



Documento de identidade digital da Justiça Eleitoral

Por: Carlos Rogério Camargo *

Introdução

Considere as operações em um caixa eletrônico para realizar uma transação bancária. Suponha que o banco ofereça um cartão com *chip* (*smart card*), uma senha pessoal e tenha colhido sua impressão digital. Após inserir o cartão na leitora, o usuário é orientado a digitar sua senha e, em seguida, colocar seu dedo polegar ou indicador em uma leitora de impressão digital. Confirmada a identidade, o sistema autoriza-o a executar a transação.



O modelo de autenticação descrito contém os três elementos de um processo de autenticação seguro, também denominada autenticação forte (Li, Chun-Ta, *et al*, 2010). Ele é baseado em: (a) algo que você tem: o cartão, (b) algo que você sabe: a senha, e (c) algo que você é: sua impressão digital. Por intermédio desse processo é confirmada a identidade de uma pessoa, requisito à autorização para que ela execute a transação desejada.

Há variantes dessa modalidade de autenticação, combinando pelo menos dois desses três elementos. Nas transações comerciais, os cartões combinam somente "a" e "b". Por exemplo, para a maior parte das operações de compra, bastam a posse do cartão e o conhecimento da senha. Transações mais seguras de alguns bancos podem exigir também a conferência das impressões digitais. Os elementos desse processo de autenticação realizado pelo usuário são o cartão digital, com os dados do seu portador em formato digital, e um terminal conectado à instituição financeira.

Imagine, agora, um documento de identidade com *chip*, com aparência semelhante a um cartão de crédito. Nele estão contidos os dados de um documento de identidade tradicional (visíveis) e um certificado digital, armazenado em sua memória interna, com dados adicionais para a identificação do seu titular. Com ele é possível realizar os processos de autenticação similares aos dos cartões de crédito, além da autenticação tradicional pela verificação da semelhança da foto e da assinatura (escrita) do seu portador. Trata-se, portanto, de um documento versátil que suporta diversos métodos de autenticação, presenciais ou remotos.

Com essas características, o documento de identidade digital permite a automação de dezenas de serviços, inclusive pela *web*, semelhante aos disponíveis por cartão de crédito. O e-CPF, comercializado por empresas privadas, é um exemplo de documento de identidade digital aceito perante a Receita Federal. Com o e-CPF é possível acessar sistemas e realizar diversas operações fiscais pela *web*, sem a necessidade de comparecer aos escritórios da Receita Federal (Receita Federal, Portal e-CAC).

Dessa forma, neste artigo são abordadas as vantagens do uso do documento de identidade digital pela Justiça Eleitoral, com destaque para a operação de autenticação do eleitor nas eleições. Como será demonstrado, a automação da autenticação do eleitor reduzirá o tempo de votação e, em consequência, contribuirá para significativa redução do número de seções eleitorais, com repercussões relevantes nos custos das eleições.

Argumenta-se no artigo, também, que a Justiça Eleitoral é o órgão público federal que reúne as melhores condições para produzir o documento de identidade digital, em substituição ao título eleitoral. Ela administra o maior cadastro de pessoas do Brasil, com informações biográficas de mais de 140 milhões de eleitores. Desde

2008, vem promovendo intenso trabalho para o cadastramento dos dados biométricos (foto e impressões digitais) desses eleitores. Além disso, é a instituição que possui a maior capilaridade entre todos os órgãos públicos federais, com cartórios eleitorais em 3.033 municípios, com jurisdição plena sobre os 5.737 municípios brasileiros, cobrindo todo o território nacional. Portanto, possui os elementos necessários à produção e facilidades para a distribuição do documento de identidade digital.

Por fim, pretende-se demonstrar que o uso do documento de identidade digital vai propiciar a racionalização dos processos de atualização dos dados dos eleitores no cadastro eleitoral. Como regra geral, as impressões digitais dos eleitores serão colhidas exclusivamente no alistamento, para integrar o cadastro nacional. Nas demais operações – revisão, transferência ou segunda-via – faz-se a identificação do eleitor mediante uso do documento de identidade digital. Somente nos casos de revisão dos dados de identificação dos eleitores ou após o vencimento do prazo de validade é que se cogitará a geração de um novo documento de identidade digital.

1 Detalhamento do problema

1.1 Autenticação com documento de identidade tradicional

A autenticação com o documento de identidade tradicional é realizada por meio da conferência dos dados pessoais, da verificação da semelhança entre a aparência e a foto e, eventualmente, da confrontação da assinatura com a constante no documento de identidade. Esse processo é denominado “autenticação por semelhança e autenticidade” (CPC, art. 369).

A autenticação é requerida em diversas situações da vida dos cidadãos: na abertura de contas bancárias, na solicitação do título eleitoral, na matrícula em escolas, no acesso a prédios públicos ou clubes, entre dezenas de outras. O grau de complexidade do processo é determinado pelo nível de segurança exigido para autorizar a operação. Por exemplo, na compra ou venda de um imóvel é necessário que as partes envolvidas na transação compareçam a um cartório e, perante o escrivão, aponham na escritura suas assinaturas, as quais serão confrontadas com os documentos de identidade. Por outro lado, no acesso a um prédio, a autenticação é mais simples, bastando, como regra, apresentar o documento de identidade.

Nas eleições brasileiras, a autenticação do eleitor é semelhante àquela realizada em transações imobiliárias, com o mesário desempenhando o papel do escrivão (Manual do Mesário, Eleições/2012). O eleitor comparece à sua seção eleitoral com um documento de identidade e assina no caderno de votação. Cumpre ao mesário verificar a semelhança entre as assinaturas e a aparência do eleitor, confrontando com os dados do documento de identidade.

A segurança do processo, portanto, é baseada na diligência e na boa-fé dos mesários e dos eleitores. A presunção é de que as partes são sérias, atentas e bem intencionadas. No entanto, sabe-se que uma parcela, ainda que pequena, dos mesários não tem a formação adequada nem a competência técnica para executar essa operação de autenticação com eficiência. Os eleitores, valendo-se da desatenção (ou contando com a colaboração) dos mesários, podem votar no lugar de outro eleitor. Mesmo os mesários, que detêm a guarda da urna durante todo o dia das eleições, em conluio ou por iniciativa individual, podem fraudar a eleição votando no lugar de eleitores da seção.

Logo, esse método de autenticação, baseado exclusivamente na confiança nas pessoas, não é avaliado seguro. O que se busca é um método com o máximo de automação e o mínimo de intervenção humana, prescindindo, inclusive, da interferência dos mesários. Em outras palavras, o que se propõe é um método de autenticação semelhante àquela realizado perante um terminal bancário de autoatendimento com biometria.

1.2 Impressão digital para confirmar a identidade do eleitor

A confirmação da identidade do eleitor por meio da sua impressão digital é um método seguro de autenticação (Jain, Anil K. *et alii*). A formação pela Justiça Eleitoral do cadastro dos eleitores com informações biométricas contribuirá para o aumento da segurança do processo eleitoral. A generalização desse método de autenticação vai reduzir o risco de fraude de identidade, ou de um eleitor votar no lugar de outro.

No processo atual, a biometria é colhida *após* a identificação do eleitor pelo mesário. O processo de identificação é executado pelo mesário que, de posse do

documento de identidade do eleitor, localiza o número do seu título eleitoral e o digita no terminal do mesário. Portanto, a biometria é utilizada para confirmar a identidade do eleitor. Esse fato tem repercussões relevantes na logística do processo.

Ainda, caso não seja possível a identificação biométrica do eleitor (hipótese em que a impressão digital não é reconhecida, também chamada de falso-negativo), o mesário tem a prerrogativa de autorizar o voto do eleitor.

1.3 Os problemas do método atual de autenticação com biometria

As consequências mais importantes do processo atual de autenticação com biometria, e que compõem o principal problema a ser tratado neste artigo, são:

- a) O processo atual não elimina o risco de fraudes de falsa identidade, passíveis de ser praticadas pelos mesários; e
- b) O considerável aumento do tempo para a operação de autenticação do eleitor.

No método atual de autenticação com biometria, o mesário continua detendo o controle sobre todo o processo. Cabe a ele fazer a identificação do eleitor perante a urna eletrônica – digitando o número do título eleitoral – e conduzir as demais operações, quais sejam:

- a) Conferência dos dados pessoais do eleitor;
- b) Localização dos dados do eleitor no caderno de votação;
- c) Coleta da impressão digital do eleitor.

Embora se reconheça o aumento da segurança do processo, vê-se que não foi eliminado o risco de fraudes passíveis de ser feitas pelos mesários, que continuam podendo inserir votos em nome de eleitores inscritos na seção. É evidente que a possibilidade dessa fraude ser detectada é maior porque, para habilitar o eleitor a votar, é necessário esgotar as tentativas de leitura de sua impressão digital. Contudo, o mesário continua tendo, em tese, os meios de lançar votos fraudulentos na urna eletrônica, ainda que incorra em maior probabilidade de o fato ser detectado.

Outro efeito indesejado relevante do atual processo de autenticação com biometria é o aumento do tempo de votação. Nas eleições gerais de 2010, o tempo dispendido com autenticação nas seções eleitorais com biometria foi maior (v. Tabela 1), passando para 40 segundos, enquanto nas seções sem biometria foi de 25 segundos, ou seja, um aumento de 15 segundos por eleitor.¹

	São João Batista	Santa Catarina
Autenticação	40 (média=52)	25 (média=43)
Votação	98 (média=114)	83 (média=103)

Tabela 1 – Tempos (em segundos) de autenticação e de votação nas eleições 2010, considerada a mediana.

Portanto, a adoção da biometria como método de autenticação dos eleitores, além de não eliminar o risco de fraudes, ainda gerou ineficiência no processo eleitoral.

2 Solução sugerida

2.1 Modelo de autenticação proposto

O cenário que se desenha como solução para a autenticação do eleitor é semelhante àquele aplicado a um cliente bancário em um terminal de autoatendimento com biometria. Esse modelo prescinde da participação do mesário, pois a identificação do eleitor perante a urna eletrônica se dá por meio da leitura dos dados diretamente do documento de identidade digital. Assim, o processo ocorre da seguinte forma:

- a) O eleitor introduz o documento de identidade digital no leitor de cartões;
- b) O sistema identifica o eleitor e verifica se ele está regularmente inscrito na seção eleitoral;
- c) Caso o eleitor esteja regularmente inscrito na seção,² o terminal orienta-o para a coleta da impressão digital;

d) Reconhecida a impressão digital e confirmada a identidade do eleitor, ele é autorizado a votar.

Essa é a regra geral, que tem como requisito a necessidade de o eleitor estar de posse do seu documento de identidade digital. Neste caso, o papel do mesário se resume a organizar o funcionamento da seção (e.g. fila de eleitores, orientação aos eleitores, etc.) e a fiscalizar a regularidade da votação.

Restam as hipóteses de contingência para os casos de:

- a) A impressão digital do eleitor não ser reconhecida (falha na operação “d”); e
- b) O eleitor não portar o documento de identidade digital.

No primeiro caso, o sistema fez a identificação do eleitor, lendo os seus dados diretamente do documento de identidade digital, mas a operação de autenticação falha no reconhecimento biométrico. Esgotadas as possibilidades de confirmar a identidade do eleitor por meio do reconhecimento biométrico, é necessário um processo de autenticação complementar, realizado pelo mesário, para atestar a veracidade da identidade do eleitor.

No segundo caso, uma vez que ele não esteja de posse do documento de identidade digital, não é possível a identificação automática do eleitor perante a urna eletrônica. Nessa hipótese, para autorizá-lo a votar deve ser adotado o método tradicional de autenticação por semelhança, com algum outro documento de identidade, facultando ao mesário autorizar o voto do eleitor. Nessa situação, retorna o risco de fraudes passíveis de prática pelo mesário.

O protocolo de autenticação do eleitor cuja impressão digital não pôde ser reconhecida envolve as seguintes operações:

- a) Confirmada a impossibilidade de leitura da impressão digital, o sistema orientará o eleitor a chamar o mesário;
- b) O mesário fará, então, a identificação do eleitor nos moldes tradicionais, colhendo a sua assinatura em documento próprio, que integrará a ata da seção;
- c) Em seguida, o mesário introduzirá o seu documento de identidade digital e autorizará o eleitor a votar.

No documento próprio também constará a identificação do mesário que avalizou a identidade do eleitor. Destacam-se as medidas de segurança desse protocolo:

- a) O eleitor e o mesário são identificados nessa operação;
- b) O voto só é autorizado se estiver vinculado a um eleitor, com o respectivo documento de identidade digital.

Com estas medidas, elimina-se o risco de o mesário votar no lugar de um eleitor. Além disso, ficam registradas na urna eletrônica as informações das partes envolvidas para a hipótese de auditoria.

2.2 Revisão do modelo de funcionamento da seção eleitoral

No modelo atual, com ou sem biometria, a autenticação do eleitor é a atividade principal do mesário durante todo o período de votação. Com a reformulação sugerida desse processo, restarão poucas atividades a demandar a sua atuação direta ao longo do dia.

Assim, as atribuições dos mesários serão as seguintes:

- a) Instalação da seção eleitoral (configuração das urnas eletrônicas e execução do ritual de abertura dos trabalhos de votação);
- b) Organização do funcionamento da seção eleitoral (ordem de votação, supervisão da fila de eleitores, etc.);
- c) Fiscalização da regularidade do processo de votação; e
- d) Como contingência, autorização do voto dos eleitores cuja impressão digital não pôde ser reconhecida automaticamente;
- e) Encerramento dos trabalhos de votação (totalização dos votos da seção e publicação do resultado); e
- f) Desinstalação da seção eleitoral, com a remessa dos equipamentos para a Justiça Eleitoral.

Em vista disso, parece certo que se pode cogitar a completa reformulação do funcionamento das seções eleitorais. No entanto, o detalhamento dessa reformulação está além do escopo deste artigo.

3 Etapas para a implantação do documento de identidade digital

A Justiça Eleitoral brasileira tem larga experiência na gestão do cadastro eleitoral com informações biográficas dos eleitores. O cadastro informatizado foi criado em 1986 e alcança, atualmente, mais de 140 milhões de eleitores. Em 2008, iniciou a coleta dos dados biométricos (a fotografia do eleitor, com registros biométricos da face, e as impressões digitais de todos os dedos das mãos), tendo cadastrado pouco mais de 20 milhões de eleitores.

Nesta seção será abordada a reformulação dos processos de gerenciamento do cadastro de eleitores, considerando a geração e o uso do documento de identidade digital. Recomendar-se-á, também, que seja facultado ao eleitor realizar algumas dessas operações via *web*, nos mesmos moldes do que hoje é feito com o e-CPF. A reformulação proposta vai reduzir o tempo de atendimento dos eleitores, aumentar a produtividade e, conseqüentemente, reduzir o custo do processo.

3.1 Dificuldades da coleta dos dados biométricos

Atualmente, as impressões digitais são colhidas em todas as operações do cadastro eleitoral (alistamento, revisão dos dados pessoais e transferência de domicílio), exceto em pedidos de segunda-via do título eleitoral, mesmo que o eleitor já tenha colhido sua impressão digital no alistamento. Essas coletas de dados biométricos redundantes seriam desnecessárias, se fosse adotado outro processo de autenticação do eleitor para as operações de revisão, transferência ou segunda-via.

A operação de coleta dos dados biométricos envolve a alocação de razoável quantidade de recursos humanos e de equipamentos (leitoras da impressão digital, máquinas fotográficas e *pad* para assinatura). O tempo para o cadastramento com biometria é da ordem de 6 minutos por eleitor.³ Desse tempo, em torno de 34% é para o cadastro biográfico, enquanto o restante é para a coleta da impressão digital (44%), assinatura (12%) e foto (9%). A variabilidade do tempo de atendimento é alta e decorre de diversos fatores, com destaque para:

- a) Baixa definição da imagem da impressão digital, decorrente de causas variadas (idade, manuseio de produtos químicos agressivos, etc.);
- b) Eleitor com dificuldade de assinar o seu nome no *pad*;
- c) Curva de aprendizado inicial do operador; e
- d) Processo não adequadamente padronizado para a realização dessas operações.

Como se trata de um processo de cadastramento de milhões de pessoas, realizado por milhares de operadores, nas mais diversas condições ambientais, é normal a alta variabilidade no tempo de cadastramento. No entanto, é esperada alguma redução desse tempo com treinamentos adequados e padronização dos processos de coleta.

Em Santa Catarina, no ano de 2013, foram realizadas 243 mil operações no cadastro eleitoral (v. Tabela 2 – Operações no cadastro eleitoral em Santa Catarina no ano de 2013), das quais perto de 32% eram de alistamento. Portanto, caso a coleta dos dados biométricos tivesse ocorrido em todo o Estado naquele ano, o que não ocorreu,⁴ a coleta repetida da impressão digital poderia ser evitada em 164 mil operações (67,5% do total), caso se adotasse outro método de autenticação do eleitor.

Operação	Quantidade	%
Alistamento	77.354	31,8%
Transferência	61.802	25,4%
Revisão	102.422	42,1%
Segunda-via	1.425	0,6%
Total	243.003	

Tabela 2 - Operações no cadastro eleitoral em Santa Catarina no ano de 2013.

Do ponto de vista operacional, a melhor alternativa para a autenticação do eleitor nas operações de transferência, revisão ou segunda-via é com o documento de identidade digital.

3.2 Geração do documento de identidade digital

Após o alistamento do eleitor com a coleta dos dados biométricos, a Justiça Eleitoral dispõe dos dados necessários à produção do documento de identidade digital. Com essas informações é possível gerar também o certificado digital, que integra o documento de identidade digital.⁵

Para a geração do certificado digital é necessário que a Justiça Eleitoral constitua uma Autoridade Certificadora (AC), subordinada à Infraestrutura de Chaves Públicas-Brasil (ICP-Brasil). Neste modelo, os cartórios eleitorais funcionariam como Autoridades de Registro (AR), os entes responsáveis pela identificação inicial dos eleitores e pela distribuição dos documentos de identidade digital.

Dessa forma, os documentos de identidade digital poderiam ser utilizados para a autenticação e assinatura digital de documentos (instrumentos públicos ou particulares). Os documentos assinados com esses certificados digitais têm validade jurídica, pois atendem à legislação vigente que regula a matéria (Medida Provisória 2.200-2). Do mesmo modo, o documento de identidade digital permitiria a autenticação remota, viabilizando o acesso a sistemas informatizados. Assim, seria possível, por exemplo, que o eleitor fizesse o requerimento das operações de transferência, revisão ou segunda-via por meio da *web*, nos mesmos moldes dos serviços oferecidos pela Receita Federal com o e-CPF.

4 Outros usos para o documento de identidade digital

É certo que o documento de identidade digital poderá vir a ser adotado em uma dezena de serviços informatizados. As aplicações mais evidentes são:

- a) Serviços na *web*: acesso aos serviços públicos que possam ser automatizados e oferecidos na *web*;
- b) Controle de acesso ou de ponto: registro automatizado do acesso de pessoas em órgãos públicos, empresas, instituições de ensino, clubes, etc.

Esses serviços são de interesse da maior parte dos órgãos públicos (federais, estaduais, municipais), empresas privadas, etc. Algumas dessas entidades desenvolvem sistemas próprios com essa tecnologia. Por exemplo, a Universidade de Campinas (Unicamp) fornece o “cartão de identidade institucional”, com *smart card*, aos seus professores, alunos e servidores, que é utilizado em dezenas de processos administrativos internos. Mesmo instituições financeiras poderiam utilizar o documento de identidade digital, em substituição aos seus cartões bancários.

5 Trabalhos relacionados – o documento de identidade digital em outros países

Em 1997, o Brasil instituiu o Registro de Identidade Civil (RIC) e o Cadastro Nacional de Registro de Identificação Civil (Lei n. 9.454/1997), que foi regulamentado em 2010 (Decreto n. 7.166/2010). A lei determina a criação de um “número único” pelo qual o cidadão será identificado e, embora não estabeleça a forma, normas complementares adotaram a biometria como meio para a identificação unívoca do cidadão (Resolução n. 2/2011, Comitê Gestor). Contudo, até o momento, o projeto não foi implementado, apesar de sucessivos anúncios do seu lançamento.

Por outro lado, mais de cem países no mundo criaram ou planejam criar documentos de identidade digital, com tecnologia *smart card*. O movimento se intensificou a partir de 2001, provocado pelos ataques terroristas nos Estados Unidos. A motivação principal, portanto, foi de segurança, para aumentar a confiança no processo de identificação das pessoas (Yeow, Paul H. P., *et al*).

Desde novembro de 2010, a Alemanha, utiliza documento de identidade com dados biométricos (face e impressão digital) dos seus cidadãos com idade a partir de 16 anos (CEU, 2014). A coleta da impressão digital é voluntária e somente armazenada no documento de identidade, com acesso exclusivo por órgãos públicos autorizados (BMI, 2010).

Diferente do projeto alemão, a Inglaterra, que instituiu o documento digital em março de 2006, armazenava os dados biométricos em um banco de dados, sendo obrigatório o registro para os residentes no país, maiores de 16 anos (UK, 2006).

Entretanto, o projeto inglês sofreu muitas críticas e, por isso, foi cancelado em janeiro de 2011, tendo sido deletados os registros das impressões digitais colhidas até então e tornado opcional o uso dos documentos de identidade gerados até aquela data (UK, 2013).

A crítica mais importante aos projetos de documentos de identidade com informações biométricas diz respeito ao risco de acesso indevido a esses dados, conhecido como “roubo de identidades”. Diferente de senhas, os dados biométricos de uma pessoa não sofrem alterações durante toda a vida e, por isso, não é possível revogá-los. Logo, o acesso indevido a essas informações pode gerar danos permanentes às pessoas cujas informações biométricas foram roubadas (Wharton, M., 2003).

Por isso a cautela da legislação alemã, que restringe o acesso a essas informações e as armazena somente no cartão do usuário. Com essa medida, de não constituir um banco de dados nacional com dados biométricos, o estado alemão elimina o risco de acesso indevido a essas informações.

6 Conclusão

Conforme se demonstrou neste artigo, a Justiça Eleitoral reúne as melhores condições para promover importante transformação no processo de autenticação, produzindo o documento de identidade digital para todos os cidadãos brasileiros. Além de possuir todos os dados necessários, é o órgão público com a melhor infraestrutura para prestar esse serviço à sociedade brasileira.

A própria Justiça Eleitoral seria grande beneficiária, adotando o documento de identidade digital nos processos do cadastro eleitoral e na votação. No longo prazo, poderiam ser revistos os processos atuais, com relevante redução dos seus custos operacionais, eventualmente compensando os gastos com a geração do documento.

No entanto, os principais beneficiários seriam as instituições públicas ou privadas, empresas e organizações da sociedade civil as mais variadas, que poderiam adotar o documento de identidade digital para automatizar vários de seus serviços, com forte impacto no aumento da segurança do processo e na redução dos seus custos.

Como estímulo à disseminação do uso do documento de identidade digital, a Justiça Eleitoral poderia priorizar o cadastramento dos eleitores de integrantes de entidades que disponibilizem aplicações imediatas para o seu uso em projetos de automação. Por exemplo, cadastrar os servidores do Poder Judiciário para usar o documento de identidade digital nos sistemas de gestão do processo judicial eletrônico ou nos sistemas de registro de ponto dos seus servidores. O mesmo tratamento poderia ser dispensado a outros órgãos públicos (ou mesmo empresas privadas) que ofereçam aplicações imediatas na automação dos seus processos internos. Medidas dessa natureza contribuirão para importante redução de custos de escala, evitando sistemas redundantes para a autenticação dos cidadãos.

Referências

LI, Chun-Ta, Hwang, Min-Shiang. *An efficient biometrics-based remote user authentication scheme using smart cards*. Journal of Network and Computer Application, Vol. 33, Issue 1, Jan. 2010. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1084804509001192> .

JUSTIÇA ELEITORAL. Manual do Mesário – Eleições/2012. Disponível em: <http://www.tse.jus.br/eleitor/mesario> .

JAIN, Anil K.; Feng, Jianjiang e NANDAKUMAR, Karthik. *Biometrics fingerprint matching*. IEEE Computer Society, Fev. 2010. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.211.1363&rep=rep1&type=pdf> .

BRASIL. Medida Provisória n. 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm .

BRASIL. Lei n. 5.869, de 11 de janeiro de 1973. Institui o Código de Processo Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L5869compilada.htm .

RECEITA FEDERAL. Porta e-CAC (Centro Virtual de Atendimento ao

Contribuinte). Sítio em: <http://www.receita.fazenda.gov.br/atendvirtual/defaultAtendCertDigital.htm> .

YEOW, Paul H. P., Yuen, Y. Y., LOO, W. H. *Ergonomics issues in national identification card for homeland security*. *Applied Ergonomics*, Vol. 44, Issue 5, Set. 2013, Pag. 719-729. Disponível em: www.sciencedirect.com/science/article/pii/S0003687012001019 .

BRASIL. Lei n. 9.454, de 7 de abril de 1997. Institui o número único de Registro de Identidade Civil e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/Decreto/D7166.htm .

BRASIL. Decreto n. 7.166, de 5 de maio de 2010. Cria o Sistema Nacional de Registro de Identificação Civil, institui seu Comitê Gestor, regulamenta disposições da Lei n. 9.454, de 7 de abril de 1997, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L5869compilada.htm .

COMITÊ GESTOR DO SISTEMA NACIONAL DE IDENTIFICAÇÃO CIVIL. Resolução n. 2, de 22 de novembro de 2011. Dispõe sobre as especificações técnicas básicas do documento de Registro de Identidade Civil. Diário Oficial da União, Brasília, DF, n. 224, de 23 de novembro de 2011, Seção 1, pag. 24-26.

COUNCIL OF THE EUROPEAN UNION. *Public register of authentic identity and travel documents online* (document: DEU-BO-02001). Disponível em: <http://prado.consilium.europa.eu/EN/5134/docHome.html> .

GERMAN FEDERAL MINISTRY OF THE INTERIOR (Bundesministerium des Innern -BMI). *German national identity card – facts about the new identity card*. 5th edition, Nov. 2010. Disponível em: www.personalausweisportal.de .

UNITED KINGDOM (UK). *Identity cards act 2006*. Disponível em: <http://www.legislation.gov.uk/ukpga/2006/15/contents> .

_____. *Guidance on the 2011 cancellation of identity cards, and information about new suppliers working with the Identity and Passport Service*. Disponível em: <https://www.gov.uk/identity-cards-and-new-identity-and-passport-service-suppliers> .

WHARTON, Matthew. *Identity and ID cards – an analysis of the national identity card scheme proposed by the British Government*. Jun. 2004. Disponível em: <http://www.electrinca.com/idcards/index2.html>

Notas

¹ Os dados dos tempos de votação foram retirados dos arquivos de log das urnas eletrônicas, considerando todos os votantes nas eleições de 2010 em Santa Catarina, desprezados os tempos de autenticação ou de votação superiores a oito minutos; a amostra resultante possui 3.832.494 e 13.885 registros, respectivamente para todo o estado e para o município de São João Batista cuja autenticação foi feita com biometria.

² Caso se trate de eleitor não pertencente à seção eleitoral e confirmado que o eleitor se encontra fora do seu domicílio eleitoral, pode ser registrada justificativa do eleitor em trânsito, nos moldes do que é feito atualmente para situação semelhante.

³ O tempo médio obtido foi de 7 minutos e 16 segundos. Porém, a média não é, neste caso, adequada como método de avaliação do tempo de cadastramento do eleitor, pois a variabilidade observada é alta – o desvio padrão dessa medição foi de 4 minutos e 22 segundos. Por isso, a mediana, de 6 minutos e 2 segundos, reflete melhor a medição do tempo de atendimento. Esses dados foram obtidos a partir de uma amostra de 31 mil eleitores cadastrados na região da Grande Florianópolis, no último trimestre de 2013.

⁴ O cadastramento dos dados biométricos dos eleitores ocorreu em 13 municípios na região da Grande Florianópolis.

⁵ Poder-se-ia acrescentar outras informações, tais como o número do Cadastro de Pessoas Físicas (CPF) da Receita Federal, o número do PIS/PASEP, o número de registro da Carteira de Trabalho, entre outros identificadores de cadastros públicos. No entanto, essa medida dependeria de concerto entre os diversos órgãos públicos envolvidos, a fim de estabelecer a sequência do cadastramento do cidadão ou, eventualmente, a troca eletrônica de dados.

* Servidor do Tribunal Regional Eleitoral de Santa Catarina; ex-Secretário de Informática (1996 a 2004 e 2007 a 2009); bacharel em Ciências da Computação, especialista em Gerenciamento de Projetos (com certificação PMP/PMI) e mestrando no Programa e Pós-Graduação do curso de Engenharia de Produção da Universidade Federal de Santa Catarina com o tema "Processo Eleitoral e Urna Eletrônica".