civil.<sup>66</sup> O usuário desses procedimentos ordinários de assinatura deverá, conseqüentemente, sempre dispor de procedimentos de assinatura qualificados ou considerar a instrumentalização em papel.

Com efeito, para a escolha dos procedimentos de assinatura poderia-se diferenciar entre atos com ou sem vinculação jurídica ou entre os diferentes potenciais de risco e o respectivo emprego, e poderia-se implantar procedimentos de assinatura variados para diferentes utilizações. Se todavia o mesmo usuário utilizar procedimentos diversos, ele deverá ter em conta a duplicação ou triplicação dos custos de investimento, dos esforços organizacionais e dos custos de implantação e de treinamento.<sup>67</sup> É fato que os procedimentos ordinários de assinatura podem demandar custos mais baixos do que os dos procedimentos conforme a lei, pois eles não utilizam cartões inteligentes para o armazenamento da chave privada nem necessitam dos leitores de cartões. Mas se a chave privada fizer parte de um software, não se pode garantir a sua propriedade de unicidade. Essa insuficiência no que toca à segurança, além das outras propriedades

---

<sup>64</sup> Governo Federal, Plano de Implantação para a iniciativa e-gov Bund Online 2005, 2001, p. 35, [www.staat-modern.de/infos/daten/bund\\_umsetzpl.pdf](http://www.staat-modern.de/infos/daten/bund_umsetzpl.pdf), 35.

<sup>65</sup> Todavia, o estabelecimento de padrões e o acúmulo de experiências são as justificativas principais para a solução temporária aqui tratada.

<sup>66</sup> Veja BT-Drs. 14/4987, 21; veja, por exemplo também, Vehslage, DB 2000, 1802.

<sup>67</sup> KPMG, Possibilidades de implantação da assinatura eletrônica na administração pública e na economia, 2001, p. 84, recomenda um procedimento de assinatura único em nível superior.

já descritas, torna inaceitável a utilização dos procedimentos ordinários para declarações de vontade que necessitem vinculação jurídica. Não há diferença<sup>68</sup>, pelo que se pode ver, quanto aos custos de implantação e operacionalização entre os procedimentos de assinatura qualificados e os credenciados para as entidades da administração pública e para as organizações empresariais internas.<sup>69</sup> Ainda que para alguns processos relevantes não seja obrigatória a utilização de procedimentos de assinatura credenciados, é fácil supor que em outros processos será essencial o emprego dos procedimentos credenciados. Esses procedimentos preenchem todas as exigências legais e previnem problemas de responsabilidade. Eles contribuem para a imagem positiva acerca da melhor qualidade e para disponibilizar o mais elevado nível de segurança e conseqüentemente satisfazer todas as exigências.

---

<sup>68</sup> O credenciamento gera para os prestadores de serviços de certificação um incremento de mais ou menos 10% nos custos em comparação com a opção de não obter o credenciamento. Isso considerado para a integralidade das instalações.

<sup>69</sup> Todavia, há diferenças decisivas na estrutura de certificação – veja, parte II, item 3.