Prioridades na segurança digital

Pedro Antônio Dourado de Rezende *

Elaborado em 06.2008.

Resumo: 1. ICP-Brasil e Criptografia Assimétrica; 2. ICP-Brasil e Fé Pública em Documentos Eletrônicos; 3. Onde está a informação? 4. Qual é o maior desafio jurídico perante o virtual? 5. Prioridades no combate ao crime digital; 6. Pulando do décimo andar; 7. Centralismo fraudocrático. A. Apêndice: Tabuada com licença

A oportunidade de lecionar para gestores públicos sobre "Modelos de Confiança para Segurança em Informática" num curso de Especialização apresentou-me, também, a de aprender com distintas visões sobre segurança na esfera digital. Neste artigo, busco refletir sobre certos assuntos que, naquela oportunidade, se destacaram pela pluralidade de perspectivas. Tento aqui esclarecer a racionalidade com que opiniões ali ventiladas se formaram, com interesses a distâncias que permitem cumprir a missão e a função acadêmicas a contento.

1. ICP-Brasil e Criptografia Assimétrica

Uma das interessantes questões levantadas foi sobre a razão da Medida Provisória 2.200-2, que instituiu a ICP-Brasil, referir-se explicitamente à criptografia assimétrica. Estaria esta norma jurídica restringindo-se a uma dentre várias possíveis tecnologias de autenticação? A reposta passa por um holandês que viveu no século XIX, e que trabalhou com criptografia militar em Paris, e pela função que a assinatura de punho desempenha no Direito, como meio de prova de manifestação de vontade.

O militar em questão se chama Augueste Kerchoffs, nome associado ao axioma que ele propôs. Este axioma, conhecido como lei ou princípio de Kerchoffs na Criptografia, diz que um sistema criptográfico pode ter eficácia independente do conhecimento público de tudo sobre ele exceto a chave. Este princípio foi reformulado, tavez independentemente, em 1949 por Claude Shannon em sua Teoria da Informação, teoria que refundou a Criptografia como ciência moderna, ali como a premissa de que "o inimigo conhece o sistema". Trata-se de um princípio acolhido por vasta maioria dos criptógrafos, certamente pelos que se mostram os mais competentes, donde o rótulo de "lei" (semiológica).

A outra parte da estória nos remete à possibilidade de se reproduzir no virtual a função que a assinatura de punho desempenha na lide jurídica. É fato que a confiança de um interlocutor na identificação do outro via canal digital inseguro (autenticação) pode ser alcançada por compartilhamento prévio de segredo entre ambos, como ilustram os esquemas de autenticação conhecidos pela sigla MAC (message authentication code). Todavia, tais esquemas autenticam apenas uma identidade, e a integridade da transmissão, de um interlocutor para o outro. Esse tipo de autenticação tem, portanto, um sentido intersubjetivo, e não objetivo.

Em situações que envolvem potencial conflito de interesses a autenticação intersubjetiva é ineficaz, visto que um terceiro não poderia decidir sobre tal conflito com base nela. Isto porque um interlocutor poderia forjar a autenticação de emissões pelo outro, de forma imperceptível ao protocolo. Em tais situações a autenticação deve ser objetiva, ou seja, oponível a terceiros (como dizem os juristas). Na autenticação objetiva, seu sentido deve excluir que um interlocutor possa forjar, com custo/benefício aceitável (a quem forja), a identificação de outro emissor através de um ataque ao protocolo.

Numa autenticação objetiva, o segredo em que se baseia a identificação do emissor não pode, por isso, ser compartilhado; o que nos remete, acolhida a lei de Kerckhoffs, à criptografia assimétrica, com a qual a chave privada do emissor autentica, a chave pública correspondente verifica, e na qual a chave privada não pode (pela propriedade que classifica o sistema como assimétrico), com custo viável (ao interesse na forja), ser obtida da chave pública correspondente. Donde o nome "assinatura digital" para esse método objetivo de autenticação.

A alternativa de se rejeitar este princípio remete, neste contexto, ao axioma central da doutrina fundamentalista de mercado, que aqui aplicado impõe ao negócio da intermediação criptográfica o selo de neutralidade semântica para análise de riscos nas esferas técnica e jurídica. Tal foi o caminho seguido pelo modelo de lei UNCITRAL, no Brasil tramitado, em tradução sofrível, através do PLS 672/99 (de "autoria" do senador Lúcio Alcântara), adormecido pelo canetaço de FHC na MP 2.200 em 28 de junho de 2001.

O modelo UNCITRAL, adotado até aqui (pelo que temos notícia) apenas pela Colômbia, diz basicamente ser o mercado quem escolhe o que substitui, na esfera virtual perante o Direito, a assinatura de punho como instrumento de manifestação da vontade, ficando desde já invertido o ônus da prova sob tal escolha. Essa alternativa nos poria mais rapidamente no rumo do mundo de Orwell, via o de Kafka. A defesa do modelo UNCITRAL passa invariavelmente pelo seguinte argumento, especulativo por natureza e ingênuo apenas na aparência:

Se, no futuro, algo como a criptografia quântica tornar ineficaz, por exemplo, o algoritmo RSA como ele é hoje usado, como ficaria um marco regulatório como o da ICP-Brasil? A resposta não precisa repelir a lei de Kerckhoffs, em favor da canonização de vendedores de caixas-pretas eletrônicas. Pois se tal coisa acontecer, isso significa que o RSA como hoje usado deixa de ser um algoritmo assimétrico, sem afetar os que continuem a sê-lo, e não que a autenticação objetiva sob a lei de Kerchoffs deixa de remeter-se à criptografia assimétrica.

2. ICP-Brasil e Fé Pública em Documentos Eletrônicos

Outra questão interessante é se a MP 2.200-2 dá ou não fé pública a documentos eletrônicos assinados digitalmente e cujas assinaturas podem ser verificadas através da infraestrurua da ICP-Brasil, com base no que diz o artigo 10 da mesma. Vejamos o que diz a respeito um mestre em Direito Constitucional e Advogado da União, numa recém lançada coletânea jurídica [1]:

"Dispõe o art. 116 da Lei 8112/96 (RJU) que são deveres do servidor:...VII-zelar pela conservação do material e a conservação do patrimônio público. Este item adquire especial significação no que diz respeito à utilização de hardware e software, ambas passíveis de danificação em caso de mau uso (sic.). Aqui podem ser enquadradas as condutas irregulares do funcionário que, por grave descuido, ou mesmo voluntariamente, facilita a ´´infecção´´ de computadores e redes por códigos mailiciosos, inclusive pela utilização de procedimentos e softwares em desconformidade com o marco da ICP-Brasil, instituída pela MP 2.200-2."

Há que se indagar, aqui, em que sentido a conformidade com tal marco regulatório preveniria contra infecções capazes de produzir falsificações, ou contra falsificações rastreáveis a "mau uso" na conduta do funcionário, e em que sentido a não-conformidade com este marco seria causa facilitadora de ´´infecções´´ capazes de causar falsificações. Sobre este último, por exemplo, a lógica da mentalidade criminosa, que só cresce em sofisticação e especialização na esfera virtual (ver [2], [3]), aponta justamente no sentido contrário: haverá mais interesse em se desenvolver código malicioso, invisível e sorrateiro (ver [4]), contra softwares que se conformam em dar fé pública a documentos ditos eletrônicos do que contra softwares que a isso não se conformam. Sobre tal fé:

"... [Dispõe o art. 117 da Lei 8112/96 (RJU)] que são ilícitos passíveis de responsabilização pelo servidor: III- recusar fé a documentos públicos.. .. Situação ainda mais grave será a daquele servidor ou autoridade pública que negue fé quando confrontado com documento produzido por órgão público e ´´assinado´´ com as características da ICP-Brasil, instituída pela MP-2200-2, que prescreve, em seu art. 10:...". Inequívoca, aqui, a interpretação do Mestre. Restou-lhe esclarecer-nos, porém, se tal fé decorre da titularidade da assinatura (órgão público) ou do citado artigo 10º, esta uma situação que daria fé pública também a documentos eletrônicos privados sob o mesmo regime.

Em qualquer caso, há que se indagar, então, como conjugar esta fé com o possível "mau uso" provocado pelo click-through, ou seja, pela síndrome da tendência de se responder, movido pela pressa ou por frustração, "OK" a alertas de segurança sem ler ou buscar entender a mensagem que se responde, ou as conseqüências de uma tal ação. Por exemplo, quando uma página web é solicitada a um sítio "seguro" (acessível via protocolo https), e o navegador web, ao tentar validar o certificado recebido, não consegue montar um trust path ancorado em um certificado-raiz que ele já possua, o que acontece?

Nesses casos, o que acontece com mais frequência é o próprio sítio oferecer ao navegador também o certificado-raiz faltante: mas em banda, antes da Criptografia iniciar. Haverá um alerta do tipo "você tem certeza que conhece este sítio?", já que toda a cadeia enviada pode, em princípio, aí ser forjada. Para piorar, o trabalho acadêmico citado em [4] mostra como um código malicioso pode suprimir tal alerta no navegador usado por nove entre dez internautas. Neste caso, se o serviço DNS ou um Proxy estiver também comprometido com o mesmo demônio de Descartes (ver "Modelos de Confiança"), a forja poderá ser indetectável à vítima antes das

conseqüências. Isso num contexto em que um Arquiteto Chefe dirige nove entre dez escolhas (de plataforma) como se tais riscos e decisões fossem questões de "usabilidade" do software [10].

3. Onde está a informação?

Outro assunto que gerou dúvida (e muita) foi a definição de informação de Shannon. Um exemplo, em especial, de um administrador de CPD, que suscitou ceticismo quanto à sensatez ou utilidade de uma tal definição. Ao exibir sinais de enriquecimento ilícito (ia trabalhar a cada dia da semana com um BMW de cor diferente), o tal administrador hipotético teria levantado suspeitas, pelas quais se descobriu depois que ele estava vendendo cópia de backups dos emails dos diretores da empresa. Conforme a defnição de informação de Shannon, a informação valiosa para ele, que o motivou a vender mídias com backups, não estava nos dados destas mídias, mas sim nos dados sobre estas mídias.

Em dialetos de programação, a informação valiosa para ele estava, segundo Shannon, nos metadados (no rótulo da mídia!). Era o seu conhecimento de que aqueles dados seguramente correspondiam aos emails dos diretores da sua empresa num determinado período (pois ele próprio gravara os backups naquela mídia), de que lhe era lícito assim gravá-los (devido à sua função), e seu conhecimento de para quem aqueles dados poderiam conter informação valiosa (para concorrentes da sua empresa), que o permitiu identificar um canal de confiança capaz de proteger com sigilo o canal físico (ele mesmo) através do qual ele traficaria esses dados.

As partes em negociação não precisam conhecer o conteúdo dos dados para traficarem, ou seja, não precisam conhecer as informações nos dados desta mídia, informações que podem ser valiosas para o comprador, se ambos estiverem dispostos a correr os subjacentes riscos. Esse exemplo não convenceu a alguns, sobre a sensatez e possível utilidade da definição de informação de Shannon, de sorte que tentaremos um outro exemplo, agora com um boato que circula em palestras sobre segurança em informática.

Dizem que no sindicato do cibercrime em Nova York se compra e se vende, por dez mil dolares em média, laptops fechados e desligados roubados de executivos. A informação valiosa para o vendedor está no metadado (a origem do laptop, que o vendedor ´´garante´´ ser de um executivo por ter sido ele quem roubou ou quem está atravessando). A informação valiosa para o comprador está inicialmente neste metadado (a origem do laptop, de um executivo) e noutros metadados (quanto pode valer os dados que estão no laptop, para quadrilhas especializadas em vender dados de executivos, dentre as quais o próprio comprador pode ser uma).

Com base nesses metadados, sem conhecer o conteúdo dos dados (e portanto, sem conhecer a informação neles contida) os interlocutores negociam o preço (que se diz em média dez mil dólares), cada um tendo assumido seu risco: o vendedor, de ser pego pelo roubo, e o comprador, de ser pego por interceptação, de não conseguir quebrar uma possível cifragem dos dados ou de não vendê-los com lucro. Aqui, não há como argumentar que um trombadinha de laptop cifrado saiba qual informação ele estará oferecendo à venda. E há como se argumentar sobre a utilidade, para executivos, da informação de quanto vale no mercado do cibercrime o metadado "laptop de executivo."

4. Qual é o maior desafio jurídico perante o virtual?

Talvez eu tenha falhado ao comunicar, ali e alhures, minha opinião sobre esta questão quando a situo na tridimensionalidade do Direito segundo Miguel Reale (Norma, Valor e Fato). Minha opinião segue a do primeiro presidente da Comissão de Informática Jurídica da OAB, Marcos da Costa, de que este maior desafio está na identificação de autoria, necessária para se estabelecer fatos juridicamente relevantes. No citado minicurso certamente falhei, ou fui mal interpretado, haja vista as discordâncias ali suscitadas. Cabem aqui alguns esclarecimentos.

Ao falar de identificação de autoria, não me refiro à identificação do computador de onde teria se originado o fato ou ato ilícito, e/ou à do responsável por tal computador, por parte de autoridade policial para efeitos de instrução processual adequada. Me refiro à identificação da pessoa que agiu com intenção de cometer o fato ou ato ilícito, e/ou que para ele contribuiu com conduta incauta ou imprópria, por parte de autoridade judicial para efeitos de proferimento de sentença robusta.

A título de exemplo da diferença entre esses dois sentidos de identificação, e de como a confusão entre ambos contribui para a erosão do Direito perante o virtual, incluo aqui um link e um pequeno relato. O link é para um caso, envolvendo acusação de pedofilia e revertido em segunda instância, escolhido aleatoriamente dentre as notícias da semana em que escrevo este texto, dentre aquelas que despertam atenção pelo inusitado, pelo aberrante ou pelo esdrúxulo na lide jurídica sobre o virtual. E o relato é o seguinte:

Logo que apareceram os primeiros instaladores de GNU/Linux para pendrives, alguns alunos reportaram um crescimento local inusitado no número de pequenas empresas interessadas em migrar para software livre. Logo se descobriu que o caso mais comum envolvia o desejo de se enfiar toda a contabilidade da empresa, ou seu caixa dois, num sistema autônomo que pudesse bootar do pendrive, deixando a plataforma do PC limpa, só com orkut e jogos da secretária e talvez o que não comprometesse. É que quando viesse a fiscalização, seria mais fácil esconder a tempo no bolso, na cueca, no sapato ou no açucareiro um pendrive do que um livro-caixa, um PC/WinXP ou um laptop/Vista.

5. Sobre prioridades no combate ao crime virtual

A opinião que expressei durante o citado minicurso, gravada em áudio pela secretaria do mesmo, se lastreia em documento encaminhado pela Direção da Polícia Federal à Casa Civil da Presidência da República, em resposta a um requerimento da Comissão de Direitos Humanos da Câmara dos Deputados, remetido pela Casa Civil à Secretaria da Mesa da Câmara em meados de maio de 2008. Neste requerimento o presidente da referida Comissão solicita informações diversas sobre o fluxo de denúncias, investigações e encaminhamentos para abertura de processo por crime contra direitos humanos praticados por meio digital. Não convém discorrer sobre ele aqui, mas é fato que tal documento é público, e está disponível na Secretaria da Comissão de Direitos Humanos da Câmara dos Deputados.

Sobre o que convém discorrer aqui, destaca-se o slide 35 da apresentação que o Presidente da Safernet proferiu recentemente na Comissão Parlamentar de Inquérito sobre pedofilia no Senado, aqui linkada [5]. Nele se identificam bandeiras de operadoras de cartões de crédito, inclusive de duas das maiores, na página de login de um site especializado em pornografia pedófila. Este slide

está ali para chamar antenção ao fato de que o substitutivo de projetos de lei apresentado pelo Senador Azeredo ao Senado, à guisa de buscar mais eficácia no combate à pedofilia e outros crimes em meio digital, não contempla nenhuma responsabilização para entidades financeiras que habilitam negócios neste setor, enquanto agora criminaliza condutas como a posse de material pornográfico envolvendo pedofilia, esta sem nenhuma excepcionalidade.

Assim, a proposta atual de Azeredo (ver [6]) criminaliza também a preservação de material para efeitos de denúncia, cerceando conselhos tutelares e entidades civis envolvidas no combate a crimes desse tipo, e provedores de serviço usados como intermediários no tráfico deste material, que queiram preservar provas para instrução processual. Ainda, e por outro lado, esta proposta expõe esses mesmos provedores à prática de crime por denunciação caluniosa caso cumpram com uma obrigação ali mesmo imposta (art. 22, inciso III), qual seja, a de denunciar tais ilícitos do seu conhecimento, se o fizerem sem a devida preservação das provas. E não por descuido, pois o principal assessor do senador Azeredo para esta proposta teria sido, conforme relato de representantes de interesses afetos, alertado deste efeito colateral.

Dentre os dispositivos controversos desta proposta, também o que insere no código penal o seguinte:

"285-B - Obter ou transferir dado ou informação disponível em rede de compudadores, dispositivo de comunicação ou sistema informatizado, sem autorização ou em *desconformidade à autorização*, pelo *legítimo titular*, quado exigida: Pena - reclusão de 1(um) a 3(três) anos e multa.

Parágrafo único: Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço"

Uma norma jurídica pode pretender qualquer coisa. O papel em que está escrito aceita. Papel aceita qualquer coisa, como prova -- no dizer atrevido do professor Evandro Lima -- o papel higiênico. Uma norma jurídica pode até pretender alterar leis físicas, decretando, por exemplo, que a constante gravitacional doravante será 0,98 m/s2, em substituição a seu antigo valor de 09,8 m/s2 (pelo que se pode agora pular do 10º andar). Mais sutilmente, uma norma jurídica pode pretender alterar leis semiológicas. Diz-se que ainda vige em Veneza uma lei, sancionada no século XVI, que proíbe às prostitutas se vestirem em determinadas cores, cores nela listadas como reservadas às damas honradas.

6. Pulando do décimo andar

Levada à CCJ pelo senador Azeredo para votação extra-pauta, e sem tempo de discussão (ao seu estilo), a atual versão do substitutivo traz dispositivos como o 285-B, este prenhe de um sentido de conexão técnico-jurídica que pretende alterar leis semiológicas, leis pelas quais a possibilidade de eficácia probante da identificação fática de "obtenção" ou "transferência" de dados pode ser logicamente erguida, ao iteragirem estas com outras leis que atuam na esfera simbólica. Pretende-o banalizando-as, ofuscando elos causais para responsabilização ou exceção através de ações ou cautelas plausíveis, comensuráveis aos efeitos, competências e necessidades subjacentes, por parte dos interesses envolvidos.

E se o dado ou informação sub judice estiver disponível através de busca, em algum ponto do ciberespaço, ali sem nenhum indício de estar também alhures disponivel mediante autorização exigida por algum pretenso "legítimo titular"? Por cautela, como saber se um dado ou informação tem ou não um pretenso "legítimo titular" alhures? E se, para os que testarão os limites da lei, a fonte ou a anterioridade da exigência de autorização, em relação à obtenção ou transferência, puder ser indetectavelmente forjada pelo demandante, como equilibrar os ônus de prova e contraprova? E se os dados cuja autorização "pelo legítimo titular" conflita com a função do documento que o veicula (documentos públicos), como aplicar (inverter?) o princípio da especificidade?

E se o dado ou informação sub judice estiver disponível através de observação, compilação, processamento ou cálculo, em algum ponto do mundo platônico, ali sem nenhum sentido plausível pelo qual alhures alguém possa se arvorar seu "legítimo titular"? Como por exemplo, dados que podem ser levantados em estatísticas, sobre dados livremente observáveis ou amostráveis, como os geográficos, os linguísticos e os aritméticos? Dados da representação decimal da relação entre circunferência e raio (pi), ou dados cujo uso estão legitimados, como os verbetes de um idioma, até em obras autorais de tipo dicionário? (ver Apêndice A).

Ou então, para falar de dinheiro, dados cujo uso são reclamados, se em mais de quatro verbetes, por multinacionais da mídia corportativa como a Associated Press? [11] Por que cargas d´´água "dado ou informação" com "legítimo titular", e não "obra autoral" ou "parte substancial de obra autoral"? Por que deixar em aberto a aplicabilidade do princípio da especificidade em conflitos com direitos civis tais como os de livre expressão e o autoral com suas excecionalidades (art. 46, Lei 9.610)? Quantos taxímetros semelhantes ao da AP serão estimulados a se instalar no ciberespaço, em meio a tanta dúvida, com o guante desse aberrante dispositivo aqui a seu serviço (ver Apêndice A)?

Ou será que dispositivos como este tem seus interesses motivadores em metas indizíveis de incertezas e de meios para chantagem juridicas, sustentadas por estridente hermenêutica positivista, à revelia de sua efiácia? É o que pode estar sinalizando tanta estultície semiológica em tamanho abuso normativo (ver Apêndice A). Se o que estão a fazer outros países é pretexto, por que deveríamos nos entregar nós, com tanta sofreguidão e à socapa, a essa nova forma de colonialismo? Se for acolhida por interesses políticos e pela hermenêutica positivista aqui dominantes, tais pretensões mágicas de se tutelar o mundo dos símbolos trarão seu custo social em insegurança jurídica, na medida em que a lógica da mentalidade anti-social fluir para cobrá-lo, pela via da sua própria evolução tecno-política, quando irrigada pelo enquadramento, num tal regime, de práticas sociais já disseminadas.

É possível, e fácil, deduzir quem poderá com isso ganhar. Trasímaco o mostrou a Platão, em República. E em exemplos mais recentes na História, o filósofo Karl Polanyi, que, ao estudar o avanço do fascismo nos anos 20 e 30, concluiu ter este avanço se dado não por patologia social ou conspiração irracional, mas pela ação de forças surgidas de dentro do capitalismo [7]. A uma conclusão semelhante também chega Franz Neumann, no seu livro "Behemoth", em que analisa as origens política, social e jurídica do nazismo. Segundo a socióloga Walquíria Rego, da Unicamp, "Neumann investigou detalhadamente as práticas judiciais absolutamente parciais, que mal conseguem ocultar seu posicionamento em favor dos grandes interesses industriais e financeiros da Alemanha de então" [9].

A socióloga explica que a forma mais recorrente de atuação empregada pelo nazismo para erguer seu poder "consistiu na criminalização dos movimentos de trabalhadores, processando e condenando sem cessar seus líderes e simpatizantes, afora outras arbitrariedades." "A direita alemã empregou a arma judicial cada vez com maior intensidade, e a investida antidemocrática não ficou nisso. Incidiu fortemente no pensamento jurídico teórico alemão. Ao longo desse processo, os juízes tiveram seu poder aumentado às expensas do Parlamento. A justiça política, na visão de Neumann, ´´constituiu a página mais sombria da República de Weimar.´´"[8] Com leis extremadas ao limite de criminalizarem quase toda prática social possível, o caminho para isso foi -- e está sendo (re) -- aberto.

Com a reorganização política da sociedade que se informatiza, a lógica do poder exige, paralelamente, uma reconfiguração política e do pensar sobre os meios de comunicação, extensiva à sua infraestrutura (TIC). Se, hoje, a anomalia funcional no Estado que gerou o nazi-fascismo volta a ocorrer, segundo Walquíria, "com intensidade assustadora", o que esperar da sociedade que assim vai-se construindo rumo ao futuro? Estamos testemunhando, em todo o mundo, as mesmas influências no controle do processo legislativo, em par com crescentes aberrações por seu abuso, como antanho. Neste ciclo a História está a se repetir, como farsa e como tragédia, com a criminalização desta vez dos movimentos que resistem em defender direitos de cidadania, trocados por miçangas e fetiches em direitos de consumir.

7. Centralismo Fraudocrático

Há uma esfera onde a troca de direitos de cidadania por miçangas e fetiches pode impulsionar sobremodo este novo ciclo da História. Nessa esfera a troca prossegue em ritmo galopante, e ainda mais obscuro, ademais a um custo econômico significativo para quem paga impostos. Não pretendo cansar o leitor com uma narrativa de como essa troca ali começou e vem evoluindo. Vou me ater aqui ao último lance que ali se descortina, referindo o interessado numa tal narrativa a outros textos (vide [12], [13], [16]). Vou me ater, mais precisamente, ao enredo que talvez exija a mais cara encenação no teatro da segurança civil que a História da nossa República já viu.

Eu não faço a menor idéia publicável de quais possam ser os reais interesses a motivar uma possível adoção de biometria para a identificação de votantes no sistema eleitoral em uso no Brasil. Os interesses até aqui comunicados, honestamente, não os compreendo como sadias motivações. No meu singelo descortino reconheço que um sistema de identificação tão complexo, caro e difícil de fiscalizar serve para bem sustentar o discurso da modernização eleitoral, pregado pela seita do santo baite [15], mas confesso-me completamente cético sobre qual problema de segurança eleitoral que tal medida viria a bem servir. Resta-me analisar o que é de conhecimento público.

Ouve-se dizer que o interesse motivador do uso da biometria no sistema eleitoral seria para erradicar "a única forma de fraude restante" no sistema atual. Falta precisar que o que se pode pretender erradicar com tal coisa seria a única forma de fraude à antiga restante no sistema atual. Trata-se da fraude no cadastro, forma de fraude varejista (num sistema de votação manual, toda forma de fraude é varejista) que no sistema atual persiste, as outras trocadas que foram por novas formas atacadistas. Esta classificação (varejo/atacado) se justifica pelo inédito patamar na proporção desvio/efeito que as novas formas de fraude, eletronicamanete provocadas, podem

causar [12]. Formas estas desconhecidas de leigos e analfabetos digitais, que, como todos, não enxergam bits, mas que, não como todos, desconhecem como operam os bits e quase nunca aspiram conhecer.

Esta antiga e resistente forma de fraude continua, de fato, a fazer parte da cultura política e do folclore sobre o modus operandi da política nativa mesmo com votação puramente eletrônica. Perpetrada através do controle de cartórios eleitorais, em áreas de influência, com vistas a inchar o cadastro eleitoral com fantasmas, eleitores que recebem vários títulos, obtidos com variantes do nome ou com documentos falsos, para votarem conforme algum interesse direto, pessoal e verificável. Enquanto o cadastramento de eleitores for controlado localmente, não há nada que uma justiça eleitoral centralizada possa fazer contra essa forma varejista de fraude.

Atualmente, como antes da informatização, cada cartório eleitoral decide como coíbe ou não coíbe, como faz vista fina ou vista grossa, como dissipa ou participa desse tipo de manipulação. O cadastro eleitoral de Camaçari-BA, por exemplo, que já foi três vezes refeito a mando da Justiça Eleitoral Federal para expurgar eleitores fantasmas, cresce a cada recadastramento, e sempre além das estimativas demográficas, num inchaço que neste caso se justificaria por estar o município em área metropolitana (Salvador) [17].

Se o objetivo a mover uma alteração na forma de identificar o votante for mesmo o de neutralizar a fraude cadastral que resiste, à moda antiga, à informatização impingida ao eleitorado brasileiro, a solução mais racional e eficaz seria, também, à moda antiga. Eficaz, barata, fácil de fiscalizar, testada e usada por democracias que se preocupam com sua própria saúde em todo o mundo: a tradicional tinta indelével no dedo de quem vota. Doutra feita, a introdução de novas tecnologias da informação, como a biométrica, traz sempre consigo novas formas de fraude, associadas à subversão do seu propósito. Cabe então ao especialista comparar os riscos prementes e os subjacentes.

Com as urnas atuais é possivel a um mesário liberar indevidamente um voto, em nome de um eleitor ausente, em cerca de 15 segundos. Daí talvez porque uma carrada de votações rapidinhas na última meia hora de votação aparecem em muitos logs de urnas eletrônicas. Talvez os votos dos sem-título. Nos testes realizados pelo TSE em 2008, em três cidades Brasileiras, com um sistema piloto constatou-se que com a identificação biométrica é possivel fazer o mesmo em cerca de 40 segundos. Para isso o mesário terá que clicar cerca de vinte vezes, ao invés de apenas três como hoje [14]. Alternadamente em dois botões, no sistema testado, ou da maneira necessária para se resolver o inevitável problema dos falsos negativos da identificação biométrica, noutros sistemas. Com a biometria, a carrada de votos dos sem-título (ou sem-dedo) talvez se extenda por uma hora.

Para quem porventura abrigue interesses motiváveis pela consequente centralização do controle dos meios -- e não da erradicação -- da fraude eleitoral, a medida tradicional da tinta no dedo obviamente não serve, por se tratar de uma medida de segurança descentralizada, que permite fácil fiscalização por parte do eleitor, e por se tratar de uma medida muito difícil de se burlar quando fiscalizada. Além de muito barata, comparada à biometria, o que poderia diminuir o interesse de fornecedores dispostos a acordos por motivos indizíveis. Caberia a tais interesses, então, demonizar a medida tradicional como atrasada e antiquada, como retrocesso ou coisa que o

valha, para vestir a ciberbobagem da panacéia biométrica com roupa nova de rei. Bem ao estilo doutrinário da seita do santo baite [15].

Se o interesse inicial que motiva a demonização do combate racional à fraude eleitoral for indizível, um que promova o combate teatral e para isso demande a centralização do controle sobre os possíveis meios de se praticá-la, a biometria, por outro lado, viria a calhar. Pois ampliaria a centralização atacadista dos possíveis meios de fraude que a informatização do processo eleitoral, para o bem ou para o mal, nele realiza. Restariam apenas os longos 40 segundos, não mais 15. Àquilo que possa demandar um tal interesse motivador indizível, chamamos de centralismo fraudocrático. Útil para mais um crivo, final e central, indizível e invisível, na democracia em agonia. Útil para eleitorados já adestrados à noção de eleição como espetáculo tecno-midiático, para os quais democracia é apertar botões em caixa-preta e correr à televisão para ver resultados, e para o qual, portanto, a biometria vai ser só mais um botão para meter o dedo. Mais uma renúncia ao direito de fiscalizar, ao que ainda restava desse direito outra vez cedido ao santo baite.

Direito cedido a quem controla tecnologias que servem tanto para impedir votos falsos e eleitores fantasmas quanto para inseri-los ou permiti-los onde quem as controla os queira [13]. Agora com a cobertura, no teatro da segurança, de um conhecido enredo reeditado: de que com a biometria, agora finalmente, se acabarão os votos falsos e os eleitores fantasmas. A trama na qual ínfimos ´´erros´´ de programação, de configuração ou de instalação do sistema, indistinguíveis da sabotagem maliciosa em seus possíveis rastros internos, poderiam causar também que não ocorram cruzamentos de impressões digitais em títulos eleitorais aqui ou ali, causando o bloqueio de fantasmas a falhar nesta ou naquela zona eleitoral, não faz parte das possibilidades neste enredo. Ainda mais com o presidente do TSE declamando em público, em reunião política da qual foi anfitrião em 11 de junho, que o uso da biometria dispensará a intervenção humana dos mesários na votação. Será?

A um custo de cerca de R$ 130 milhões só em equipamento para coleta eletrônica de impressões digitais [14], digitais para um processo de identificação "automatizada" dominado na escala pretendida só por poucas empresas transnacionais (quatro ou cinco), empresas que talvez só estejam interessadas se com "acordos de cooperação" (por exemplo, para integrar a base de dados biométricos dos eleitores brasileiros, mantida por impostos dos próprios, a esquemas de monitoramento e espionagem transnacionais, mantidos por sottogovernos [9]), "acordos" que talvez só venham a tona, se vierem, após a contratação e instalação de suas tecnologias secretas e serviços não menos, o centralismo fraudocrático estaria bem servido. Com "testes já realizados" [14] gerando o fato a ser consumado. E com aquele que levantar qualquer lebre a ser visto como paranóico ou conspiracionista. Quando não retrógrado, impatriota ou desrespeitoso. Mas há que se combater o bom combate, e guardar a fé.

Referências

[1]- Luiz F T Vergueiro: Internet e seus reflexos estruturais no Direito Processual. Em "Direito e Internet, Vol. II", pp. 325-354. Ed. Quartier Latin (2008).

[2]- FBI - IC3: Internet Crime Complaint Center Annual Reports http://www.ic3.gov/media/annualreports.aspx

[3]- Symantec: Internet Security Threat Report Tracks Notable Rise in Cybercrime www.symantec.com/about/news/release/article.jsp?prid=20060307_01

[4]- Marchesini, J & Smith, S.& Zhao M, Dartmouth College: Keyjacking: Risks of the Current Client-side Infrastructure Proceedings of the 2nd Annual PKI Research Workshop, NIST http://middleware.internet2.edu/pki03/presentations/11.pdf

[5]- Thiago Tavares: Apresentação da Safernet na CPI da Pedofilia no Senado http://www.safernet.org.br/tmp/apresentacao-cpi-senado.pdf

[6]- Eduardo Azeredo: Relatório de Substitutivo de Projetos de Lei https://www.safernet.org.br/tmp/PLS-Azeredo-aprovado-CCJ-18jun2008.pdf

[7]- Karl Polianyi: The essence of fascism, http://www.voiceoftheturtle.org/library/essence_of_fascism.php

[8]- Walquiria Rêgo: "Política da Justiça e Democracia", Carta Capital n. 418, 8 de Novembro de 2006, p. 19

[9]- Pedro A D Rezende: Software Cultura e Liberdade http://www.cic.unb.br/docentes/pedro/trabs/goethe.html

[10]- Todd Bishop: "Full text: An epic Bill Gates e-mail rant" http://blog.seattlepi.nwsource.com/microsoft/archives/141821.asp

"The lack of attention to usability represented by these experiences blows my mind. I thought we had reached a low with Windows Network places or the messages I get when I try to use 802.11. (don´´t you just love that root certificate message?)"

[11]- Pamela Jones: What is fair use anyway? AP has a thought, and so do I. Groklaw http://www.groklaw.net/article.php?story=20080622144323977

[12]- Pedro A D Rezende: Sistema Eleitoral em Uso no Brasil http://www.cic.unb.br/docentes/pedro/trabs/urnas_pt.html

[13]- Pedro A D Rezende: Electronic Voting: A Balacing Act http://www.cic.unb.br/docentes/pedro/trabs/Brazil_election.html

[14] Amilcar Brunazo: Eleição com biometria – Simulado http://www.mail-archive.com/votoeletronico@googlegroups.com/msg00151.html

Nos testes que o TSE já realizou (Colorado do Oeste, RO) ou realizará (São João Batista, SC, e Fátima do Sul, MS) para simulação da votação com as "urnas biométricas" pelas quais esses tres municípios devem votar em outubro de 2008, o procedimento de identificação dos eleitores é o seguinte:

1- o eleitor fornece o seu título eleitoral (sem foto) ao mesário;

2- o mesário confere o nome do eleitor na Folha de Votação impressa que possui, na qual haverá uma foto 3x4 do eleitor;

3- o mesário digita o número do eleitor no micro-terminal a sua frente.

4- no visor do terminal do mesário será solicitado a colocação do polegar direito do eleitor no sensor ótico que fica acoplado ao próprio terminal;

5- o eleitor terá 15 s para colocar o dedo e ser identificado;

6- se a identificação for positiva, a urna é liberada para a votação;

7- se a identificação for negativa, começa o drama. O mesário é consultado se o eleitor insiste com o mesmo dedo ou se passa para o dedo seguinte (indicador da mão direita);

8- o eleitor poderá tentar a identificação de cada dedo por 3 vezes até que consiga uma identificação positiva;

9- a ordem dos dedos solicitados para identificação é: do polegar para o mindinho da mão direita, seguido pelo polegar até o mindinho da mão esquerda;

10- se ao final das tentativas ainda não tiver ocorrido a identificação positiva, o mesário digita uma senha padrão (a mesma para todas as urnas) que libera a urna para a votação daquele eleitor;

Os 3 primeiros passos deste procedimento são os mesmos de uma votação nornal sem biometria. O que se segue, são passos adicionais que, obviamente, demandam tempo (no mínimo uns 10 a 15 s quando ocorre identificação positiva na primeira tentativa). No caso de eleitor com "dedos ruins" (para biometria), a identificação poderá demorar até 5 mim, bloqueando a votação dos demais eleitores.

O motivo da urna-b pedir os dedos em ordem pre-determinada, em vez de simplesmente deixar o eleitor colocar algum dedo qualquer no sensor e ela fazer a identificação entre os eleitores daquela seção eleitoral (até uns 500), é que este procedimento de encontrar a identificação no arquivo de eleitores autorizados estava demorando até 1 mimuto.

Portanto, a votação em urnas com biometria será necessariamente mais lenta (o contrário que alguns arautos do Santo Baite têm anunciado). Também, ao contrário do anunciado por estes "iludidos da tecnologia", não será eliminada a necessidade de títulos e de mesários. Devido o problema do falso negativo (quando a urna-b não identifica um eleitor legítimo) sempre será necessário um mesário para esta liberação extra, o que remete ao problema seguinte: o mesário desonesto.

Nestes testes provavelmente não será permitido simular a liberação da urna por um mesário sem que o eleitor esteja de fato a sua frente. Mas isto é perfeitamente possível, bastando o mesário digitar repetidas vezes as teclas CANCELA/CONFIRMA do seu micro-terminal quando

for solicitado ao eleitor colocar os seus dedos no sensor. Se nas urnas-e normais era possivel para um mesário introduzir um voto falso por eleitor ausente em 15 a 20 s, com as urnas-b será possivel fazer o mesmo em uns 40 s.

Hoje, o cadastramento de eleitores é feito usando as computadores normais dos cartórios. Com o novo sistema, a coleta dos dados biométricos passará a ser feita por um equipamento especial, chamado de KitBio, cuja compra dos primeiros 63 equipamentos saiu em torno de R$ 850 mil (R$ 13.460,31 cada KitBio). Considerando que cada um dos 3100 cartórios eleitorais terá ao menos 3 deste super-caros equipamentos... dá aqueles R$ 130 milhões.

Para se ter uma ideia do custo total que o TSE terá para montar o seu "maior cadastro biométrico do mundo" deve-se ainda acrescentar o custo para recadastramento dos 130 milhões de eleitores, mais o custo de equipar as 400 mil urnas-e com leitores de impressão digital, mais o custo dos computadores/servidores do novo banco de dados para guardar as 1,3 bilhões de impressões digitais, mais o custo de operar este cadastro e fazer o batimento (conferência) das 1,3 bilhões de impressões digitais para detectar duplicidade cada vez que um novo eleitor é inscrito.

O TSE não divulgou nenhuma estimativa do custo deste sistema biométrico para se poder avaliar se vale a pena em vez de simplesmente usar tinta indelével para pintar os dedos de quem já votou.

[15]- Pedro A D Rezende: A seita do Santo Baite. http://www.cic.unb.br/docentes/pedro/trabs/azeredo.htm

[16]- Luiz Paulo do Nascimento: Urna Eletrônica Brasileira: Símbolo de sucesso, ou caixa-preta cercada de controvérsias http://www.votoseguro.org/textos/LPNascimento-monografia.pdf

[17]- Amilcar Brunazo: Sobre o cadastro eleitoral de Camaçari, BA http://www.brunazo.eng.br/voto-e/textos/camacari1.htm

Apêndice A

Tabela com acesso sob licença

Declaração: O autor deste artigo, identificado no título em epígrafe, para fins e efeitos legais cabíveis se declara o legítimo titular dos dados ou informações na Tabela abaixo, por ser esta uma criação e confecção do seu intelecto como parte deste documento em que se fixa a referida autoria. Obter ou transferir qualquer desses dados ou informações estará sujeito aos termos da licença xyz abaixo, esta derivada de licença adotada pela Associated Press conforme descrito na referência [11].

Aviso importante: Caso o substitutivo do senador Azeredo citado na seção 6 acima seja aprovado e sancionado em Lei, os infratores estarão sujeitos a pena de um a três anos de reclusão e multa, e poderão ser processados com todo o rigor cabível.

1 x 1 = 1

1 x 2 = 2

1 x 3 = 3

1 x 4 = 4

1 x 5 = 5

1 x 6 = 6

1 x 7 = 7

1 x 8 = 8

1 x 9 = 9

2 x 1 = 2

3 x 1 = 3

3 x 2 = 6

3 x 3 = 9

3 x 4 = 12

3 x 5 = 15

3 x 6 = 18

3 x 7 = 21

3 x 8 = 24

3 x 9 = 27

4 x 1 = 4

4 x 2 = 8

4 x 3 = 12

4 x 4 = 16

4 x 5 = 20

4 x 6 = 24

4 x 7 = 28

4 x 8 = 32

4 x 9 = 36

5 x 1 = 5

5 x 2 = 10

5 x 3 = 15

5 x 4 = 20

5 x 5 = 25

5 x 6 = 30

5 x 7 = 35

5 x 8 = 40

5 x 9 = 45

6 x 1 = 6

6 x 2 = 12

6 x 3 = 18

6 x 4 = 24

6 x 5 = 30

6 x 6 = 36

6 x 7 = 42

6 x 8 = 48

6 x 9 = 54

7 x 1 = 7

7 x 2 = 14

7 x 3 = 21

7 x 4 = 28

7 x 5 = 35

7 x 6 = 42

7 x 7 = 49

7 x 8 = 56

7 x 9 = 63

8 x 1 = 8

8 x 2 = 16

8 x 3 = 24

8 x 4 = 32

8 x 5 = 40

8 x 6 = 48

8 x 7 = 56

8 x 8 = 64

8 x 9 = 72

9 x 1 = 9

9 x 2 = 18

9 x 3 = 27

9 x 4 = 36

9 x 5 = 45

9 x 9 = 54

9 x 7 = 63

9 x 8 = 72

9 x 9 = 81

Licença xyz

Objeto desta licença:

Autorização para Obter ou Transferir, de forma digital, mental, oral ou escrita, qualquer dado ou informação da Tabela acima nela expressável por mais de quatro verbetes (por exemplo, 2 x 2 = 4).

Termos e condições desta licença:

Cláusula 1: O licenciado terá que pagar, pelo direito de obter ou transferir dados ou informações disponíveis pela Internet a partir da Tabela acima, US$ 12.50 (doze dólares e cinquenta centavos de dolar norteamericano) por cada sequência de cinco verbetes que deseje obter ou transferir, convertidos a reais pelo câmbio oficial do Banco Central no dia da contratação do licenciamento;

Cláusula 2: O pagamento deve ser efetuado em espécie, ao titular desses dados e informações identificado em epígrafe ou seu preposto, na secretaria do departamento de Ciência da Computação da Universidade de Brasília, em horário comercial, com o licenciado identificando os verbetes que deseja licenciar após plantar bananeira e declamar o verso: "Viva o senador!"

único: Em caso de impossibilidade do pagamento ser efetuado de forma presencial, poderá ser efetuado via depósito identificado em conta corrente a ser informada mediante solicitação, que deve incluir, além da identificação do solicitante e dos verbetes que este deseja licenciar, link para vídeo mostrando o solicitante plantando bananeira e declamando "Viva o senador!"

Cláusula 3: O licenciamento é pessoal e intransferível. É proibido o sublicenciamento, total ou parcial, dos dados ou informações licenciadas individualmente.

* professor de Ciência da Computação da Universidade de Brasília (UnB), coordenador do programa de Extensão Universitária em Criptografia e Segurança Computacional da UnB, ATC PhD em Matemática Aplicada pela Universidade de Berkeley (EUA), ex-representante da sociedade civil no Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)