Sociedade da Informação, Sociedade (in)Segura?

Paulo Esteves Veríssimo

Faculdade de Ciências da U.Lisboa

pjv@di.fc.ul.pt

Resumo

A construção da Sociedade da Informação (SI), como desígnio, é não só inevitável, como desejável. "SI" é muitas vezes assimilado a "tecnologia", perdendo-se então o primordial nexo de causalidade de dever a tecnologia estar, incondicionalmente, ao serviço da SI, e não o contrário. Posto isto, pretendem estas linhas analisar se a tecnologia tem estado ao serviço da sociedade, despistar ocasiões em que tal possa não estar a acontecer, e avaliar uma possível contradição específica que, a existir, iria contra o propósito social da SI que atrás enunciámos: *poderemos, com a sociedade da informação, estar a caminhar para uma sociedade menos segura*? Fá-lo-emos portanto ao longo da pista da segurança informática, e das implicações sociais da insegurança do ponto de vista dos cidadãos e dos parceiros sociais. No decorrer deste texto, analisaremos vertentes muito importantes desta questão, como: Identidade Digital; Privacidade; Democracia Electrónica; Transacções Electrónicas; Infraestruturas Críticas.

Palavras-chave: Segurança Informática; Infraestruturas Críticas; Identidade Digital; Privacidade; Democracia Electrónica; Transacções Electrónicas.

1 INTRODUÇÃO

A construção da Sociedade da Informação (SI), como desígnio, é não só inevitável, como desejável. E assim tem sido em Portugal. Como em todas as construções, é preciso saber se têm um bom plano, se o seguem, se as matérias-primas e as técnicas de construção são adequadas. Passando da metáfora à realidade, há questões que devemos analisar: SI quer dizer tecnologia (leia-se tecnologia digital, computadores, redes)? Quanto mais tecnologia tivermos, mais "SI" somos? Ou SI quererá primeiramente significar que o acesso alargado à informação, como patamar do acesso ao conhecimento, enriquecerá o cidadão, criará uma sociedade melhor? Nesse caso, não terão as tecnologias de estar, incondicionalmente, ao serviço desse *plano*, desse desígnio, e ser portanto, em primeira instância, *adequadas* a ele?

Posto isto, pretendem estas linhas analisar se a tecnologia tem estado ao serviço da sociedade, despistar eventuais ocasiões em que tal possa não estar a acontecer, e avaliar uma possível contradição específica que, a existir, iria contra o propósito social da SI que atrás enunciámos: *poderemos, com a sociedade da informação, estar a caminhar para uma sociedade menos segura*?

Fá-lo-emos, como o leitor terá adivinhado, ao longo da pista da segurança informática, e das implicações sociais da insegurança, vistas por isso, maioritariamente, pela perspectiva dos cidadãos e das instituições e empresas enquanto parceiros sociais. No decorrer deste texto, analisaremos vertentes muito importantes desta questão, como: Identidade Digital; Privacidade; Democracia Electrónica; Transacções Electrónicas; Infraestruturas Críticas. De facto, o problema é mais lato do que a segurança, tem de ver com dominarmos a tecnologia ou sermos dominados por ela. Infelizmente, o que está em jogo ultrapassa largamente os dissabores da história do aprendiz de feiticeiro. A tecnologia não se cria sozinha, ainda é feita por humanos e aqueles que a fabricam e configuram têm sobre ela um controlo avassalador. A

insegurança informática apenas acrescenta a este universo os que se podem aproveitar maliciosamente das dificuldades de quem não domina a tecnologia.

2 IDENTIDADE DIGITAL

A identidade digital (ID) tem estado na moda, mas nem sempre pelos melhores motivos. A identidade digital, mais do que uma tecnologia que dá um toque moderno às sociedades, é acima de tudo uma pedra de toque do caminho para a sociedade da informação. A ID deve vir ajudar a resolver problemas, e os problemas que ela resolve devem ser mais do que aqueles que ela cria.

Nos países que possuem bilhete de identidade físico--- e são bastantes--- a confiança no mesmo é uma questão fulcral de solidez da sociedade e mesmo assim é sabido que se prestam a falsificações e fraudes. A opção ID deve reunir consenso em volta da confiança: introdução de tecnologias seguras e robustas; inclusão de procedimentos transparentes de verificação, teste e certificação; garantia de auditabilidade pela sociedade. A ID deve incondicionalmente respeitar os níveis de privacidade existentes com a identidade física, ou até melhorá-los. Isto sim, seria uma demonstração incontestável das vantagens da migração para a ID. Os cidadãos são obrigados a ter B.I., não é uma opção, portanto a evolução para o B.I. digital não pode nem deve comprometer qualquer direito dos cidadãos.

Por exemplo, seria grave que, por termos migrado para cartões de identidade digital, pudessem entidades não discriminadas (por exemplo, um porteiro de um cinema, um segurança de um edifício) ter acesso não só ao nosso número e dados de identidade civil, mas também e de uma vez só, aos de identificação fiscal, segurança social, etc., sem a nossa permissão. Seria igualmente grave que, como cidadãos, não pudéssemos *justificadamente confiar*, isto é, ter uma certeza fundamentada que, em operações digitais feitas com o tal cartão digital, não era possível, inadvertida ou maliciosamente, aceder a, ou mesmo modificar indevidamente dados do cartão.

Um cartão de ID deve ser pelo menos tão robusto quanto o antecessor físico. A lusitana ofuscação pelas tecnologias pode levar-nos a crer quer sim sem muito pensar, mas não é bem assim. Um cartão de ID tem de facto um chip e esse chip é um computador. Tem um programa, e fala com outros computadores, os leitores/escritores do cartão. Portanto, sofre potencialmente de todos os males congénitos dos computadores dos nossos dias, só que na utilização de um cartão de ID os problemas não se resolvem fazendo *reset*, ou aplicando um *patch*, ou fazendo *updates*, para usar linguagem muito em voga. Estes sistemas, por serem críticos, devem ser desenvolvidos e operados a níveis superiores de exigência. Percebe-se assim que as questões da robustez e da credibilidade acima mencionadas, bem como a sua certificação por entidades independentes e da confiança dos cidadãos, são factores chave, não alienáveis, da introdução de qualquer sistema de ID.

Na verdade, alguns especialistas advogam que um cartão de ID deve ser ainda mais robusto do que a alternativa física, pois a velocidade a que as fraudes se processam no mundo digital e a verosimilhança delas com operações genuínas aumenta significativamente o risco de danos de monta, materiais e pessoais, no caso de um problema. A velocidade a que se poderão (e podem já hoje) perpetrar fraudes em transacções digitais com IDs falsas escapa à nossa imaginação. Para termos uma pálida ideia, lembremo-nos das situações caóticas, na altura do rebentamento da bolha do mercado bolsista, causadas por programas de compra e venda automáticos que escaparam ao controlo. Essas transacções extremamente rápidas (mas que

comparadas com o mercado digital vindouro, se processaram à velocidade de um caracol) causaram danos inimagináveis antes que se conseguisse sequer perceber o que estava a acontecer. E eram, digamos, bem intencionadas...

Por outro lado, as fraudes podem atingir níveis de perfeição que as tornarão virtualmente indistinguíveis de operações verdadeiras, levando à criação de duplos digitais perfeitos, possivelmente operados por cibercriminosos, assombrando a existência de alguns cidadãos e causando o pânico nos já ciberófobos tribunais.

Porque nem tudo é mau, a utilização de tecnologias digitais pode abrir-nos um mundo totalmente novo, mais seguro, mais privado, mais responsável. A utilização correcta de pseudónimos digitais, por exemplo, permitir-nos-á criar várias personalidades digitais para diversos usos, incluindo transacções comerciais, protegendo a nossa anonimidade e privacidade, enquanto que manterá uma ligação segura à nossa identidade real, que nos responsabilizará enquanto cidadãos, nos necessários planos financeiro, fiscal, ou jurídico. Esta será aliás, uma das poucas formas seguras de libertar selectivamente parte das diversas identidades, como a fiscal ou a civil, ou outra informação pessoal que possa ser armazenada num mesmo cartão de ID.

No momento actual, o debate sobre a gestão da identidade está inevitavelmente ligado aos documentos de identificação oficiais, como é o caso do cartão do cidadão (CC) e o passaporte electrónico português (PEP), processos em que Portugal se encontra recentemente envolvido. Gostar-se-ia de ser mais optimista, mas é certo que os processos mencionados não terão obedecido a alguns dos pressupostos resumidamente explicitados acima, com as inevitáveis consequências nefastas já vindas a público, leia-se alguma imprensa técnica internacional acerca do PEP ter sido já quebrado, ou o parecer da CNPD acerca dos problemas de concepção do CC e sistemas associados. É fundamental que esses processos possam concretizar-se da forma mais vantajosa para a sociedade e ainda estamos a tempo de trilhar o caminho certo.

3 PRIVACIDADE

Ouve-se amiúde a frase «Mas porquê, eu não tenho nada a esconder!» quando se argumenta acerca da necessidade indiscutível de privacidade. Pior ainda é a réplica, em tom desconfiado, «Mas o que é que você tem a esconder?», a alguém que, cioso da sua privacidade, não quer, contra a usual bisbilhotice dos “burocratas de serviço”, fornecer mais elementos sobre si ou as suas acções do que os estritamente necessários.
Essa atitude vai permeando as sociedades e corroendo um dos mais desprezados direitos fundamentais, a privacidade, precisamente porque a maior parte dos cidadãos não compreende o que está em jogo se o perder, abrindo portas aos avanços da cupidez e controleirismo de empresas, políticos e administrações, a quem o fim da privacidade convém por várias razões, umas confessas, outras não. Triste unanimidade, de onde apenas sobressai a meritória e competente acção da Comissão Nacional de Protecção de Dados. Observamos, no nosso dia-a-dia português, como a erosão da privacidade acontece das mais variadas formas, com a complacência de quem a devia assegurar, e a omissão de quem se devia queixar da sua falta:

- A luta contra a insegurança, crime e terrorismo, tem desculpado tudo, esquecendo-se os zelotas do securitarismo de que a superioridade do estado de direito democrático se funda precisamente em lutar contra esses males dentro das próprias regras e garantias para os cidadãos. E que, ironicamente, tal como a necessidade aguça o

engenho, a necessidade de respeitar esse princípio tem sido um enorme factor de progresso (no fundo, a lição que aprendemos na série televisiva CIS). É mais fácil espiolhar sem restrições os ficheiros e comunicações das pessoas do que desenvolver sofisticadas técnicas informáticas e criptográficas que mantenham as coisas dentro dos princípios: perseguir os “maus” e proteger os “bons”.

- O surgimento de tecnologias que facilmente capturam e desvendam informação privada, como telefones com câmera ou vídeos de vigilância. Os atentados à privacidade devidos aos telefones GSM com câmera levaram alguns países a ponderar a obrigatoriedade legal de emitir som ao disparo da câmera. Os vídeos de vigilância, que antes gravavam em contínuo e analogicamente, sobrepondo gravações modernas a gravações anteriores na mesma fita, passaram a digitalizar e (pasme-se) a arquivar os resultados.

- O surgimento de serviços necessários ou úteis mas que são “bisbilhoteiros”, como câmeras de vigilância anti-fogo ou de supervisão de tráfego, localização de utentes de telemóveis, ou portagens automáticas. Em qualquer destes exemplos, pode-se polemizar acerca da “necessidade de sacrificar a privacidade”. Na verdade, fosse a privacidade considerada um bem importante e teriam em todos esses casos sido desenvolvidos métodos sofisticados e quiçá, avançados mesmo a nível internacional, para resolver o problema. Por exemplo: as câmeras de vigilância anti-fogo não devem guardar imagens de alta resolução dos cenários que vigiam, porque estão apenas em busca de infra-vermelhos, ou padrões de fumaça; as câmeras de supervisão de tráfego, pelas mesmas razões, não precisam mais do que capturar a densidade de objectos em movimento; a localização de utentes pelo telemóvel, se bem que aparentemente desejada por alguns respondentes a obscuros estudos de mercado, até nos EUA se está a tornar um assunto polémico; e finalmente, a utilização sistemática de dados de passagem em portagens para outros fins que não os da cobrança das mesmas deve ser liminarmente impedida por meios tecnológicos.

- Planos e modelos de negócio propositadamente destinados a recolher dados de consumidores, como sejam alguns cartões de fidelidade com extensos campos obrigatórios sobre o próprio, ou serviços de e-correio e discussão (*chat*) na Internet. Os cidadãos são frequentemente assaltados com a necessidade de preenchimento de um sem-fim de campos obrigatórios com informação pessoal quando, por exemplo, recorrem à assistência ou serviços de empresas comerciais e/ou fornecedoras de tecnologia. Este é um campo extremamente delicado, porque é o campo onde recusar pode significar exclusão do *chat on-line* onde «está toda a gente», ou do acesso a “toques”, músicas, programas grátis de vários *gadgets*, para muitos adolescentes e jovens.

- Dispositivos que furtivamente expõem dados privados, como os badalados casos de programas de PC que enviavam dados locais para fora da máquina, ou programas de PC mais ou menos maliciosos ou perniciosos, como *adware* e *spyware*. É interessante verificar o número de vezes que certos programas comerciais, quando lançados, tentam comunicar com a rede, mesmo quando lhes é dito na configuração que o utilizador «não tem rede». Tal comportamento é redutor da confiança nos sistemas informáticos, pois os cidadãos cada vez mais esclarecidos começam a não ver diferenças significativas em relação a outros programas (maliciosos) que recolhem informação na sua máquina e a enviam a outrem.

- Sistemas que inadvertidamente ou por inépcia expõem dados privados, por exemplo albergados em bases de dados de empresas indevidamente protegidas. A paranóia da

digitalização está a levar as empresas a arquivarem *on-line* dados pessoais e mesmo institucionais que anteriormente eram no máximo fotocopiados e guardados em armários. Números de cartões de crédito são apenas a conhecida ponta do icebergue. Essas empresas não são a maior parte das vezes capazes de garantir a segurança dos dados, nem necessitavam, em rigor, de os guardar, pelo menos mais tempo do que durasse a transacção em causa. Talvez se as medidas punitivas em caso de violação de privacidade fossem elevadas, começassem as empresas a pensar duas vezes antes de arquivar o que quer que fosse dos seus clientes.

- Entidades que exigem--- e muitas vezes expõem--- quantidades absurdas de dados privados que são depois albergadas sem qualquer garantia de segurança. Tal não acontece apenas em agressivas empresas comerciais. É frequentíssimo na administração pública a dois níveis: ficheiros de cidadãos requerentes, com informação exaustiva e mais do que necessária; e processos instruídos a mando de zelosos chefes obrigando as "vítimas do guichet" a disponibilizar quantidades astronómicas de informação, muita dela privada, desnecessária e, por vezes, sem mais fundamento legal do que um autoritário despacho. Mas a situação atinge igualmente instituições e empresas como vítimas e, por vezes, de modo potencialmente lesivo da sua competitividade. Qualquer organismo de suporte a fundos, de investigação ou de desenvolvimento empresarial, exige informação sobre as instituições numa qualidade e quantidade tal que prefigura "exposição de informação operacional confidencial". Esta informação, de valor estratégico e táctico, é hoje em dia quase toda convertida em formato digital e depois permanece guardada em servidores desses organismos gestores, de segurança duvidosa, muitas vezes acessíveis sem muita dificuldade pela Internet. Serve pois de pouco a uma empresa tomar medidas para salvaguardar a sua informação estratégica e confidencial. O panorama da informação clínica não deverá ser muito melhor, tendo valido aos cidadãos ela não estar em grande medida digitalizada, bênção que está em vias de extinção. Estes são procedimentos comuns em Portugal, cujo efeito danoso se vai agravar à medida que os materiais são digitalizados.

Na maioria dos casos acima existe uma omissão quase pecaminosa dos legisladores e dos reguladores, sendo que os maus exemplos muitas vezes vêm da administração pública. O armazenamento indevido de dados que leve ao seu comprometimento deve ser severamente punido. A interligação e a operação de repositórios de informação privada de outrem, de modo inseguro, deve de igual modo ser severamente punida. No fundo, trata-se apenas de transpor para o digital o que já é óbvio no domínio do social: ninguém se espanta se um funcionário for punido por ter permitido fugas de informação confidencial de um armário que se esqueceu de fechar à chave.

A perda da privacidade de dados pessoais por causa da utilização imprópria de tecnologias digitais pode causar catástrofes pessoais irreparáveis. É por vezes incompreendido o cepticismo de alguns mais esclarecidos acerca de operadores e fornecedores de serviços na Internet que impõem como cláusula aos utilizadores, alguma revogação de direitos à privacidade de dados pessoais albergados, transaccionados ou transmitidos por eles. Estão nessas condições por exemplo, o Microsoft MSN, ou o Gmail. O facto é que conversações e vários dados da esfera pessoal podem assim ficar registados incondicionalmente e *ad aeternum* por outrem. Esses dados podem, com muita naturalidade e legalmente, com o consentimento dos donos, entrar no circuito comercial por onde já andam muitas das informações que inadvertidamente os cidadãos fornecem quando por exemplo pedem um cartão de uma qualquer loja ou marca. Mas podemos pensar em coisas mais sinistras, por exemplo, nos danos que os adolescentes de hoje podem fazer à sua vida profissional

futura, por tratarem o ciberespaço como um gigantesco prolongamento da candura e irreverência do seu quarto ou da mesa de café dos amigos. Universidades (e empresas concerteza...) pesquisam hoje avidamente na Net, em lugares de encontro como o MySpace ou o Hi5, num rasto deixado ao longo de vários anos, elementos acerca de candidatos, que assim poderão falhar, muitas vezes sem saberem porquê, uma oportunidade merecida.

Os adeptos do "não-privado" deviam perceber, através de exemplos deste tipo, o que quer dizer «O direito a estar sozinho» e que, se abdicar dele pode trazer custos individuais, ser o mesmo coartado numa sociedade em geral será desastroso.

4 DEMOCRACIA ELECTRÓNICA

Democracia electrónica envolve toda uma tradução e transferência dos processos tradicionais do funcionamento da sociedade democrática, para a esfera digital. Vamo-nos concentrar no aspecto mais emblemático: a *votação electrónica*.

Há certamente várias razões para uma sociedade enveredar pela votação electrónica, das quais as principais serão: (i) Ajudar a assegurar as condições básicas para eleições livres e justas, em sociedades em que essas condições possam estar ameaçadas, por exemplo, por fraude ou pressão. (ii) Melhorar as condições qualitativas das eleições num sistema já estável, por exemplo, a velocidade do escrutínio.

É pacífico que as sociedades europeias se encontram no segundo grupo, tendo os vários países vindo a equacionar ou a lançar o voto electrónico de forma mais ou menos prudente. É igualmente pacífico que certas sociedades emergentes caem no primeiro grupo e, tendo algum domínio sobre a tecnologia, obtêm um saldo positivo da introdução da votação electrónica, uma vez que, mesmo imperfeita e com falhas ou fraudes, a situação melhora drasticamente em relação ao processo tradicional. Já é atípico que sociedades evoluídas como os EUA tenham enveredado pela votação electromecânica e electrónica de modo generalizado sem serem asseguradas as devidas condições de controlo, segurança e fiabilidade, levando a situações inesperadas de falhas e mesmo fraudes, conhecidas porque reportadas não só na comunicação social mas também em artigos técnico-científicos.

Esta breve análise permite perceber que existem bastos sistemas de voto electrónico que são mais do que insuficientes, mesmo que apresentados como «estando presentes em vários mercados», porque como se viu acima, isso não é necessariamente prova de qualidade. Não parece salutar repetir os erros de outros, mas sim aprender com os mesmos. Não parece igualmente que a Europa, de um modo geral, esteja a avançar pela via da democracia electrónica de modo aventureiro.

Como perceber, então, se um sistema de voto electrónico serve os objectivos de uma democracia estável e evoluída como a portuguesa? Parece-me que há dois factores que deviam ser dados como garantidos face a quaisquer escolhas tecnológicas que fossem feitas: (a) manutenção da confiança dos cidadãos no sistema de voto; (b) condições de confiabilidade e segurança no mínimo ao nível das dos sistemas tradicionais. Significa isto que essas mesmas tecnologias devem justificadamente garantir que previnem: quebra do anonimato ou da privacidade; modificação ou eliminação dos votos individualmente expressos pelos eleitores; falhas de contagem ou de robustez do sistema; ou problemas de usabilidade.

Na verdade, em democracias estáveis, há algo a ganhar com a introdução de um sistema de voto electrónico, mas muito a perder se, por apressada, for imperfeita: as imperfeições só virão a ser descobertas depois do facto, e poderão ter consequências (fraude, perda de anonimato, colapso) que comprometam por longo tempo a confiança dos cidadãos e aí, sim, atrasando o progresso na via para a sociedade da informação.

Por exemplo, o processo de introdução de um sistema de voto electrónico deve começar por dar aos cidadãos garantias que eles compreendam: que a caixa que lhe põem à frente é pelo menos tão confiável como uma urna selada e que os botões que prime ou o cartão que passa é tão anónimo como o boletim de papel; ou que a "abertura" da caixa e contagem dos votos é tão séria como a abertura e contagem actual. Mas para isso é necessário que o sistema seja efectivamente merecedor dessa confiança. É imperativo que um sistema de voto electrónico obedeça a especificações que possam ser verificadas e auditadas, face ao projecto, concretização e modo de operação do mesmo, no sentido de saber se cumprem, além dos objectivos de funcionalidade, os de confiabilidade e segurança.

Ora a única forma de isto acontecer, dada a complexidade dos sistemas informáticos e criptográficos subjacentes, é que alguém em que o cidadão confie o faça por ele. Mas para isso é necessário que toda a informação possa ser escrutinada com toda a transparência, por entidades independentes, com a competência adequada e representando a sociedade. Será inadmissível e lesivo do conceito de sociedade democrática, basear um acto tão importante como a votação, em sistemas cujo funcionamento não se compreende, ou em que não se confia.

Seria uma inconsciência, depois dos variadíssimos azares conhecidos noutros países, avançar para um sistema de voto electrónico como se se estivesse a comprar mais um servidor ou *mainframe*, confiando apenas em especificações e «experiência noutros mercados» de um fornecedor por mais prestigiado que seja, ou decidindo com base em enganadoras demonstrações. O voto é uma operação crítica para a sociedade. Todas as operações críticas de cariz tecnológico são certificadas e auditadas nos países desenvolvidos (aeronáutica, telecomunicações, energia, etc.), porque não o haveriam de ser os sistemas da democracia electrónica?

5 TRANSACÇÕES ELECTRÓNICAS

O comércio e a banca, importantes pilares da actividade económica, continuarão naturalmente a sê-lo à medida que assistimos à digitalização da sociedade. O comércio electrónico tem vindo a desenvolver-se paulatinamente, mas a não ser que algo mude drasticamente, é a digitalização da banca, ou talvez mais propriamente do sector financeiro, que será o pivô de toda essa evolução. E se vimos há alguns anos atrás o pioneirismo da banca na introdução da informática na gestão da sua actividade, interna e interbancária, não observamos o mesmo sucesso na introdução da mesma informática para "vender", ou aquilo que se designa por B2C (do negócio para o consumidor), mormente no grande expoente deste negócio, a banca electrónica na Internet.

É estranho, se constatarmos que a banca é hoje um dos sectores mais competitivos e que, na arte de "vender" clássica, se tornaram mestres, passando facilmente das notas aos cristais, quando não seguros, imobiliária ou obras de arte (o famoso *cross-selling* pelo qual os sinos das bases de dados pessoais tocam...). Na verdade, a resposta para esta questão apaixonante parece residir menos em factores tecnológicos sofisticados (pois os bancos sempre souberam rodear-se de tecnologia quando assim

o quiseram) e mais, mas ironicamente, em alguns dos factores que fizeram o sucesso dos bancos de pedra-e-cal: intuição, conservadorismo, arrogância e complacência legal. Mas se foram factores de sucesso, porque ameaçam agora esse mesmo sucesso? Porque o mundo virtual é drasticamente diferente.

Durante muitos anos, a análise de risco foi iminentemente intuitiva e bem sucedida. «Qual o montante máximo de um cheque à caixa que se deve pagar sem verificar a assinatura?». Essa intuição ainda não se conseguiu transportar para os riscos do negócio virtual, talvez porque também não abundam as luminárias da informática nos conselhos executivos ou superiores dos bancos. Essa confiança exagerada leva à incapacidade de destrinçar situações extremamente arriscadas para o negócio, sejam elas a diferença entre falsificar uma assinatura num cheque ou falsificar um certificado digital, ou saber qual a efectiva autenticidade de uma palavra de passe, ou perceber que o PC de um cliente remoto não é «o próprio ao balcão», ou ainda qual é a diferença entre roubar PINs num ATM ou através da Internet.

Por outro lado, existe um conservadorismo político e tecnológico que faz os bancos cometerem relativamente poucos erros. Mas quando os cometem, custam a corrigi-los. O problema é que, na esfera digital, as coisas passam-se depressa demais. Tendo sido dos primeiros a utilizar a informática, os bancos tratam-na essencialmente como um custo e assim têm feito ao longo dos anos. No entanto, hoje em dia ela é não só um factor produtivo, como se está a transformar *no* meio de negócio: as agências de pedra-e-cal passam a virtuais, os clientes tornam-se agentes de software na web, as notas de euros passam a posições de memória num *smart-card*, as cabalísticas assinaturas caligráficas são substituídas por funções criptográficas. Esta evolução requer investimento, em tecnologia e recursos humanos de alto nível que dominem o negócio virtual, a informática moderna, e tem sido muito difícil aos bancos compreendê-lo. Assim, não espanta, no difícil domínio da banca em casa na Internet, ver-se repetidamente a aplicação de técnicas e tecnologias de segurança inadequadas, vindas de uma mistura de leitura fugaz de clássicos de criptografia e segurança e de tentativa de vitória por exaustão tecnológica.

Pode parecer surpreendente como tem escapado à compreensão dos bancos que uma percentagem significativa dos problemas de segurança das operações remotas via Internet, tipo *phishing* por exemplo, se deve à falta de autenticação do lado do servidor, em adição à do lado do cliente, o que se chama autenticação mútua. Na verdade, tal parece derivar de uma certa, digamos, arrogância, do tipo «Não temos de nos autenticar, somos um banco!». Essa arrogância pode ser compreensível no mundo real e, aliada ao conservadorismo, faz parte de um certo estilo distante de que as pessoas até gostam. No entanto, mais uma vez há um erro de perspectiva na compreensão do virtual. O ciberespaço é um palco de ilusionismo. Não chega dizer-se que se é, tem de se provar que se é. Se não nos passa pela cabeça desconfiar de que entrámos numa agência bancária falsa e pedir a identificação ao caixa, já o mesmo não se pode dizer de uma agência virtual. A experiência das máquinas ATM (que estão a meio caminho) com frontais falsificados deveria ter sido um sinal de alerta para os bancos. O não-temos-nada-a-aprender contrasta depois, em situações de aperto, com um certo deslumbramento com ditos ex-*hackers*, contratados como consultores de segurança, prática que, infelizmente, grassa nestes meios. Para que se compreenda o que é, na minha opinião, a asneira e o risco desta prática para as empresas e para os seus clientes, é como ir um banco ou operadora de telecom contratar uns (ditos-ex) arrombadores de fechaduras ao submundo para testar e *atestar* da segurança das fechaduras das suas sedes. Havendo escolas no País com excelente formação superior nesta área, é incompreensível que se contratem

arrombadores de computadores, em vez de engenheiros e arquitectos especialistas em segurança informática.

Esta filosofia é geradora de outro erro de perspectiva de igual quilate, que só não tem consequências de maior para os bancos devido à inadmissível complacência legal. Falo de os bancos considerarem o par <NomeDeUtilizador; PalavraDePasse> uma "assinatura" inequívoca de um cliente e de os responsabilizarem contratualmente por isso. Será como obrigar-se alguém legalmente através de uma assinatura fotocopiada e está na altura de ser esta aberração corrigida legalmente por mecanismos de protecção dos consumidores.

É essencial quantificar e fazer pagar os custos da falta de segurança informática. É essencial transferir para os operadores dos serviços *online* o ónus das falhas e fraudes, erradamente colocado do lado dos clientes e, por vezes, de forma injustificada. No entanto, há uma grave complacência legal nestas matérias, que permite que certas empresas façam do risco para o consumidor um modelo de negócio. Mais do que para o consumidor, esta situação é detrimentosa para as próprias empresas porque as desmobiliza de desenvolverem processos tecnologicamente mais evoluídos e por isso mais competitivos. Esta questão abrange os legisladores e/ou regulamentadores, sem cuja acção moralizadora as empresas não evoluirão para melhores práticas.

6 INFRAESTRUTURAS CRÍTICAS

Fala-se muito dos riscos que pendem sobre redes de electricidade, de gás e de água, da rede Internet e de telecomunicações, das redes de controlo de tráfego terrestre, aéreo, marítimo e de emergência. Todas estas infraestruturas pertencem àquilo que se designa por Infraestruturas Críticas (IC): sistemas cujo eventual mau funcionamento tem um impacto negativo significativo para a uma sociedade ou nação. Durante muitos anos, funcionaram mais ou menos bem, e discretamente, como convinha. Hoje em dia, um conjunto de factores fez a situação mudar drasticamente: liberalização de mercado; abertura a múltiplos operadores; computorização e interligação em rede; espectro do terrorismo.

A combinação destes factores tornou-se explosiva, sem que as sociedades se apercebessem bem das consequências. Por razões culturais, a análise de risco sobre ICs é frequentemente centrada numa de duas visões alternativas: considerar que infraestruturas virtuais só são atacáveis virtualmente; ou considerar que infraestruturas físicas só são atacáveis fisicamente. Na verdade, tanto um serviço web pode perecer por um ataque à bomba ao centro de dados, como uma central eléctrica pegar fogo por um ataque vindo pela rede. É esta última a questão mais preocupante, pois a computorização e interligação em rede trouxeram a possibilidade de se actuar remota e/ou automaticamente uma grande parte daquilo que, por exemplo, mantém a rede eléctrica a funcionar, nos põe água nas torneiras, permite fazer chamadas telefónicas, ou enviar mensagens de correio electrónico. Isto é, as ICs tornaram-se progressivamente "redes de computadores" específicas, em que alguns desses computadores, em lugar de receberem e-correio e navegarem na web, são controladores de máquinas eléctricas, de bombas de água, de sinais de tráfego, de estações de telefone móvel ou de radar, de comutadores e encaminhadores Internet. A estrutura física das ICs ficou assim exposta, quando antes só podia ser acedida local e internamente. Além disso, a exposição alargou-se com a abertura e interligação dessas redes, acabando por as tornar interdependentes. Isto é, tornou-se fisicamente possível que: um problema num ponto de uma IC alastre para toda a IC e para outras

ICs; que um problema físico numa IC seja causado a partir de um acesso remoto e virtual (por computador), vindo por exemplo, da Internet.

A liberalização de mercado e abertura a múltiplos operadores, uma realidade incontornável, complicou o cenário do ponto de vista da divisão de responsabilidades e da introdução de tecnologias digitais comercialmente competitivas mas, por isso mesmo, com um grau de vulnerabilidades apreciável. É esta a nova realidade trazida pela "informatização" das ICs clássicas, e pela proliferação dos serviços prestados através de meios informáticos. De tal modo que se convencionou denominar de Infraestruturas de Informação Crítica (IIC) as redes de computadores desempenhando funções críticas para a sociedade, incluindo não só a Internet e outras redes de informação, mas também o suporte informático do controlo e comando das redes de telecomunicações, controlo de tráfego aéreo e terrestre, eléctricas, água, etc.

É hoje em dia assente por vários peritos que: as vulnerabilidades das infraestruturas críticas são múltiplas; o nível e o tipo de ameaças a que estão sujeitas (i.e. o potencial de serem atacadas) varia com condições políticas, geográficas e mesmo temporais, tendo sido exacerbado por esta exposição imprevista. De tal modo que os riscos em que essas infraestruturas incorrem se tornaram muito mais difíceis de avaliar. Mas sendo os riscos possíveis, serão prováveis?

Dividamos os riscos em: riscos físicos acidentais, riscos físicos propositados, riscos informáticos acidentais, e riscos informáticos devidos a ciberataques. Ganha progressivamente corpo em vários sectores (ex. UE, EUA, Japão) que os riscos mais elevados se centram hoje nas Infraestruturas de Informação Críticas (IIC), e que pertencem à categoria dos ciberataques. Os ciber-riscos, isto é, os riscos para as ICs veiculados pela sua infraestrutura de informação e operação, tornaram-se mais importantes do que os riscos físicos. Isto pode ser difícil de compreender para o leitor não técnico, mas imagine-se o que será mais difícil de montar para um grupo agressor hoje em dia, para um mesmo efeito destruidor ou inibidor: uma série de ataques físicos à mão armada com explosivos ou *cocktails molotov* a várias sub-estações eléctricas; ou uma série de ataques informáticos a várias sub-estações interligadas, feitos remotamente pela Internet, até de fora do país em causa, que provoquem desequilíbrios e falhas em cascata, ou até danos graves nas aparelhagens. Isto não quer dizer que vamos passar a ser atacados todos os dias, mas sim que o risco condicional para as infraestruturas é de um modo geral elevado e Portugal não é excepção. Isto é: existindo um conjunto de ciber-ataques com a potência e precisão adequadas, o risco de falha das infraestruturas críticas é elevado.

A Internet e a interligação global são inegavelmente o veículo destes ataques. As vulnerabilidades dos sistemas são deficiências e insuficiências dos fabricantes, operadores, utilizadores e em última análise legisladores e governantes. Existe ainda uma margem de resistência que deriva do facto de os sistemas de controlo serem de modo geral fechados, obscuros, de gerações informáticas anteriores, e por isso menos conhecidos e mais difíceis de atacar. É um avanço ilusório, que se esfumará quando começarem a ser divulgados na Internet os primeiros métodos de ataque a sistemas informáticos de controlo, assim como o foram há uma década as receitas de ataques a sistemas clássicos na Internet. O cenário de evolução das ameaças pode vir a ser muito semelhante se nada ou pouco for feito, excepto na dimensão dos danos físicos possíveis. Além de que essas vagas serão as testas-de-ponte, as plataformas de ensaio, que poderão permitir ataques precisos, profissionais, dirigidos, tal como aconteceu na Internet.

O esforço que as sociedades dedicaram a tornar as suas ICs mais modernas, operacionalmente seguras e eficientes, tornando mais eficaz a gestão e supervisão dos riscos físicos das mesmas (sistemas de supervisão e de controlo remoto (*SCADA*), redes de sensores, etc.), revelou-se afinal uma faca de dois gumes. Devemos portanto começar de novo, urgentemente e sem hesitação, disponibilizando os meios necessários para estabilizar e neutralizar esta nova ameaça, desta vez às IICs, a face cibernética das mesmas.

Estão as nossas infraestruturas críticas seguras em relação a ciberataques? Sendo a rede eléctrica uma das mais delicadas, compreendemos, por exemplo, o que um ataque bem sucedido à infraestrutura eléctrica pode fazer? Nem mesmo os poderosos EUA se sentem seguros disso, pois citando um colega nos média locais: *"what's a superpower without power?"* (O que é de uma superpotência sem potência (eléctrica)?)

A negação da realidade não vai ajudar a sociedade. É necessário pôr no terreno as medidas adequadas, numa área em que pode haver auto-suficiência nacional, começando pelos aspectos tecnológicos: suporte inequívoco à investigação e desenvolvimento de arquitecturas informáticas inovadoras para infraestruturas de informação críticas e investimento na sua concretização, com partilha de esforços entre Estado e empresas. Este esforço deverá ser complementado com medidas societárias importantes: análises de risco que influenciem o planeamento e ordenamento territorial das ICs e moderem as suas interdependências; regulamentação eficaz acerca de segurança e confiabilidade informática, que seja de facto responsabilizadora dos fornecedores de tecnologia e serviços nos sectores abrangidos e punidora dos transgressores.

7 CONCLUSÃO

Tem sido muitas vezes dito: «Eis como nós, um país atrasado, poderemos utilizar a SI como grande fautor da necessária corrida de recuperação!». Não se pode estar mais de acordo com esta declaração de princípio. É verdade que Portugal tem tradição e condições para dar saltos qualitativos, por vezes contra a corrente ou de forma inesperada. O que é necessário é que a ideia acima não passe de um *slogan* passageiro. Esse desígnio pode e deve ser eminentemente nacional, mobilizador de todas as partes interessadas, e deve constituir-se como meta de longo prazo a atingir. Para que se não venha a dizer: «Eis como nós, não tendo pensado por nós próprios, não tendo sido capazes de escolher, decidir e criar o que seria melhor para nós, perdemos esta corrida e ficámos enredados em tecnologias que outros dominam, sacrificando irremediavelmente a nossa capacidade de auto-determinação, e ultimamente, o progresso prometido pela SI».