A Identidade Digital

A Identidade Digital (ou ID) é talvez um dos assuntos mais apaixonantes dos dias de hoje. Não há um único cidadão, instituição, entidade colectiva, a quem ela não vá afectar quando, de modo irremediável, a actividade da sociedade se deslocar preponderantemente para a esfera do ciberespaço. Não ter identidade digital, dentro de alguns anos, será em grande medida como não ter bilhete de identidade nos dias de hoje.

Na sua essência, a identidade digital baseia-se em informação, a qual é compilada, organizada e actualizada em sistemas informáticos, relativamente a pessoas físicas e jurídicas.

A atestação e verificação da identidade digital de um sujeito baseia-se no que se chama uma assinatura digital, resultado da aplicação de uma função criptográfica a um texto arbitrário (aquilo que é assinado), função essa apenas possível de executar, em teoria, pelo dono da assinatura (o sujeito), detentor do que se chama uma chave privada.

A elegância do processo é que a verificação da assinatura pode ser feita por qualquer pessoa que tenha a chamada chave pública.

Assim, temos por exemplo uma melhoria da robustez de uma assinatura e uma interessante democratização da função de notariado com assinalável precisão. Mas por outro lado, no caso de roubo de identidade, o problema assume uma muito maior gravidade, uma vez que se torna virtualmente impossível distinguir entre uma assinatura feita pelo sujeito e uma feita por um impostor.

Além disso, os processos de definição, criação e gestão de identidades digitais numa sociedade extravasam em muito este simples processo tecnológico, e na nossa sociedade, a migração para a Identidade Digital avança conspicuamente à reveza da compreensão, aceitação e participação das partes interessadas, os cidadãos e organizações.

Parte do problema reside no potencial alheamento dos vários poderes públicos, desde a administração pública ao poder judicial, das profundas implicações sociais que a migração para o digital implica.

Um projecto de Identidade Digital não é um mero projecto tecnológico.

---

1 As opiniões expressas são da responsabilidade exclusiva dos autores, e não reflectem necessariamente as posições da APDSI ou de qualquer outra das entidades referidas no texto.
A questão da identidade digital pertence ao universo normalmente referido como «sociedade da informação», é multifacetada, e alguns dos problemas que têm surgido no processo de “digitalização” da identidade derivam de percepções estreitas dessa realidade.
Isto é, derivam de se abordar a ID somente pela perspectiva tecnocrática, ou comercial, ou política, ou mesmo policial/securitária.
A manter-se esta abordagem, a visão sobre a ID nunca será bem sucedida.

Acerca das vertentes securitária e tecnocrática, poder-se-á argumentar, como tem sido ouvido e lido amíúde, que «tudo ou quase tudo se justifica para garantir a nossa segurança» face às mais diversas ameaças, ou ainda que o mais importante é a «eficiência e eficácia dos processos administrativos, financeiros e comerciais».

Na verdade, estas são visões precipitadas e algo ingênuas da realidade, que se baseiam no pressuposto de que o cidadão tem uma atitude estática e passiva em relação à sociedade da informação e às medidas que lhe são impostas.

Citando [1]: «... os cidadãos têm uma desconfiança crescente nos serviços e infra-estruturas de informação e comunicação ...» ou «... a experiência do cidadão comum é dominada pelo conhecimento público de falhas de computadores, grandes projectos de software mal sucedidos, programas maliciosos (vírus, spam, espóios). Não se encontra outra razão para esta atitude que não sejam os problemas de segurança percebidos pelos utilizadores, que estão longe de estar resolvidos e que levam à deterioração da confiança sentida nos sistemas. A não percepção destas dinâmicas pelas partes interessadas pode levar a situações de difícil retorno no que respeita à sociedade da informação.

Citando de novo [1]: «... se uma sociedade baseada em TIC não for capaz de criar confiança nos serviços, isto é, confiança que se baseie em argumentos justificados e credíveis, então esses serviços, que serão de qualquer modo disponíveis devido à pressão do mercado: serão vistos com desconfiança pelos utilizadores; serão geridos por grupos restritos de “peritos”, aumentando a info-exclusão; poderão ser mal geridos, levando ao ciber-crime, e-fraude, ciber-terrorism ou sabotagem...».

Não é difícil intuir os graves problemas que podem surgir, num futuro próximo: com sistemas de Identidade Digital aparentemente interessantes do ponto de vista tecnológico mas não adequadamente balastrados em propriedades de segurança certificáveis e auditáveis; com a ausência da mais que necessária modernização da lei do crime informático, ou da geral adequação das leis relacionadas com a identidade e identificação; com a falta de acompanhamento de meios, predominantemente de natureza tecnológica, que garantam a eficácia das polícias e dos tribunais na esfera digital.

Hoje em dia, qualquer cidadão é detentor soberano do seu documento de identificação, da sua assinatura, e dos direitos de privacidade sobre estas e dados associados que lhe são garantidos pela Constituição Portuguesa.

Em consequência, o mais grave problema virá se se enveredar por soluções tecno-político-legais que não garantam a posse e o controlo da sua Identidade Digital pelas partes interessadas.

A Identidade Digital está a montante de vários outros processos críticos, como sejam: votação electrónica; controlo de acessos (incluindo passagem de fronteiras); comércio electrónico; digitalização de processos na administração pública.

No momento actual, para os responsáveis políticos, o debate sobre a gestão da identidade estará intensamente ligado aos documentos de identificação oficiais, como
é o caso do Cartão de Cidadão e do novo Passaporte Electrónico Português. Ao mesmo tempo, para os fornecedores de serviços e de produtos, a discussão centra-se sobre a selecção de tecnologias para autenticar cidadãos e negócios. No entanto, o debate sobre a gestão da identidade deveria ser colocado de modo a responder simultaneamente a um conjunto de problemas: os anseios justificados dos cidadãos, ligados à protecção das liberdades, privacidade e outras prerrogativas; as preocupações de segurança nacional, ligadas por exemplo à passagem de fronteiras e à autenticação de operações; e a eficiência funcional do “todo” público, ligada à reengenharia da Administração Pública numa orientação para o cidadão.

Estes problemas foram abordados com algum pormenor num estudo recente [2], que analisa as várias vertentes e enumera possíveis riscos, destacando os principais: furto, falsificação ou perda de identidade; violação da privacidade e do controlo sobre os dados pessoais; síndrome do número único; velocidade e automatização das fraudes; fidedignidade das fraudes.

No mesmo estudo são propostas algumas direcções estratégicas para a actuação dos poderes públicos, quer nas esferas que directamente dizem respeito ao Estado, quer naquelas que indirectamente deverão balizar a actuação e comportamento, direitos e deveres, das restantes partes interessadas (cidadãos, organizações, empresas).

Abordemos com mais detalhe algumas dessas questões numa perspectiva de governação.

As elevadas capacidades dos sistemas tecnológicos actualmente disponíveis facilitam tremendamente o acesso, a transmissão, a manipulação e dissimulação indevidas, o roubo e mesmo a chantagem sobre a informação. Levantam-se assim questões de protecção de privacidade, de segurança de activos e de práticas equilibradas na disponibilização de informação.

Os governos precisam de pesar diversos aspectos que são muitas vezes difíceis de harmonizar, como por exemplo: concretizar determinados serviços por razões de conveniência para o cidadão, mas que podem reduzir a sua privacidade e segurança; concretizar processos e sistemas destinados a identificar terroristas e outros criminosos mas que podem levantar dúvida moral; adoptar soluções de interoperabilidade com sistemas de origens diversas mediante soluções abertas, afectando porém o contrato social entre os cidadãos e o estado.

À medida que se vão integrando sistemas de informação e adoptando soluções tecnológicas mais evoluídas e modernas, normalmente com o objectivo de aumentar os benefícios para os cidadãos e/ou para os utilizadores de determinados negócios, surgem portais e outros pontos de acesso a múltiplos serviços na Web. Este tipo de serviços é normalmente caracterizado pela elevada fluidez e volatilidade, podendo aparecer, mudar e desaparecer em poucos instantes.

Essa evolução intensifica a necessidade de se aperfeiçoar a gestão de identidades, ou seja, a forma como são feitas as autenticações dos indivíduos, evitando o estabelecimento indevido e/ou a demasiada fluidez da identidade.

As políticas relativas a sistemas (técnicas e não técnicas) para operação no âmbito da Administração Pública e no domínio da gestão de identidades digitais devem ser forçosamente sensíveis aos quadros existentes: legal, económico e social.

No caso da Administração Pública, podemos considerar que a “gestão de identidades digitais” está baseada em sistemas que combinam tecnologia, procedimentos, práticas de actuação, leis e políticas que:
IDENTIDADE DIGITAL

i. Enquadram e suportam necessidades comuns de identificação em transacções envolvendo entidades estatais e governamentais e privadas.

ii. Permitem reduzir os custos de governação e melhorar a qualidade dos serviços das entidades públicas.

iii. Salvaguardam o recurso a mecanismos sancionatórios.

iv. Permite preservar ou melhorar a privacidade, as liberdades relacionadas com a identidade dos cidadãos, e a protecção de informações sobre pessoas e organizações.

No entanto, deve ser notado que estes sistemas tendem a adaptar-se às novas soluções tecnológicas de forma muito mais lenta do que estas evoluem. Utilizando uma imagem da teoria do controlo: a resposta do sistema é subamortecida. Todavia, estes períodos de adaptação dos sistemas às novas soluções abrem muitas possibilidades para a ocorrência de falhas não previstas, quer legais, económicas ou sociais.

Em Portugal, a gestão de risco e gestão da mudança face às novas tecnologias mantém-se algo difusa, não sendo evidente que factores e tendências serão mais relevantes e influenciariam decisões (de âmbito nacional) a médio e longo prazo.

Actualmente verifica-se uma pressão natural e habitual por parte do sector privado sobre a governação para se adoptarem determinadas soluções de gestão de identidade digital sem previamente serem acuátelados os factores de risco e o processo de planeamento e gestão da mudança, mormente no que respeita à protecção efectiva da esfera privada dos cidadãos.

Recorde-se a este respeito um parecer produzido recentemente pela Comissão Nacional de Protecção de Dados [3], relativo ao Cartão de Cidadão, que permite prever a ocorrência de modos de interacção digital com a coisa pública que possam vir a desproteger o cidadão, em sede de privacidade e não só.

Os cidadãos devem ter uma percepção clara das vantagens de migrarem para a ID. Isto é, os cidadãos ganharão uma confiança (trust) sólida na Identidade Digital, na medida em que esta for construída com base em processos e sistemas confiáveis (trustworthy).

Sem isso, trata-se de uma fé imposta, que será minada à primeira adversidade.

Tal só pode racionalmente ser conseguido se os processos e sistemas informáticos da Identidade Digital forem apresentados à sociedade com uma transparência e simplicidade tais que se torne possível a esta organizar-se de modo a compreendê-los, analisá-los e avaliá-los de forma independente, e/ou fazer o mesmo com os próprios estudos produzidos necessariamente pelos “donos” desses sistemas de ID (administração pública, sistema financeiro, outras empresas).

Torna-se oportuno assinalar que, no que respeita às vertentes de segurança e de tecnologia dos mais recentes símbolos da ID no nosso país--- o Cartão de Cidadão e do Passaporte Electrónico Português --- existem algumas razões de preocupação, assinaladas por várias fontes [2-4].

Cabe ao Estado e à sociedade actuar no sentido de evitar que daí derivem problemas de monta que, uma vez minada a confiança no sistema, sejam de difícil retorno. Relembrando o que foi dito no início deste breve texto, é a procura do equilíbrio simultâneo entre os vários pilares (sociedade, leis, polícia e tribunais, segurança e tecnologia) que assegurará soluções eficazes para o Estado, aceites pelos cidadãos,
preservadoras dos seus direitos e garantias, e inclusivamente melhoradoras de certas facetas da vida social.

**Bibliografia**


**Nota**
Este texto foi previamente publicado no número 139 (Setembro de 2007) da Revista Interface Administração Pública, e é aqui reproduzido com o acordo da respectiva Direcção.

Lisboa, 2007.10.19