Processo n°: 201600029001929
Nome: Gerência de Informática
Assunto: Solicitação

PARECER GEJUR Nº 0088/2016 -

1. Trata-se de solicitação, formulada pela Coordenação de Informática, de análise, apontamentos de adequações e autorização do uso do Termo de Adesão dos Serviços de Cadastramento Eletrônico da Agência Goiana de Regulação, Controle e Fiscalização de Serviços Públicos – AGR, para ser publicado no portal de serviços eletrônicos e assinado pelas empresas que deles necessitarem.

2. A solicitação foi formalizada com o memorando nº 0009/2016-CI (fl. 02) que informa que esse termo de adesão, cuja minuta encontra-se nas fls. 03/05, permitirá às empresas reguladas e fiscalizadas da AGR, diretamente ou por meio de seus procuradores, demandarem serviços e praticarem atos processuais que dependam de petição escrita, por meio de formulários eletrônicos próprios, fazendo uso da Internet.

3. Na sequência, a solicitação da Coordenação de Informática foi acatada pela Gerência de Gestão, Planejamento e Finanças para análise legal da minuta do termo de adesão de serviços – cadastramento eletrônico de empresa, ferramenta virtual que permitirá as empresas demandarem atos por meio eletrônico em substituição aos atuais formulários manuscritos (fl. 06).

4. Registre-se que foram realizadas pela Coordenação de Informática duas reuniões nos dias 11 e 12 de abril de 2016 para apresentação do Sistema Eletrônico de Cadastro de Empresas, que conterá diversos módulos, como o cadastramento de empresas, cadastramento de veículos e as autorizações de viagem.

5. Dessas reuniões, constatou-se a necessidade, para maior compreensão das possíveis implicações jurídicas relacionadas, de retorno dos autos à Coordenação de Informática para juntada de uma descrição, em linguagem leiga, do referido sistema, com a indicação de seus principais documentos, inclusive aqueles que dependem de assinatura, razão pela qual foi juntada a

descrição técnica de software Sistemas de Transporte, Sub módulo de Cadastro e Licenciamento e anexos (fls. 11/44).

6. Após, os autos retornaram à Gerência Jurídica. É o relatório.

7. Antes de se adentrar na parte jurídica de análise do termo de adesão, considerando-se o estágio atual de desenvolvimento da tecnologia da informação, em que os ambientes virtuais já substituem e substituirão determinados ambientes físicos com as facilidades de acesso remoto por meio da rede mundial de computadores, convém fazer-se uma breve contextualização sobre o assunto segurança da informação.

8. A norma ISO/IEC 27002:2013, da Associação Brasileira de Normas Técnicas-ABNT, que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização, é de grande importância para implementação de um sistema como o proposto. Oportunamente, informa-se que essa norma pode ser comprada no sítio http://www.abntcatalogo.com.br/norma.aspx?ID=306582, acesso em 18/05/16.

9. Nesta norma, na versão anterior a que se teve acesso (ISO/IEC 27002), em sua introdução, consta o que é e porque a segurança da informação é necessária, conforme transcrito à seguir:

> 0 Introdução
>
> 0.1 O que é segurança da informação
>
> A segurança da informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ver OECD Diretrizes para a Segurança de Sistemas de Informações e Redes).
> A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.
A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

0.2 Por que a segurança da informação é necessária?

A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado.
As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por códigos maliciosos, hackers e ataques de *denial of service* estão se tomando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.
A segurança da informação é importante para os negócios, tanto do setor público como do setor privado, e para proteger as infra-estruturas críticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como o governo eletrônico (e-gov) ou comércio eletrônico (e-business), e evitar ou reduzir os riscos relevantes. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída reduz a eficácia da implementação de um controle de acesso centralizado.
Muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados. A identificação de controles a serem implantados requer um planejamento cuidadoso e uma atenção aos detalhes. A gestão da segurança da informação requer pelo menos a participação de todos os funcionários da organização. Pode ser que seja necessária também a participação de acionistas, fornecedores, terceiras partes, clientes ou outras partes externas. Uma consultoria externa especializada pode ser também necessária.

10. Além disso, existe uma publicação chamada COBIT 5 (*Control Objectives for Information and related Technology*), disponível em http://www.isaca.org/COBIT/Pages/COBIT-5-portuguese.aspx, acesso em 18/05/16, que "... é um modelo de negócios e de gestão global para governança e gestão de TI corporativa. (...)O COBIT permite às organizações maximizar o valor e minimizar o risco relacionado à informação, que tornou-se a moeda corrente do século 21. COBIT 5 é um modelo abrangente dos princípios globalmente aceitos, das práticas e das ferramentas analíticas e que podem ajudar qualquer organização para efetivamente resolver problemas críticos dos negócios relacionados à governança e gestão da informação e tecnologia".

11. Tais documentos, pois, consolidam práticas aceitas sobre a segurança da informação que podem ser úteis para a área de tecnologia da informação na implantação e desenvolvimento de sistemas como o referente ao Cadastro de Empresas.

12. Ainda sobre segurança da informação e outros aspectos da Internet, é importante citar a Lei nº 12.965/14, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e regulamenta, dentre outros assuntos, a necessidade de proteção da privacidade[1], dos dados pessoais[2], a adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados[3], a proteção da intimidade e do sigilo[4] e, em relação ao poder público, a adoção preferencial de tecnologias, padrões e formatos abertos e livres e a prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos[5].

13. Especificamente em relação ao Poder Público, destaca-se o art. 25 da Lei nº 12.965/14:

---

[1] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
(...)
II - proteção da privacidade;

[2] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
(...)
III - proteção dos dados pessoais, na forma da lei;

[3] Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:
(...)
IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

[4] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

[5] Art. 24. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil:
(...)
V - adoção preferencial de tecnologias, padrões e formatos abertos e livres;
(...)
X - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos.

> Art. 25. As aplicações de internet de entes do poder público devem buscar:
> I - compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;
> II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;
> III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;
> IV - facilidade de uso dos serviços de governo eletrônico; e
> V - fortalecimento da participação social nas políticas públicas.

14. Finalizando as citações da Lei nº 12.965/14, transcreve-se seu art. 15, que determina que determinados provedores de aplicações de internet deverão manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento:

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
> § 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no *caput* a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no *caput*, observado o disposto nos §§ 3º e 4º do art. 13.
> § 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
> § 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

15. Esse art. 15, em regra, conforme seu *caput,* não se aplicaria à AGR, que, por ser autarquia, não tem fins econômicos. Como exceção, entretanto, nos termos do § 1º desse artigo, a AGR, caso se configure como provedora de aplicações de Internet, pode ser obrigada a guardar registro de acesso a aplicações da Internet em relação à fatos específicos em período determinado.

16. Dito isso, passa-se às questões jurídicas relacionadas ao sistema proposto, com a indicação das normas pertinentes, não necessariamente na ordem cronológica, e análise da descrição de fls. 11/44.

17. A Medida Provisória nº 2.200-2, de 24 de agosto de 2001, que permanece em vigor por força do art. 2º da Emenda Constitucional nº 32/01, de 11 de setembro de 2001[6], instituiu a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil - para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras[7].

18. Essa Medida Provisória, em seu art. 10, considerou documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que ela trata, presumindo-se verdadeiros em relação aos signatários as declarações constantes nesses documentos produzidos com a utilização de processo de certificação disponibilizado pelo ICP-Brasil.

19. O § 2º desse mesmo artigo 10, entretanto, não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

20. Quanto ao Estado de Goiás, a Lei estadual nº 17.039/10 dispõe sobre a informatização e a digitalização dos processos e atos da Administração Pública Estadual e dá outras providências.

21. Nessa lei estadual (art. 2º, § 2º), nos moldes da Lei federal nº 11.419/06, que dispõe sobre a informatização do processo judicial, existe a definição do que seja assinatura eletrônica:

---

[6] Art. 2º As medidas provisórias editadas em data anterior à da publicação desta emenda continuam em vigor até que medida provisória ulterior as revogue explicitamente ou até deliberação definitiva do Congresso Nacional.

[7] Maiores detalhes sobre a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil - e a assinatura eletrônica podem ser obtidos no sítio www.iti.gov.br.

> Art. 2º O uso de meio eletrônico no registro e na comunicação de atos administrativos ou normativos, nas instruções processuais e na tramitação de processos administrativos da Administração Pública Estadual será admitido nos termos desta Lei.
> (...)
> § 2º Para o disposto nesta Lei, considera-se:
> (...)
> **II – assinatura eletrônica: as seguintes formas de identificação inequívoca do signatário:**
> **a) assinatura digital baseada em certificado digital emitido por autoridade certificadora credenciada, na forma de lei específica;**
> **b) cadastro de usuários junto à unidade de registro, conforme disciplinado em regulamento.** (destaque nosso)

22. Assim, coexistiriam, na Lei estadual nº 17.039/10, com validade jurídica, a assinatura digital baseada em certificado digital emitido por autoridade certificadora (ICP-Brasil) e a assinatura eletrônica na forma de cadastro de usuários junto à unidade de registro. Esta última dependeria de regulamentação por decreto que, até a presente data, não foi editado.

23. Sobre essa ausência de regulamentação, José dos Santos Carvalho Filho doutrina que, ultrapassado o prazo previsto para esse fim, a lei deve tornar-se exequível. Confira-se a lição do autor[8]:

> O Executivo não pode se eximir de regulamentar a lei no prazo que lhe foi assinado. Cuida-se de poder-dever de agir, não se reconhecendo àquele Poder mera faculdade de regulamentar a lei, mas sim dever de fazê-lo para propiciar sua execução. Na verdade, a omissão regulamentadora é inconstitucional, visto que, em última análise, seria o mesmo que atribuir ao Executivo o poder de legitimação negativa em contrário, ou seja, de permitir que sua inércia tivesse o condão de estancar a aplicação da lei, o que, obviamente, ofenderia a estrutura de Poderes da República.
> Com tal fundamento, se for ultrapassado o prazo de regulamentação sem a edição do respectivo decreto ou regulamento, a lei deve tornar-se exeqüível para que a vontade do legislador não se afigure inócua e eternamente condicionada à vontade do administrador.

24. E, como o art. 15 da Lei nº 17.039/10 fixa em até 60 (sessenta) dias contados da data de sua publicação o prazo para sua regulamentação, constata-se que tal prazo já expirou, pois a lei foi publicada em 25/06/10, sendo possível aplicá-la com determinadas cautelas[9],

---

[8] *In* Manual de Direito Administrativo, 19ª Ed., Editora Lumens Juris, Rio de Janeiro, 2008, p. 52.

[9] Dentre tais cautelas, além daquelas já citadas sobre a segurança da informação, mencionam-se as constantes nos parágrafos do art. 2º da Lei federal nº 11.419/06, que dispõe sobre a informatização do processo judicial:

Art. 2º O envio de petições, de recursos e a prática de atos processuais em geral por meio eletrônico serão admitidos mediante uso de assinatura eletrônica, na forma do art. 1º desta Lei, sendo obrigatório o credenciamento prévio no Poder Judiciário, conforme disciplinado pelos órgãos respectivos.
§ 1º O credenciamento no Poder Judiciário será realizado mediante procedimento no qual esteja assegurada a adequada identificação presencial do interessado.
§ 2º Ao credenciado será atribuído registro e meio de acesso ao sistema, de modo a preservar o sigilo, a identificação e a autenticidade de suas comunicações.

recomendando-se, entretanto, como melhor alternativa, que seja solicitado à Secretaria de Estado da Casa Civil providências para a referida regulamentação.

25. Oportunamente, informa-se que o Conselho Nacional de Justiça-CNJ, órgão do Poder Judiciário, por meio da Resolução nº 185, de 18/12/13, que institui o Sistema Processo Judicial Eletrônico (PJe) como sistema de processamento de informações e prática de atos processuais e estabelece os parâmetros para sua implementação e funcionamento, definiu, em seu art. 3º, I, a assinatura digital apenas como resumo matemático computacionalmente calculado a partir do uso de chave privada e que pode ser verificado com o uso de chave pública, estando o detentor do par de chaves certificado dentro da Infraestrutura de Chaves Públicas Brasileira (ICP-Br), na forma da legislação específica.

26. O CNJ, pois, não optou pelo cadastro de usuário como forma de assinatura eletrônica conforme previsto na Lei federal nº 11.419/06 cuja redação, nesse ponto, é similar à da Lei estadual nº 17.039/10. Corrobora essa afirmação o art. 36 da Resolução nº 185/13, do CNJ, que reza que "A partir da implantação do PJe, o recebimento de petição inicial ou de prosseguimento, relativas aos processos que nele tramitam, somente pode ocorrer no meio eletrônico próprio do sistema, sendo vedada, nesta hipótese, a utilização de qualquer outro sistema de peticionamento eletrônico, exceto nas situações especiais previstas nesta Resolução."

27. Em relação à assinatura eletrônica na forma de cadastro de usuários junto à unidade de registro, conforme previsto no art. 2º, § 2º, II, b, da Lei estadual nº 17.039/10, faz-se as seguintes considerações.

28. A validade jurídica de documentos em razão da forma de sua assinatura é matéria de direito civil, área cuja legislação é de competência privativa da União, nos termos do art. 22, I, da Constituição Federal, *in verbis*:

> Art. 22. Compete privativamente à União legislar sobre:
> I - direito civil, comercial, penal, processual, eleitoral, agrário, marítimo, aeronáutico, espacial e do trabalho;

---

§ 3º Os órgãos do Poder Judiciário poderão criar um cadastro único para o credenciamento previsto neste artigo.

29. Exercendo essa competência, a União editou a Medida Provisória nº 2.200-01/01 que, conforme já consignado, estabeleceu duas formas de validade de documentos com assinatura eletrônica: os documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil e os documentos produzidos com a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

30. Em relação a essa segunda forma, o Instituto Nacional de Tecnologia da Informação - ITI, em um Manual de Perguntas e Respostas Jurídicas, Capítulo 7 – Administração Pública e Certificação Digital, disponível em http://www.iti.gov.br/publicacoes/manuais#capitulo7, acesso em 18/05/16, responde as duas seguintes perguntas: "Um órgão ou entidade integrante da Administração Pública Federal que queira utilizar certificado digital somente em seu âmbito interno pode se valer de certificados emitidos por uma Autoridade Certificadora própria, gozando da mesma presunção de validade garantida aos certificados ICP-Brasil?" e "Órgãos e entidades públicas da esfera estadual e municipal podem utilizar certificados digitais emitidos por autoridades certificadoras não credenciadas pela ICP-Brasil?". Confira-se a transcrição das respostas às duas perguntas citadas:

> 51. Um órgão ou entidade integrante da Administração Pública Federal que queira utilizar certificado digital somente em seu âmbito interno pode se valer de certificados emitidos por uma Autoridade Certificadora própria, gozando da mesma presunção de validade garantida aos certificados ICP-Brasil?
>
> R: A resposta é negativa. Apenas o certificado da ICP-Brasil, e nenhum outro, gera a certeza da validade jurídica do documento eletrônico, pois se sabe, com garantia legal (MP 2.200-2/01, art. 1º), quem assinou (autenticidade) e que o documento não sofreu qualquer modificação entre o emissor e seu destinatário (integridade). Não significa dizer, porém, que não possam existir outros certificados. Não só podem como possuem expressa previsão nessa mesma Medida Provisória 2.200-2/01 (a partir de sua segunda edição), que dispõe em seu art. 10 §2º que "O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento." Ou seja, o destinatário de um documento eletrônico pode aceitar como válido qualquer certificado digital, ainda que não emitido pela ICP-Brasil. Porém, é justamente pela insegurança propiciada por esses outros certificados – que não possuem qualquer infraestrutura pública como o certificado ICP-Brasil possui – que se condicionou a sua validade (rectius: eficácia) à aceitação dos partícipes.

Esses outros certificados cuidam, portanto, de interesses privados, e não públicos (como o certificado ICP-Brasil cuida). Significa dizer, então, que se migra de um modelo de imposição legislativa (vez que o certificado digital ICP-Brasil tem sua validade obrigatoriamente reconhecida) para um modelo potestativo, de acreditamento, frágil por definição. Apesar de nesse passo a legislação brasileira ter seguido a Diretiva Européia 1.999/93, tal sistema de certificados digitais potestativos não é aconselhável. Isso porque o interessado em utilizá-los fica a depender da aceitação do outro contratante e, uma vez dada, ainda pode ser impugnada judicialmente, sob a alegação, por exemplo, de qualquer vício de consentimento (coação, erro). A justificativa para a existência do certificado, que é justamente dar segurança aos seus usuários, acaba por desaparecer, podendo ser transformada em um longo e desgastante processo judicial. Porém, essa possibilidade teórica de utilização de outros certificados que não da ICP-Brasil - não atinge os órgãos e entidades da Administração Pública Federal, direta e indireta, haja vista a existência do Decreto 3.996/01, que, em seu art. 2º, é expresso ao dizer que "os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil"

Assim, à Administração Pública Federal, apenas é permitida a utilização do certificado ICP-Brasil, e nenhum outro, ainda que seja apenas para o âmbito interno de utilização, pois somente essa infraestrutura confere a segurança jurídica necessária ao desempenho das relevantes funções públicas exercidas. Portanto, conclui-se respondendo que pelos princípios constitucionais da legalidade (CF/88, art. 37) e segurança jurídica (CF/88 art. 5º, caput), apenas o certificado digital ICP-Brasil pode ser utilizado para as finalidades desejadas pela Administração Pública Federal.

52. Órgãos e entidades públicas da esfera estadual e municipal podem utilizar certificados digitais emitidos por autoridades certificadoras não credenciadas pela ICP-Brasil?

R: As mesmas considerações realizadas para a utilização de certificados no âmbito federal, respondidas acima, podem ser aproveitadas aqui, com uma diferença. Enquanto na órbita federal o Decreto n° 3.966/01 proíbe qualquer certificado digital diverso daquele emitido pela ICP-Brasil, na esfera Estadual e Municipal a sua utilização, teoricamente, seria possível. Entretanto, não é aconselhável, haja vista a insegurança propiciada por esses outros certificados que, além de não possuir qualquer infraestrutura pública como o certificado ICP-Brasil, condicionou a sua eficácia à aceitação dos partícipes. Mas não apenas. Compete privativamente à União legislar sobre direito civil, conforme expresso mandamento contida na CF/88, art. 22, inc. I. E o certificado digital, ao conferir validade jurídica às manifestações eletrônicas, trata, justamente, da teoria geral do direito, que, no Brasil, está contida na parte geral do Código Civil. Assim, sob a ótica da competência legislativa, os Estados e Municípios ver-se-iam impedidos de dispor diferentemente a respeito da utilização de certificados digitais que não os da ICP-Brasil. Pela simetria, ainda, não teria sentido o modelo federativo brasileiro adotar soluções diferentes para a mesma questão da validade dos documentos eletrônicos, fato esse que, sem dúvida alguma, aponta para a utilização obrigatória dos certificados digitais ICP-Brasil para os Estados e Municípios, que sempre visam o interesse público e não privado, devendo sempre observar, também, aos princípios da legalidade (CF/88, art. 37) e da segurança jurídica (CF/88, art. 5º, caput). A possibilidade de utilização de certificados digitais outros fica deferida, apenas, às relações privadas, inter-partes.

31. Dessas respostas, três conclusões, sob a ótica do ITI, são extraídas:

a) a utilização de cadastro de usuários como forma de se produzir documentos assinados eletronicamente é possível, com fundamento no § 2º do art. 10 da MP nº 2.200-02/01, mas tais documentos não têm a mesma presunção de validade garantida aos certificados ICP-Brasil e sua eficácia depende da aceitação das partes;

b) os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil - por força do art. 2º do Decreto nº 3.996/01;

c) Estados e Municípios não podem legislar sobre direito civil, o que incluiria assinatura digital de documentos e, por simetria, em razão do interesse público e dos princípios da legalidade e da segurança jurídica, deveriam utilizar os certificados digitais ICP-Brasil. Outros certificados digitais devem ser usados apenas às relações privadas, inter-partes.

32. Sobre a conclusão do item 31, c, observa-se que o Estado de Goiás, optando por utilizar o cadastro de usuários para assinatura digital de documentos (art. 2º, § 2º, II, b, da Lei estadual nº 17.039/10), não estaria legislando sobre matéria de competência da União e, sim, utilizando a possibilidade prevista no § 2º do art. 10 da MP nº 2.200-02/01.

33. Expressamente, a MP nº 2.200-02/01 não dispõe que os outros certificados não emitidos pelo ICP-Brasil não poderiam ser utilizados pela administração pública estadual e municipal.

34. Entretanto, esse cadastro de usuários, reconheça-se, nos termos das respostas do ITI já transcritas, não tem a mesma presunção de validade garantida aos certificados ICP-Brasil, possuindo validade desde que admitido pelas partes ou aceito pela pessoa a quem for oposto o documento. Possuem, portanto, menor grau de segurança jurídica.

35. Nesses termos, considerando que a AGR é uma autarquia e, como tal, sujeita ao regime jurídico de direito público, o mais recomendado, para assinatura eletrônica de documentos em um sistema eletrônico próprio, é a utilização de certificado emitido pelo ICP-Brasil, restando, porém, a avaliação do custo-benefício desse tipo de assinatura digital levando-se em conta, dentre outros fatores, o porte das empresas que utilizarão o Cadastramento Eletrônico e o tempo que os documentos produzidos produzirão efeitos.

36. Em relação ao termo de adesão de fls. 03/05, cabem as seguintes observações.

37. Primeiramente, observa-se que a base do referido termo de adesão coincide com o termo de adesão ao sistema e-INPI, que é um sistema eletrônico de gestão de propriedade industrial do Instituto Nacional de Propriedade Industrial, disponível em http://formulario.inpi.gov.br/e-inpi/termo/Termo.jsp?action=28, acesso em 18/05/16.

38. Quanto aos itens do termo de adesão proposto, recomenda-se o seguinte:

a) em razão da abrangência que se pretende dar ao sistema, sugere-se alterar seu nome para, por exemplo, e-AGR – Sistema Eletrônico AGR, já que o objetivo não é somente o cadastro eletrônico de empresas, mas sim outros cadastros como o de veículos e de autorização de viagem. Caso acatada essa sugestão, deve-se providenciar a mudança do nome do sistema em todo o termo de adesão;

b) no item 1: substituir "... , DO USUÁRIO" por "... E DO USUÁRIO";

c) no item 1.2: escrever "... de Cadastro ..." ao invés de "... da Cadastro ..." e escrever "... Serviços Públicos – AGR, autarquia estadual criada em 1999, vinculada ..." ao invés de "... Serviços Públicos, Autarquia Estadual – AGR, criada em 1999, vinculada ...";

d) no item 1.4: no lugar do texto proposto, escrever "Considera-se USUÁRIO o próprio interessado, pessoa física ou jurídica (AUTORIZATÁRIO, PERMISSIONÁRIO, CONCESSIONÁRIO e outros), que pode atuar na AGR sem a intermediação de terceiros, e o seu representante legal habilitado perante a AGR";

e) sobre os itens 2.1 e 2.2, deve-se, preliminarmente, estudar o custo-benefício da adoção da assinatura eletrônica baseada em certificação digital emitida pelo ICP-Brasil, nos termos dos itens 16 a 35 desse parecer, ou adotar-se o cadastro de usuários ou, ainda, adotar-se, preferencialmente, a assinatura eletrônica baseada em certificação digital emitida pelo ICP-Brasil e, em caráter secundário, o cadastro de usuários, como fez INPI em seu sistema e-INPI.

Nessa última hipótese, considera-se adequado, para o texto do item 2.1, o seguinte:

> "2.1. O acesso ao sistema e-AGR é efetuado mediante 'login' e senha, que constitui sua identificação eletrônica. A habilitação do 'login' e senha de acesso ao sistema e-AGR se dá por meio de identidade digital, adquirida perante qualquer autoridade certificadora credenciada pelo ICP-BRASIL".

Como consequência, deve-se substituir o texto do item 2.2 pelo seguinte:

> "2.2. O USUÁRIO que não possuir identidade digital pode obter a habilitação do 'login' e senha de acesso por meio de cadastramento do usuário e entrega presencial, na sede da AGR (Av. Goiás, nº 305, Ed. _____ , Sala ____ , telefone _____Setor Central, Goiânia-GO), de toda a documentação obrigatória exigida, que será validada e arquivada juntamente com uma via assinada desse Termo de Adesão."

Ainda, deve-se compatibilizar a redação desse item 2.2 com a do item 2.5.

f) o item 2.4 deve ter a seguinte redação: "Ao aderir a este Termo, o USUÁRIO deverá ser o representante legal da empresa para utilização dos serviços diretamente com a AGR." Isso em razão de que, quando se fala em representante legal, esse somente pode ser pessoa com capacidade civil, o que incluiu menores emancipados, motivo pelo qual não se vislumbra a necessidade de mencionar-se menores ou emancipados;

g) no item 2.5, substituir "escolherá" por "terá". Nesse item é mencionado uma Resolução da AGR, que ainda será elaborada, sobre a qual recomenda-se, no momento oportuno, que seu conteúdo seja mencionado em outras resoluções da AGR como a Resolução nº 005/08-CG, que dispõe sobre a regulamentação de prestação de serviços de fretamento no transporte rodoviário intermunicipal de passageiros do Estado de Goiás;

h) no item 2.6 deve-se substituir a expressão "A escolha do ..." por "O", já que não se trata de escolha e sim de imposição;

i) no item 2.7, escrever " ... (e-mail)..." ao invés de "... :e-mail,...". Separar "deserviços" e acrescentar crase ao "a" de "... a AGR...";

j) no item 2.8.B, deve-se acrescentar, após "sentido", a expressão ", observada, nesse último caso, a vedação do inciso III do art. 4º da Lei estadual nº 18.025, de 22 de maio de 2013, e outras vedações

legais.” A Lei estadual nº 18.025/13, que dispõe sobre o acesso a informações e a aplicação da Lei federal nº 12.527, de 18 de novembro de 2011, no âmbito do Estado de Goiás, institui o serviço de informação ao cidadão e dá outras providências, assim dispõe nesse art. 4º, III:

> Art. 4º O direito de acesso a informações de que trata esta Lei será franqueado às pessoas naturais e jurídicas, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão, vedada a sua aplicação:
> (...)
> III - às informações relativas a atividade empresarial de pessoas físicas ou jurídicas de direito privado obtidas pelas agências reguladoras ou por outros órgãos ou entidades no exercício de atividade de controle, regulação e supervisão da atividade econômica cuja divulgação possa representar vantagem competitiva a outros agentes econômicos;

k) no item 3.3.F, é preciso compatibilizar sua redação com a redação do item 2.2 sugerida na letra “e”, já que, no caso do usuário não ter certificação digital, os documentos deverão ser entregues presencialmente. Assim, sugere-se excluir a palavra “digitalmente’ desse item 3.3.F;

l) o item 4.1.E deve ser renumerado para item 4.2, deve ser retirada a vírgula após “contratados” e acrescentado, antes de “força maior”, a expressão “caso fortuito”. Sem se adentrar na distinção entre esses fenômenos feita por diversos autores, muitas vezes de forma não coincidente, informa-se que, para o Direito Civil, não há interesse público na distinção dos conceitos, até porque o Código Civil Brasileiro (Lei nº 10.406/02) não a fez conforme a redação de seu art. 393:

> Art. 393. O devedor não responde pelos prejuízos resultantes de caso fortuito ou força maior, se expressamente não se houver por eles responsabilizado.
> Parágrafo único. O caso fortuito ou de força maior verifica-se no fato necessário, cujos efeitos não era possível evitar ou impedir.

m) o item 4.2 deve ser renumerado para 4.3, assim como seus subitens;

n) em relação ao item 5.1, esclarece-se que a proteção aos direitos sobre o sistema pela legislação própria ocorre desde a data de sua criação[10], mas para se ter maior segurança jurídica quanto à essa

[10] A Lei nº 9.609/98, em seu art. 2º, § 3º, dispõe:
Art. 2º O regime de proteção à propriedade intelectual de programa de computador é o conferido às obras literárias pela legislação de direitos autorais e conexos vigentes no País, observado o disposto nesta Lei.
(...)
§ 3º A proteção aos direitos de que trata esta Lei independe de registro.

proteção é necessário documentar-se a data dessa criação, o que pode ocorrer pelos seguintes meios[11], listados na ordem de menor para maior custo:

- auto-enviar um e-mail, a fim de que fiquem registradas no servidor, com aquela determinada data, informações sobre as imagens transmitidas;

- é possível proteger o *layout* das páginas de um *website* com o simples registro na Biblioteca Nacional ou no Cartório de Títulos e Documentos, com o pagamento respectivo;

- também é possível a remessa dos códigos-fonte por Sedex lacrado para o endereço do próprio desenvolvedor. Nesse caso, o desenvolvedor deve manter guardado o envelope lacrado até que, eventualmente, haja necessidade de utilizá-lo para solucionar problemas judiciais ou outros litígios, nos quais seja necessário comprovar a data de autoria;

- por fim, a maior segurança jurídica é obtida com a solicitação de registro de programa de computador no Instituto Nacional de Propriedade Industrial – INPI – com pagamento de taxas.

o) no item 6.1 deve-se excluir "..., desses novos termos e condições" por ser redundante;

p) o item 7.1 deve ter a seguinte redação: "7.1. Eventuais desavenças ou litígios entre o USUÁRIO e a AGR serão submetidos à prévia análise da área técnica, que emitirá parecer opinativo sobre a questão, para posterior decisão do Conselho Regulador da AGR." Justifica-se essa redação sugerida em razão do disposto nos seguintes dispositivos da Lei estadual nº 13.569/99, transcritos à seguir:

> Art. 11. O Conselho Regulador da AGR é a autoridade pública revestida dos poderes legais para exercer a regulação, o controle e a fiscalização da prestação dos serviços públicos e do exercício de atividades econômicas de competência do Estado de Goiás, concedidos, permitidos, autorizados ou delegados sob qualquer forma a terceiros para exploração, dirigindo para esse fim a estrutura executiva da Agência Goiana de Regulação, Controle e Fiscalização de Serviços Públicos, sendo suas principais atribuições:
>
> I - apreciar e deliberar sobre as normas de funcionamento da AGR;
> (...)
> III – analisar e aprovar normas, regulamentos gerais e específicos para a regulação, o controle e a fiscalização da prestação de serviços, tendo por base a Constituição, as leis e decretos, compreendendo as suas dimensões técnica, econômica e social, que abrangerão, pelo menos, os seguintes aspectos:
> (...)
> b) requisitos operacionais e de manutenção dos sistemas;
> (...)
> VIII – deliberar sobre quaisquer questões afetas às atividades de regulação, controle e fiscalização dos serviços públicos regulados, controlados e fiscalizados, apresentadas pelo Conselheiro Presidente;

[11] Sugestões extraídas do artigo Como proteger seu software sem gastar muito, disponível em https://webinsider.com.br/2006/11/24/como-proteger-o-seu-software-sem-gastar-muito/, acesso em 18/05/16.

> (...)
> IX – fixar procedimentos administrativos relacionados com o exercício das competências da AGR.
> (...)
> § 4º Compete ao Conselho Regulador da AGR deliberar, com exclusividade e independência decisória, sobre todos os atos de regulação, controle e fiscalização inerentes à prestação dos serviços públicos concedidos, permitidos ou autorizados.

q) no item 7.2, substituir os dois pontos (:) por hífen (-). Além disso, substituir "... da Seção Judiciária Estadual do Município de Goiânia" por "... da Comarca de Goiânia-GO." em razão dessa estrutura de Seção Judiciária ser própria da Justiça Federal (existe uma Seção Judiciária da Justiça Federal em cada Estado) e a AGR sem demandada, em regra, na justiça estadual.

38. Especificamente em relação à nota fiscal eletrônica, embora o art. 21, II, da Resolução nº 005/08-CG, a exija, informa-se que o Gerente de Informações Econômico-Fiscais da Secretaria de Estado da Fazenda, por meio do Ofício nº 0168/2016-GIEF, informou que prorrogou o prazo para sua exigência até 31/12/16 em virtude de inviabilidade técnica, razão pela qual deve-se mencionar, ao invés de "nota fiscal eletrônica", "nota fiscal exigida pela legislação pertinente".

39. Em relação aos documentos que as empresas devem encaminhar eletronicamente para a AGR por meio de *upload* no módulo e-Licença, conforme consta nas fls.19 e 35, deve-se garantir sua autenticidade nos termos dos itens 16 a 35 desse parecer.

40. Por fim, quanto aos documentos certificado de registro cadastral (fl. 30), certificado de registro de veículo (fl. 34) e licença de viagem (fl. 44), os mesmos devem ser assinados eletronicamente pela autoridade competente por uma das duas formas possíveis, já explicitadas, preferindo-se a utilização de processo de certificação disponibilizado pelo ICP-Brasil. Em qualquer caso, deve-se inserir um texto ao final de cada documento com a informação de que ele foi assinado eletronicamente e a forma de sua validação.

41. Ante o exposto, reconhecendo a excelência do trabalho desenvolvido pela Coordenação de Informática da AGR, conclui-se:

a) que a legislação reconhece valor jurídico às assinaturas digitais, garantindo a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações

eletrônicas seguras, por meio da utilização de processo de certificação disponibilizado pelo ICP-Brasil, que é o recomendado e possui maior segurança jurídica;

b) que é possível a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento, como o cadastro de usuários junto à unidade de registro, conforme disciplinado em regulamento, ainda não editado,

c) que a ausência de regulamento do cadastro de usuários junto à unidade de registro não impede sua utilização, nos termos dos itens 23 e 24 desse parecer, recomendando-se, entretanto, caso opte-se por sua utilização, que seja solicitado à Secretaria de Estado da Casa Civil providências para a referida regulamentação;

d) que o termo de adesão de fls. 03/05 necessita das adequações descritas nos itens 37 e 38 desse parecer;

e) que o sistema proposto deve seguir as recomendações desse parecer, inclusive as dos itens 39 e 40.

Submeta-se à apreciação da Gerente Jurídica da AGR.

Gerência Jurídica, em Goiânia-GO, aos 18 dias do mês de maio de 2016.

Evandro Arantes Faria
Gestor Jurídico
OAB/GO nº 46.057

A