A alocação dos riscos na utilização da assinatura digital

Fabiano Menke
Advogado e Professor da Graduação e do Programa de Pós-Graduação
da Universidade Federal do Rio Grande do Sul

Texto publicado em 02.06.2020, em:
https://migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/328076/a-alocacao-dos-riscos-na-utilizacao-da-assinatura-digital

A pandemia do novo coronavírus colocou em ainda maior evidência a necessidade de os negociantes realizarem atos e celebrarem contratos pelo meio eletrônico. Desde o ano de 2001, com a edição da Medida Provisória nº 2.200-2 (MP 2.200-2), o Brasil consolidou o que se denomina Infraestrutura de Chaves Públicas Brasileira[1], que tem por escopo garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, a partir da emissão de certificados digitais que identificam as pessoas naturais e pessoas jurídicas que pretendam acessar soluções virtuais ou se vincularem juridicamente a declarações de vontade no meio eletrônico.

A denominada assinatura digital ICP-Brasil funciona, portanto, como mecanismo de identificação e como substituto da assinatura manuscrita. Esta equiparação legal[2]. à assinatura manuscrita foi realizada a partir da incorporação, pelo art. 10, § 1º, da MP 2.200-2[3], do art. 219 do Código Civil e foi possível porque a Infraestrutura de Chaves Públicas Brasileira se vale de um conjunto de regras com arrimo em *standards* internacionais que buscam atingir os mais altos níveis de segurança. Dentre estes, vale destacar dois, de grande relevância no que toca a implicações jurídicas: 1) a identificação do titular do certificado digital se dá mediante a sua presença física por meio do comparecimento perante um terceiro de confiança, uma Autoridade de Registro vinculado a uma Autoridade Certificadora[4]; 2) o emprego da criptografia assimétrica, baseada no conceito de chave pública e chave privada.

Quanto ao primeiro aspecto, a identificação do indivíduo por meio de sua presença física agrega um elemento de robustez à ferramenta que posteriormente será utilizada para a interação social, a prática de atos e a conclusão de contratos no meio eletrônico. Basta que se faça a comparação com os mecanismos que habitualmente se utilizam para a comprovação de identidade e de autoria nas interações e negócios virtuais. As redes sociais, instituições financeiras, *sites* de comércio eletrônico, entre outros tantos modelos de negócios, adotam comumente o *login* e a senha, sendo que, no mais das vezes, tanto um quanto o outro são criados e/ou alterados pelo próprio indivíduo, que poderá confeccionar um perfil falso e causar danos ao se passar por outra pessoa.

Quanto ao segundo aspecto, a criptografia assimétrica agrega algo que implica em verdadeira guinada no que diz respeito à lógica das ferramentas de identificação, uma vez que segrega, o que poderia ser chamado de senha, em chave pública e chave privada. A chave pública, como a denominação indica, é de conhecimento e acesso geral. Mas a chave privada é armazenada em dispositivos seguros como *tokens* e cartões inteligentes, de onde não é exportada. Novamente, calha a comparação com *login* e senha, porquanto estes, além de serem conhecidos do titular que os criou, ficam armazenados nos bancos de dados dos fornecedores, de modo que, para efeitos de imputação jurídica ambos podem ser considerados, tanto titular quanto fornecedor. O compartilhamento da senha que existe no mecanismo de *login* e senha não se faz presente no emprego do certificado digital com criptografia assimétrica e chave privada.

Na hipótese de danos causados no uso de *login* e senha e de outros mecanismos que não o certificado digital, pode-se cogitar de o *site* responder pelos prejuízos causados em virtude de fraudes na identificação, isto é, o fornecedor que disponibiliza a oportunidade de interação ou de fazer negócios, como as redes sociais, instituições financeiras e lojas e plataformas do comércio eletrônico.

De outra banda, ao mesmo tempo em que os procedimentos e requisitos da emissão do certificado digital agregam maior confiabilidade e segurança para identificar pessoas *online*, e, consequentemente, diminuem as fraudes, resta alterada a distribuição dos riscos normalmente conhecida no que toca à responsabilização pelos danos causados.

E estes riscos passam a ser alocados nos fornecedores de certificados digitais, quais sejam Autoridades Certificadoras e entidades a elas vinculadas[5], bem como nos próprios usuários.

Autoridades Certificadoras e Autoridades de Registro, como regra geral, responderão por eventuais erros na identificação, o que pode ocorrer a partir da apresentação de documentos falsos na ocasião em que o solicitante comparece mediante a sua presença física para obter o certificado digital, e é justamente por isso que todo o cuidado é pouco nesta atividade.

Os usuários poderão ter de responder pelos danos que venham a experimentar, sem ter como imputá-los ao *site* ou à aplicação na qual o certificado digital foi utilizado, sempre que não tomarem as devidas cautelas na guarda do certificado digital que lhes tenha sido corretamente emitido[6].

Recorde-se: não se tem mais o argumento da utilização das senhas, sob a alegação de que possa ter vazado do banco de dados do fornecedor, pois aqui não se cuida mais de senha, mas sim de chave privada, que fica armazenada em dispositivo que é fornecido pela Autoridade Certificadora ao titular do certificado digital, e, a partir da geração da chave privada, que ocorre dentro da própria mídia de armazenamento que está na posse do titular, ela será de sua exclusiva custódia.

O *site* ou aplicação não fornecem mais um importante elemento de identificação do usuário e de formalização de suas declarações de vontade, mas são "visitados" pelo titular do certificado digital, que o obteve perante outro fornecedor (Autoridade Certificadora e Autoridade de Registro).

Há que se atentar, neste contexto, ao vocábulo "infraestrutura", contido na denominação Infraestrutura de Chaves Públicas Brasileira, pois ele remete à ideia do que conceitualmente seja uma infraestrutura[7], ou seja, o conjunto das instalações necessárias que disseminem uma funcionalidade para um amplo ambiente ou para um grande universo de interessados, de modo que qualquer usuário possa simplesmente acoplar-se a ele e dele fazer uso quando necessário, exatamente como ocorre nas infraestruturas de saneamento, de eletricidade, de transporte, entre outras.

Em outras palavras, usuários da infraestrutura de identificação e de vinculação de negociantes do ambiente eletrônico passam a ser, além dos próprios usuários do certificado digital (pessoas naturais e pessoas jurídicas), os *sites* e aplicações das mais variadas atividades de interação social na medida em que optam pelos mecanismos de atribuição de identificação e de atribuição de autoria instituídos pela MP 2.200-2.

A cada vez mais crescente migração da prática de atos e de negócios para o meio eletrônico, intensificada pela recente pandemia, faz com que se tenha de incrementar as rotinas de segurança das organizações, e, em muitos aspectos, como o relativo aos mecanismos de identificação e de comprovação de autoria, é possível se valer de alternativas como as da Infraestrutura de Chaves Públicas Brasileira. Neste sentido, é oportuno o conhecimento acerca de conceitos e consequências jurídicas de sua utilização, como os expostos no presente artigo.

---

[1] O termo Infraestrutura de Chaves Públicas é tradução da expressão do inglês, *public-key infrastructure (PKI)*.

[2] A mesma equiparação legal feita no Brasil foi realizada em países como a Alemanha, que inclusive a previu em dispositivo específico de seu Código Civil, o BGB, a partir da inclusão do §126a com a Lei de Adaptação das Formas (*Formanpassungsgesetz*) do ano de 2001. Ver, sobre as formas eletrônicas no Código Civil Alemão bem como no direito brasileiro, em MENKE, Fabiano, *Die elektronische Signatur im deutschen und brasilianischen Recht: Eine Rechtsvergleichende Studie*, Baden-Baden: Nomos, 2009.

[3] Determina o referido dispositivo: "§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil."

[4] O Comitê Gestor da ICP-Brasil editou a Resolução nº 170, de 20 de abril de 2020, que dispõe sobre o regime transitório de emissão de certificados digitais em face da pandemia do novo coronavírus, facultando que a identificação do interessado se dê por videoconferência, observando-se, todavia, que o prazo de validade máximo do certificado digital será não de três anos, mas sim de um ano.

[5] As Autoridades Certificadoras poderão ser tanto pessoas jurídicas de direito privado quanto de direito público. As Autoridades de Registro são sujeitos de direito vinculados às Autoridades Certificadoras, e que na ponta final identificam os usuários.

[6] No que toca às cautelas que devem ser tomadas pelo usuário, há farta jurisprudência valorando a sua conduta e os cuidados com a posse dos cartões de banco e senhas, que também podem inspirar o julgador nos casos que contemplem a certificação digital. Veja-se os seguintes exemplo: REsp 1.633.785/SP, Rel. Ministro Ricardo Villas Bôas Cueva, 3ª Turma, julgado em 24/10/2017, DJe de 30/10/2017; AgInt no AREsp 1.305.380/RJ, Rel. Min. Raul Araújo, 4ª Turma, julgado em 18/02/2020, DJE 13/03/2020.

[7] ADAMS; LLOYD. *Understandig Public-Key Infrastructure:* concepts, standards, and deployment considerations. Indianapolis: New Riders, 1999, p. 27-28.