Repensar o Futuro da Sociedade da Informação

Segurança, Privacidade e Identidade Digital

Documento final

5º Fórum da Arrábida
20 e 21 de Outubro de 2006

Com o patrocínio da ANACOM

Segurança, Privacidade e Identidade Digital

O convento da Arrábida acolheu este ano mais um Fórum promovido pela Associação para a Promoção e Desenvolvimento da Sociedade da Informação, desta vez subordinado ao tema da Segurança, Privacidade e Identidade Digital. O quinto encontro contou com o patrocínio exclusivo da Anacom e continuou um processo de análise e reflexão sobre o que se considera ser o caminho para desenvolver uma Sociedade baseada na Informação e no Conhecimento, reunindo novamente um conjunto de personalidades que oferecem diferentes perspectivas sobre a matéria.

O tema da Segurança, Privacidade e Identidade Digital deu o mote às várias apresentações dos *keynote speakers*, mas acompanhou também os grupos de reflexão, que em sessões de trabalho paralelas analisaram as várias componentes identificadas no tema geral.

Os trabalhos foram iniciados com o tema da Segurança na Sociedade Moderna, abordado pelo Tenente-General José Garcia Leandro, seguindo-se a Privacidade e a Sociedade da Informação, temática a cargo de Luís Lingnau Silveira, presidente da Comissão Nacional de Protecção de Dados. No primeiro debate plenário estenderam-se as discussões sobre os dois temas, aliciando os participantes do encontro para a troca de ideias nas sessões paralelas.

A segurança na Sociedade Moderna

O mundo está a entrar numa nova Era que se faz anunciar através de um conjunto de sinais premonitórios. A tese é do Tenente-General José Garcia Leandro, *keynote speaker* no primeiro painel da 5ª Edição dos Encontros da Arrábida e suporta-se num conjunto de 20 indicadores que fazem adivinhar mudanças radicais no equilíbrio de forças que suporta a teia mundial de relações internacionais, conduzindo a um novo capítulo da história.

O conjunto de sinais que se conjugam (alinhados em caixa) só podem, na opinião do Tenente-General, conduzir a um de dois caminhos: o reforço de cooperação global, como forma de evitar um conjunto de novas ameaças que se afirmam um pouco por todo o mundo, abalando o equilíbrio de poderes que ao longo das últimas décadas tem assegurado estabilidade; ou um confronto global materializado numa quarta guerra mundial que já não se rege pela mecânica nem pelas motivações das guerras tradicionais: espaço ou ideologias. O teatro de operações é agora o mundo e a única ideologia a economia liberal, defende.

11 de Setembro abriu caminho para uma mudança inevitável

Os cenários apresentam-se como o culminar de uma mudança que se iniciou com o 11 de Setembro, pedra de toque para uma tentativa de mudança do sistema mundial que se torna mais premente à medida que um conjunto de outros aspectos se conjuga.

Às fragilidades das alianças que garantem a estabilidade mundial juntam-se factores como a emergência de novos Estados (como a China), a crescente ameaça do terrorismo transaccional e das armas de destruição maciça, que cresce sem base territorial, como ilustra o fenómeno al-Qaeda, que ajudou a tornar claras algumas fragilidades dos Estados Unidos enquanto potência hegemónica.

O Tenente-General referiu que desde o fim da Guerra Fria os Estados Unidos consolidaram um conjunto de poderes que lhes garantiram posição de destaque e liderança na cena internacional (poder nuclear, industrial, militar, tecnológico, aero-espacial, financeiro, orgulho nacional, entre outros). Um estatuto que se quer manter, como ilustram as políticas externas relativamente aos países árabes ou as guerras no Afeganistão e no Iraque. As mesmas acções que têm ajudado a mostrar fragilidades importantes, seja no campo militar, seja mesmo a nível interno, indicando mais um dos factores premonitórios apontado na tese de Garcia Leandro.

Vinte sinais premonitórios:

- Um mundo em rede
- Sacralização do mercado
- Drásticas alterações climatéricas
- Falta de recursos híbridos e energéticos
- Terrorismo transaccional e armas de destruição maciça
- Emergência brusca de novas grandes potências
- Crença de que não há limite para a expansão da ciência
- Tecnologia, informação e comércio: três poderes que a globalização tende a igualizar entre os Estados
- Poder das igrejas e diferenças e os diferentes modos como são encaradas
- Manipulação cientifica das massas pelos vários poderes
- Demografia e novas correntes migratórias
- Aumento da concentração urbana
- Deficiências dos poderes tradicionais aumentando os problemas sociais internos
- Alargamento do fosso entre ricos e pobres
- Os extremismos do desespero
- Os Estados falhados
- Confronto entre grandes potências
- Guerras assimétricas
- Enfraquecimento das regras de relacionamento internacional
- Grandes alterações dos comportamentos individuais

Poder tecnológico dissemina-se por vários Estados

Acresce o facto de poderes que historicamente se concentravam (tecnologia, informação e comércio) para dar poder a um Estado estarem hoje "espalhados por todo o mundo, criando uma tendência de igualdade do poder dos Estados" nota o Tenente-General.

O desenvolvimento tecnológico e científico é aliás referido como aspecto que contribui de forma decisiva para a mudança que, segundo defende, se aproxima. "A tecnologia é um dos factores que mais alteram o pensamento estratégico", defende Garcia Leandro. Da mesma forma, também a evolução científica produziu no homem a crença de que "vai resolver todos os problemas, o que altera a sua relação com o sagrado".

Esta mudança criou espaço para a emergência de fundamentalismos ligados ao contexto religioso, que em muitos países é indissociável do contexto político e serve de bandeira a acções de manipulação das populações, fragilizadas pelas questões ambientais, de sobre povoação, pobreza ou falta de recursos.

É ainda sublinhada a importância dos "Estados falhados" nesta relação de equilíbrio que garante a segurança da sociedade moderna. A expressão refere-se a países soberanos que por não se terem conseguido impor política e economicamente podem ser subjugados por inte-

resses e acabar por desempenhar um papel negativo relevante na cena internacional.

O Tenente-General confessa que, na sua convicção, a passagem para uma nova Era implicará um conflito global generalizado, que já começou e está a ser travado em várias frentes.

A segurança interna e externa dos Estados é cada vez mais um único e mesmo tema, endereçado em forma de cooperação no âmbito das alianças internacionais de segurança. Para Portugal fundamentalmente a União Europeia e a Aliança Atlântica.

Entrada no debate de ideias

A apresentação do Tenente-General José Garcia Leandro motivou um conjunto de questões que serviram de introdução à discussão que a seguir se iria desenrolar nos grupos de reflexão, alinhados em torno de três temas diferentes.

A independência da Europa face aos Estados Unidos em áreas estratégicas, como a segurança marítima ou energética, foi um dos tópicos principais de debate, com o responsável a considerar que a UE tem nesta matéria uma posição de clara dependência face aos Estados Unidos.

Também a necessidade de informar o cidadão para as questões da segurança que este pode enfrentar no dia-a-dia, enquanto cidadão de um mundo globalizado, foi discutida como as respectivas necessidades das estruturas governativas para este esforço de informação e de promoção da cidadania.

Garcia Leandro deixou ainda um alerta relativamente ao fim do serviço militar obrigatório, considerando que, a prazo, esta opção contribui para aumentar a falta de consciência para a cidadania nos diversos actores de amanhã - gestores, empresários, professores, sindicalistas, etc.

Privacidade no centro da Sociedade da Informação

Convidado para abordar o tema da Privacidade na Sociedade da Informação, o Dr. Luís Lingnau da Silveira, Presidente da Comissão Nacional de Protecção de Dados, partiu da premissa de que o conceito e a caracterização de privacidade têm sido alvo de uma discussão generalizada, utilizando um pensamento: "A melhor forma de caracterizar a privacidade é perdê-la".

O responsável da CNPD introduziu nesta questão dois paradoxos paralelos: o histórico e o geográfico. O primeiro traduz-se na ideia de que o conceito de privacidade nasceu e foi consagrado nos EUA – em 1890 foi criado o artigo que definiu a privacidade como "o direito a estar sozinho", em resposta a determinados abusos da imprensa norte-americana face à vida privada de personalidades mais ou menos relevantes –, mas as preocupações têm vindo a esmorecer. Nos últimos tempos, verifica-se um cuidado muito menor em relação à privacidade, sobretudo naquilo a que a dados pessoais diz respeito.

Mais do que isso, há uma tendência para se generalizar em vez de se proteger esses mesmos dados pessoais. Enquanto que a noção de privacidade se vai esbatendo no país que a "descobriu", na Europa esta discussão - sobre a privacidade, em geral, e sobre protecção de dados em particular - tem vindo em crescendo, em que se multiplicam as leis internas inspiradas numa directiva alemã.

No "velho" continente, os países legislaram internamente acerca das questões da privacidade ainda antes da integração europeia. Tanto na UE como na Europa do alargamento, a perspectiva geral é a de um respeito acrescido pela privacidade.

Paralelamente, o paradoxo geográfico coloca a Rússia, China e EUA fora do grupo de países envolvidos na batalha pela privacidade e pela defesa da protecção de dados. Luís Silveira justifica a ausência de China e Rússia pela "falta de respeito pela privacidade, que é típica dos regimes autoritários".

O presidente da CNPD também abordou um exemplo das diferenças existentes dentro da Europa: enquanto nos países do sul o rendimento das pessoas é considerado da esfera da privacidade de quem os aufere e é coberto pelo segredo fiscal, nos países escandinavos a perspectiva é a de "destapá-los" em favor de uma alegada democracia transparente. Em suma, o conceito de privacidade tem variado ao longo do tempo e difere em termos geográficos.

Esta questão aponta para a necessidade de análise do tipo de informação em causa: se provém da Administração Pública ou, pelo contrário, se diz respeito à intimidade das pessoas. "A CNPD rejeita a instalação de câmaras de vigilância nas vias públicas, excepto em alguns pontos estratégicos e apenas durante tempo limitado", ilustrou Luís Silveira.

A retenção de dados do tráfego de comunicações, utilizadas como instrumento fundamental pelas autoridades para a prevenção e investigação de actos de terrorismo ou outras práticas ilícitas, foram consideradas um exemplo "chocante" da violação da privacidade – embora sem culpa da sociedade da informação nem das tecnologias.

Também a questão do ponto de vista empresarial foi referenciada: quanto mais informações as empresas tiverem acerca do perfil dos

consumidores, mais facilmente a eles chegam e orientam o seu *marketing*, potenciado e reforçado pelas diversas tecnologias emergentes.

Em síntese, "a privacidade não é um valor absoluto, mas facilmente relegado para segundo plano perante determinadas situações de excepção", afirmou o interlocutor. Embora com um conteúdo que varie geograficamente e que ceda aos interesses públicos relevantes, a defesa da privacidade é um valor universal irrefutável.

"A privacidade deve ser um direito nosso", concluiu Luís Lingnau Silveira.

O futuro e a necessidade de fiscalização

À apresentação do Presidente da CNPD seguiu-se um período de debate com perguntas/respostas, cuja reflexão principal recaiu sobre o futuro: para onde caminhamos? "Não sei quais serão as futuras inovações tecnológicas, que certamente surgirão com muitos benefícios, mas introduzindo riscos acrescidos na privacidade dos cidadãos", apontou o orador, acrescentando que "será numa «luta» permanente no bom e no mau sentidos, na qual os países, como Estados-Membros, procurarão encontrar os seus equilíbrios".

Já no final da sessão, foi discutido o regime de protecção de dados: se este funcionar bem, conseguir-se-á uma redução de riscos. Existe a informação de quais as entidades podem ter acesso aos dados pessoais e, a partir daí, torna-se importante a fiscalização da sua actuação no processo de gestão da protecção de dados.

Um dos exemplos levantados é de que os registos não podem ficar eternamente ao dispor dessas entidades. Por fim, foi abordado um problema tido como ameaça real no contexto actual da sociedade: a ilusão das pessoas no sentido da existência de privacidade, quando, pelo contrário, se verifica uma generalização dos instrumentos para o abuso da utilização ilegítima da informação.

Percepção da Identidade Digital

A meio do dia, coube ao Professor Paulo Veríssimo a responsabilidade de enquadrar o terceiro tema em discussão, "A Identidade Digital". Para o orador, a questão da Identidade Digital faz parte do processo da Sociedade da Informação e é multifacetada, sendo que alguns dos problemas daquilo que se pode denominar "digitalização da identidade" resultam da percepção estreita dessa realidade.

O que significa que a Identidade Digital não deve ser abordada de uma perspectiva tecnocrática, comercial ou política, ou mesmo de uma perspectiva policial. O erro fundamentalista radical oposto é igualmente grave.

Na opinião de Paulo Veríssimo, a via para a Identidade Digital deve assentar numa perspectiva equilibrada entre as duas visões, que passe por cinco pilares: a sociedade, a lei, as polícias e os tribunais, a segurança e a tecnologia.

"Começa tudo com a Sociedade, por uma determinada ontologia acerca do ser, da identidade, da autenticidade", diz Paulo Veríssimo. A intenção é transpor para o digital aquilo que já funciona no domínio do social: pessoas, os papéis, os pseudónimos.

A lei é a segunda questão a observar quando se fala da passagem da Identidade Social para a Identidade Digital porque, segundo o orador, vai tornar obsoletas algumas noções antes aplicadas. Vai abrir vazios, por exemplo, em relação à criação de pseudónimos; não vai estar preparada para conceitos mais ricos ou mais complexos, como são os *avatares* e a biometria.

Face às polícias e os tribunais colocam-se problemas relativamente à velocidade e à perfeição. Nesta perspectiva temos que pensar no *timing* de acção/reacção entre criminosos e polícias e tribunais, na imaterialidade de algumas provas e da responsabilização e na esperada verosimilhança da identificação fraudulenta.

A segurança informática faz a ligação entre o conceptual – as leis, os tribunais – e a tecnologia. A tecnologia sem segurança não serve de nada. Quando representamos a identidade na vertente digital passamos para o mundo dos computadores, ficando sujeitos aos riscos inerentes a esse universo.

"Como crucial na vida social a identificação digital vai com certeza ser atacada, cabendo à segurança informática estudar as formas de a proteger", defende Paulo Veríssimo.

A tecnologia surge ao serviço dos pilares anteriores, gerindo, mantendo e verificando a Identificação Digital, sem comprometer direitos de cidadanias e o equilíbrio funcional das sociedades democráticas.

Panorama corrente

O orador afirma que hoje em dia existe uma atitude obsessiva relativamente à segurança que antes não existia e que resulta, em parte, de alguns enquadramentos legais e policiais que podem vir a prejudicar o conceito moderno de sociedade democrática. Deparamo-nos, então, com atitudes de recolha, digitalização e arquivamento dos dados biométricos dos cidadãos estrangeiros que entram em território norte-americano.

Na opinião de Paulo Veríssimo, a União Europeia titubeia neste campo, "manifestando uma notória falta de iniciativa e estratégia". "Ao submeter-se ao silêncio relativamente ao caso dos dados biométricos nas fronteiras norte-americanas, a União Europeia admite a primazia dos EUA, comprometendo de forma muito grave a sua liderança tecnológica em algumas áreas das TIC, áreas capazes de gerar as tecnologias necessárias para combater as ameaças sem militarizar a sociedade".

Ao abdicar da iniciativa política e estratégica em áreas chave onde tem avanço, a Euro-

pa poderá perder a iniciativa tecnológica. Um exemplo crítico reside nas normas e nas tecnologias de autenticação impostas pelos EUA, mas também no Passaporte Electrónico e nos sistemas de voto electrónico.

Uma questão de confiança

A identidade digital (ID) está a montante de vários outros processos críticos da sociedade da informação, como sejam a votação electrónica, o controlo de acessos incluindo a passagem de fronteiras, a digitalização de processos na Administração pública, de saúde e comércio electrónico.

Por outro lado, a identidade digital é a ligação umbilical dos cidadãos e de outros *stakeholders* à vertente digital da sociedade. "A falência da confiança na identidade digital, ou do equilíbrio entre os vários pilares da via para a ID, terá consequências dramáticas para a Sociedade da Informação", considera Paulo Veríssimo.

O orador partilhou com a assistência alguns cenários que se podem colocar em cada um dos pilares da via para a Identidade Digital, fazendo sobressair questões como o roubo da identidade, a automatização e a fidedignidade da fraude, entre outras, e que têm que se evitar.

A dicotomia privacidade/controlo de dados pessoais, a relação entre federação e cruzamento de identidades, as garantias e a certificação, a adequação das leis, a eficácia dos tribunais são igualmente questões que se colocam e que, na opinião de Paulo Veríssimo, só se resolvem com confiança nos processos e sistemas.

Questões a estudar

Em cada um dos pilares da via para a identidade digital há igualmente questões que deverão continuar a ser analisadas. É o caso das novas possibilidades que a identidade digital proporciona com a criação de avatares, pseudónimos e outras identidades alternativas, por oposição à identificação ou cartão únicos, no plano da sociedade.

Garantir que as tecnologias asseguram uma projecção precisa entre a identidade social e a identidade digital, no plano da tecnologia; caracterizar as ameaças e vulnerabilidades a que estão sujeitos os meios da identidade digital, no que diz respeito à segurança; caracterizar e enquadrar legalmente a separação de facetas entre identidade digital e dados pessoais, no sentido da protecção da identidade, no plano legal, e definir os novos desafios colocados pela utilização alargada da noção de identidade digital são igualmente pontos que, na opinião de Paulo Veríssimo, não deverão ser descurados

Dados lançados, a discussão prosseguiu nas sessões paralelas dos três Grupos de Trabalho, já estruturadas à volta de alguns tópicos que marcaram a agenda dos trabalhos.

Grupo de Trabalho - Segurança

Discutir a segurança faz surgir quase imediatamente questões relacionadas com o acesso à informação: quem e como se acede? Como é possível garantir qualquer tipo de acesso sem considerar primeiro a questão das infra-estruturas críticas que fornecem o suporte mais básico a qualquer sistema de informação, como sejam a energia eléctrica, por exemplo. Estas preocupações marcaram o ponto de partida dos trabalhos para o grupo que na 5ª Edição do Fórum da Arrábida reflectiu sobre o tema da Segurança.

Analisar a questão impõe uma visão sobre o seu carácter multidisciplinar e transversal. O primeiro revela a necessidade de encarar a segurança como uma questão educacional, que remete directamente para a área da formação. Trata-se de uma questão tecnológica/técnica e de uma questão cultural, defende-se.

Por outro lado, a sua transversalidade impõe um alerta para a necessidade de alterações profundas nas estratégias de actuação das empresas, considera o grupo, que reflecte sobre o facto de muitas vezes os atacantes dos sistemas de informação empresariais terem melhor preparação e maior *know how* que os "guardiães" da segurança nas instituições.

Isto acontece por não haver hoje, na maioria dos casos, uma prioridade clara das empresas para esta área. O problema surge ainda no ensino, que marginaliza o tema nos seus *curricula*, e intensifica-se já no terreno com a falta de capacidade dos responsáveis pelas áreas da segurança para justificar o retorno dos investimentos à gestão de topo, falhando na missão de posicionar a segurança como elemento crítico para o sucesso do negócio.

É neste contexto que o grupo sublinha a necessidade urgente de olhar para a segurança "num contexto de risco técnico", deixando para trás a visão redutora que muitas empresas têm nesta matéria. Isto implica também uma análise mais rigorosa das vantagens e desvantagens de algumas medidas de redução de custos, como o *outsourcing*, sempre que estão envolvidas áreas criticas do negócio.

Principais questões focadas

- ✔ Acesso à informação
- ✔ Infra-estruturas críticas
- ✔ Carácter transversal e multidisciplinar da segurança
- ✔ Noção dos riscos
- ✔ Educação e formação para a segurança
- ✔ Importância da certificação e boas práticas
- ✔ Papel das associações empresariais
- ✔ Papel da Administração Pública
- ✔ Importância das medidas de continuidade de negócio

Moderador
Pedro Veiga

Participantes
Aníbal Rodrigues
António Paiva Morão
Carlos Correia
João Chaves
João Taron de Oliveira
José Alegria
José Fernandes de Almeida
José Palma Fernandes
Luís Barata
Ricardo Machado

Tomar consciência dos riscos é prioritário

A falta de consciência dos riscos é também

eleita como um dos principais problemas a combater na esfera dos utilizadores particulares de Sistemas de Informação, até para vencer receios e desconfiança nos meios electrónicos. Importa que também este público perceba o que implica fazer parte de uma sociedade em rede, uma tarefa que deve contar com o auxílio dos prestadores de serviços e dos fornecedores de tecnologia. Seja através de associações empresarias e outros organismos colectivos, seja de forma directa e pró-activa.

A informação e a formação são propostas de acção prioritárias para alterar questões educacionais e prioridades, seja no campo das empresas ou da sociedade em geral. É preciso que a formação mais básica, introduzida logo nos primeiros anos do ensino, seja ministrada por professores, também eles formados, da mesma forma que é preciso rever conteúdos programáticos no ensino superior e apostar no *long life learning* nas empresas, trazendo a segurança para um plano mais central. "A segurança é intensiva em conhecimento", concordou o grupo, sem deixar de referir que aspectos como a falta de recursos especializados (nas PMEs) e as questões de *time-to-market* muitas vezes conduzem à não assunção deste facto.

De qualquer forma interessa vincar que a tecnologia não é uma solução para resolver as questões de segurança - embora crie muitas vezes essa ilusão -, um conselho que se dirige sobretudo às empresas e que alerta para o facto de "estar protegido" não depender apenas de elevados *budgets* para investir em moder-

nas ferramentas, se os recursos não estiverem bem formados e se não existir uma política de partilha de informação e de coordenação de esforços entre gestão, informática e segurança. É essencial formar *Chief Risk Officers*, sublinha-se.

Boas práticas e certificação, essenciais para cultura da segurança

Face ao diagnóstico, torna-se essencial levar a cabo um conjunto de medidas que ajudem a mudar mentalidades e estratégias que acompanhem as mutações do próprio conceito de segurança. Nas organizações (públicas e privadas) é fundamental uma participação mais activa no campo das normas de segurança e das boas práticas, sobretudo quando estão em causa infra-estruturas críticas. A Administração Pública deve aliás assumir a posição de divulgadora dessas boas práticas.

É sublinhado o desconhecimento e até alguma desconfiança relativamente às normas de segurança, sobretudo no que se refere às normas internacionais adaptadas de grandes contextos para a realidade do mercado português que é preciso contornar. No campo empresarial junta-se à formação a necessidade de adoptar medidas de continuidade de negócio que protejam os Sistemas de Informação das ameaças do Mundo Digital.

Mudar o cenário é uma tarefa de todos, a começar pelo indivíduo, que deve procurar compreender melhor o alcance das novas ferramentas postas à sua disposição. É também uma tarefa das escolas, das empresas, dos gestores e dos políticos.

Embora seja uma construção do homem, a Sociedade da Informação impõe que sejam mitigados riscos que estão cada vez mais um pouco por toda a parte. Afinal os Sistemas de Informação estão dentro de quase todos os dispositivos que usamos no nosso dia-a-dia, para as tarefas mais simples ou mais complexas, e as ameaças de segurança vão para além dos vírus ou do *spam*.

Grupo de Trabalho - Segurança
Conclusões

Propostas e Recomendações

- Criação de campanhas de formação e informação dirigidas à difusão de uma Cultura de Segurança e de boas práticas no Mundo Digital
- Associações profissionais e empresariais devem preparar os seus associados para os desafios de segurança dos sistemas de informação e das redes
- Sensibilizar os gestores de topo das organizações para a necessidade da segurança dos sistemas de informação e das redes ser vista como um factor crítico de sucesso
- A Administração Pública deve implementar políticas de segurança dos sistemas de informação e das redes, desde a concepção dos sistemas à sua exploração. Deve ainda formar os seus dirigentes, quadros técnicos e utilizadores internos sobre os problemas de segurança no mundo digital
- A Administração Pública deve ainda concretizar políticas e planos de continuidade de negócio em sistemas fundamentais do Estado
- Concretização de políticas de informação, dirigidas ao público em geral, sobre as boas práticas no domínio da segurança dos dispo- sitivos digitais
- As empresas devem assumir as suas responsabilidades na criação e aplicação de normas, recomendações e boas práticas na área da segurança dos sistemas de informação, das redes e das infra-estruturas de suporte
- Incluir nos programas escolares do ensino nas áreas das TIC os aspectos específicos aos desafios de segurança na Sociedade da Informação
- A nível do ensino técnico, profissional e superior devem ser criados cursos especializados na temática da segurança na sociedade da informação

Grupo de Trabalho - Privacidade

O grupo de trabalho iniciou a sua discussão sobre o tema a partir da questão "No conceito de "privacidade", do que estamos a falar?". Em primeiro lugar, à condição de qualquer cidadão ser "dono" da informação a que lhe diz respeito e não abdicar disso. No entanto, chega-se facilmente à realidade de que todos gostaríamos de ser "donos" dos nossos dados pessoais, mas sabemos que não somos (por exemplo, basta ter uma ligação permanente à Internet para perder essa condição desejável).

Então, a privacidade é apenas um preâmbulo da liberdade individual e nunca pode ser um parâmetro absoluto. "A privacidade é um direito relativo, tanto quanto o é a nossa liberdade", sublinha-se. Aceitando a definição de *right to be alone*, dever-se-á acautelar o controlo de quem tem acesso aos nossos dados ou registos.

Há duas alternativas: ou se assume um comportamento marginal (pouco recomendável), ou faz-se parte integrante de uma comunidade que interage com cada cidadão – mas essa interacção pode ser efectuada sem violar a sua privacidade.

Há, no entanto, níveis de informação pessoal cuja partilha não preocupa, ao contrário de outro tipo de registos pessoais e relativos à própria privacidade (informação privada íntima). Foi dado o exemplo da Internet: a maioria das pessoas que autoriza a utilização dos seus dados/ registos electrónicos não conhece os riscos inerentes e está, a partir daí, sujeito a uma devassa total. Neste caso, cumpre aos Estados promover campanhas maciças de esclarecimento para uma consciencialização dos potenciais riscos em que os cidadãos incorrem aquando do fornecimento de informação pessoal.

Pontos de Partida

- ✔ Confidencialidade dos dados pessoais
- ✔ Quadro legal dos aspectos de privacidade no mundo digital
- ✔ Tecnologia de apoio e suporte à privacidade
- ✔ Fraude informática

Moderador
João Álvaro Carvalho

Participantes:
António Augusto Fernandes
Filipe Montargil
Henrique O'Neill
João Matias
José Amaral Gomes
José Gomes Almeida
José Matos Pereira
Luís Vidigal
Rui Baião

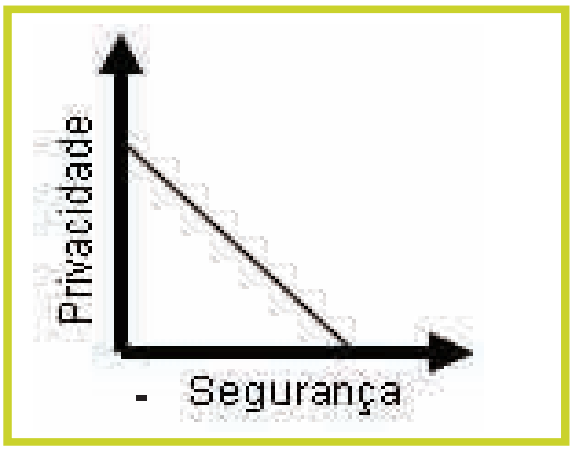
Qualidade de vida e direito à informação

Foi referida a relação entre a privacidade e a segurança e qualidade de vida: quanto maior for a segurança e a qualidade de vida, menor será a privacidade (por exemplo, no seu direito a ser protegido, o cidadão abdica da sua privacidade). Assim, a privacidade é a esfera do que é privado, exigindo-se uma articulação com o domínio público. A questão da identidade é feita a partir deste último, mas existem registos pessoais que são públicos e outros não.

Quando me relaciono com o Estado, com empresas ou com outros indivíduos, tenho de admitir a minha esfera do privado, defendeu

o grupo, acrescentando o "direito ao esquecimento", ou seja, a possibilidade de determinada informação desaparecer com cada indivíduo, desde que não interfira com os direitos de outrem (limitar a privacidade à esfera do colectivo).

Debateu-se então se temos o direito de saber informações de outros. Sim, à partida, mas dependendo da contextualização. O que acontece, por vezes, é que a privacidade é violada inconscientemente. A informação que é recebida sem se ter a noção que é privada ou



confidencial e, depois, é difundida sem essa limitação.

Sobre a liberdade de pensamento, o grupo lembrou que esta "sempre existiu e, antes da Revolução de Abril, a liberdade de expressão é que não existia". Acrescentou ainda que "a Igreja teve um papel de manipulação de consciências durante muito tempo, sendo hoje substituída por outros instrumentos", sendo que cada um deles "é eficaz no seu tempo". Chegou-se depois aos dois principais valores da privacidade: a liberdade (conjunto de direitos e relativizada pela igualdade e fraternidade) e o respeito pelo colectivo (não desrespeitar as regras do "jogo").

A ética na defesa da privacidade

Mais tarde, em torno da discussão foi introduzido o conceito de Ética pelo coordenador do grupo, como elemento básico nas normas que são legisladas para esta temática: "A existência de dados e registos sobre os cidadãos é inevitável, mas baseada numa ética". Nesta questão, a norma consigna a ética e cada instituição recolhe os dados estritamente necessários de acordo com a lógica da sua actividade num período de tempo suficiente.

O que se espera é que essa informação em causa não seja canalizada para outros fins (que não aqueles que se pretende) e que sejamos "proprietários" da mesma, no sentido do controlo da sua utilização.

O problema que surge é que a legislação, normalmente, está desajustada da realidade: "A realidade anda sempre à frente da Lei". Neste contexto, foi referido que a maior parte das fraudes têm origem interna (em pessoas que integram as instituições que têm acesso aos registos). Outro obstáculo referenciado foi a cultura de falta de segurança e de responsabilidade existente em Portugal (potenciada pela subcontratação).

Foi então definido o princípio básico da ética: guardar os registos pessoais apenas durante o tempo necessário. Sendo a ética traduzida por leis, todas as entidades que possuem ou acedem aos registos têm de informar a Comissão Nacional de Protecção de Dados do tipo de informação de que dispõem (e por quanto tempo).

A ética deve garantir um molde como os registos são tratados: não serem facultados a outras entidades para as quais não foram fornecidos, poderem ser verificados, mas não alterados por terceiros e garantia de sigilo profissional nas pessoas que têm contacto directo com essa informação (possibilidade de rastreio transparente e de responsabilização).

Complementarmente, tem de ser efectuada uma auditoria/fiscalização regular do sistema e reforçados os meios e a actuação da estrutura da CNPD. A ética, a cultura de segurança e a *accountability* não devem existir apenas na CNPD, mas em toda a Administração Pública e em toda a sociedade.

Grupo de Trabalho - Privacidade
Conclusões

Definição

- Parâmetro da liberdade individual a ser "ajustado" (não é algo absoluto e pertencer a uma comunidade implica relativizá-lo)
- Relação com a qualidade de vida
- Direitos dos indivíduos que assentam sobre valores fundamentais (liberdade)

Contextos

- Qualidade de vida - registos pessoais sobre os clientes e sobre as transacções efectuadas com empresas e Serviços Públicos
- Interesse colectivo - registos pessoais que viabilizam o controlo dos cidadãos relativamente ao não desrespeito dos seus deveres
- Segurança - registos sobre os cidadãos e sobre o seu comportamento (incluindo observações realizadas por vídeo, som, ou resultado da monitorização de comunicações) para efeitos da protecção do Estado e dos cidadãos

Ética para o tratamento dos registos

- Limitação dos registos ao estritamente necessário, durante o tempo necessário e devem ser tratados de forma confidencial
- Os registos não devem ser facultados a terceiros
- Possibilidade do cidadão verificar e corrigir os seus registos
- Responsabilidade da entidade "registadora" na protecção dos registos contra quebras de confidencialidade e acesso não autorizado
- Existência de sigilo profissional por parte dos colaboradores da entidade "registadora"

Caminhos/Soluções

- Criação de entidade reguladora do processo de utilização dos registos
- Desenvolvimento de mecanismos fiscalizadores da gestão dos registos (como são guardados e usados)
- Definir/autorizar:
  - O que é registado
  - Durante quanto tempo
  - Que tratamentos vão ser efectuados sobre os registos e com que finalidade
  - Que mecanismos para verificar quem acede a quais registos
- Responsabilizar entidades "registadoras"
- Permitir a rastreabilidade e a responsabilização ('*accountability*')

Perigos/ameaças

- Subcontratação e consequente enfraquecimento da responsabilização
- Falta de cultura de privacidade e confidencialidade (exibicionismo e '*voyeurismo*')
- Actos maliciosos (fraude, crime)
- Eventuais exageros nos mecanismos de segurança dos Estados
- Novas tecnologias e práticas comerciais

Recomendações práticas

- Sensibilização e consciencialização dos cidadãos relativamente aos riscos decorrentes da utilização dos serviços ('*awareness raising*')
- Reforçar os mecanismos que viabilizam a auditabilidade das entidades "registadoras" (privadas ou públicas) relativamente às autorizações que possuem
- Recrutamento de mais e melhores técnicos de auditoria informática
- Sensibilizar a classe política para a necessidade de:
  - Reforço dos recursos das entidades reguladoras e fiscalizadoras para o cabal cumprimento das competências
  - Maior articulação entre estas entidades para o aumento da sua eficácia
  - Maior pró-actividade para enfrentar todos os problemas e desafios

Grupo de Trabalho - Identidade Digital

Além dos pontos de partida fornecidos pela organização do 5º Fórum da Arrábida, o grupo de reflexão sobre a Identidade Digital propôs-se abordar outros aspectos que se consideraram importantes. Os tipos de identidade digital, a sua multiplicidade, a necessidade de informar o cidadão sobre os seus direitos e a regulação foram alguns dos temas que se discutiram durante as sessões.

Os trabalhos iniciaram-se com uma proposta de descrição do conceito de identidade digital, ou mais precisamente, das possibilidades que o conceito encerra. Neste contexto, a identidade digital foi sugerida como "algo que está ligado à pessoa física no mundo digital", "algo que permite que alguém se possa autenticar de várias formas no mundo digital". Algumas dessas formas já estão a ser utilizadas.

Diversidade e multiplicidade

"A tecnologia tem que fornecer meios de gerar/manter/verificar a Identidade Digital, sem comprometer direitos de cidadania e o equilíbrio funcional das sociedades democráticas".

Actualmente podem assumir-se diferentes identidades digitais: a que se escolhe quando se acede a um jornal *online* para ler as notícias, a que se mantém para se escrever num *blog*, a que se adopta para criar uma caixa de correio electrónico num prestador de serviços, e muitas outras que, na maior parte das vezes, já nem se recordam nem controlam.

Perante esta dispersão levantam-se algumas questões: a quem pertence a informação da Identidade Digital? Como é que se pode gerir essa utilização?

Neste momento é o utilizador que, na maior parte das vezes, controla quem tem os seus dados e de que forma, mas a evolução da Identidade Digital vai no sentido de atribuir ao sujeito digital a reivindicação de algumas propriedades, cabendo depois às partes confiantes verificar a sua autenticidade.

Antecipam-se igualmente alguns riscos, nomeadamente o roubo, o "forjamento" ou a manipulação da identidade digital. Nesta área, os membros do grupo consideram que a actividade da polícia e dos tribunais é muito complexa, sendo por isso fundamental investir na sua formação e nos meios de investigação, que

Moderador
José Pina Miranda

Participantes
António Serrano
Conceição Casanova
Francisco Tomé
João Catarino Tavares
José da Costa Ramos
José Dias Coelho
José Lopes costa
Leonel Santos
Luís Amaral
Luís Borges Gouveia
Paulo Veríssimo
Sérgio de Sá

Pontos de Partida

- ✔ Diferentes formas de Identidade Digital
- ✔ Benefícios e riscos sociais da Identidade Digital
- ✔ Roubo de Identidade
- ✔ O papel das entidades certificadoras

terão de ser tecnologicamente equiparados aos utilizados pelos infractores.

Tipos de Identidade Digital

"O direito à privacidade não nos iliba da responsabilidade da Identidade Digital"

No campo da evolução previsível é também possível considerar cinco tipos de identidade digital, consoante o contexto e o género de informação que fornecem: a relativa ao Cidadão, atribuída pelo Estado e que inclui os dados de identificação presentes no Bilhete de Identidade; aquela relacionada com as transacções *online*, normalmente outorgada pelo sistema financeiro e onde se inclui os dados necessários para a realização de compras através da Internet; a profissional, adjudicada pela entidade empregadora e que transporta informação necessária para utilização da Internet nas relações profissionais; a pessoal, disponibilizada pelo próprio e que integra a informação que cada cidadão considera suficiente para terceiros o identificarem *online*; e, por último, a de *browsing*, que inclui informação o mais reduzida possível para navegar na Internet.

Hoje em dia também se coloca cada vez mais a questão das identidades múltiplas: ou seja, cada pessoa tem ou pode ter várias identidades. Isso acontece porque há necessidade de autenticação da identidade física no Mundo Digital, porque há uma rejeição do mundo físico e da identidade real ou como factor de resistência à violação da privacidade, nomeadamente o recurso aos pseudónimos num *chat* ou num *blog*, num comentário *online*, de modo a preservar algum nível de anonimato.

Neste ponto pode distinguir-se claramente entre a Identidade Digital que se atribui ao cidadão - e que se prende maioritariamente com factores de identificação -, em contraposição à Identidade Digital que é possível construir.

Múltiplas Identidades Digitais

Existência de tipos diferentes de Identidade Digital, conforme o contexto em que a utilizamos, e incluindo conjunto de informação bem determinada:

- Cidadão – atribuída pelo Estado; inclui informação de identificação presente no Bilhete de Identidade;
- Transacção *online* – atribuída pelo sistema financeiro; inclui informação necessária para a realização de compras *online*;
- Profissional – atribuída pela entidade empregadora; inclui informação necessária para utilização da Internet nas relações profissionais;
- Pessoal – disponibilizada pelo próprio; inclui a informação que cada cidadão considera suficiente para terceiros o identificarem *online*;
- *Browsing* – inclui informação o mais reduzida possível para *browsing*.

Identidade Digital em português

"A falência da confiança na Identidade Digital terá consequências dramáticas na Sociedade da Informação"

A "materialização" da Identidade Digital em Portugal foi outro dos pontos discutidos pelo grupo de reflexão. Neste processo cabem o projecto do Cartão do Cidadão, o Passaporte electrónico Português e os Cartões de Crédito.

Pegando nos exemplos propostos pelo Estado, o grupo de reflexão considera ser necessário garantir a confiança nos sistemas envolvidos, nomeadamente a *framework* de serviços comuns e a plataforma de federação de identidade.

Neste campo será importante garantir a máxima transparência possível dos processos, nomeadamente possibilitando o acesso dos especialistas interessados a informação prévia sobre os projectos – especificações e requisitos – e

assegurando a auditoria e a rastreabilidade externas dos mesmos.

Dar a conhecer as reais vantagens dos projectos estatais em curso, assim como o seu impacto e funcionalidades, descortinando igualmente possíveis riscos e ameaças, é outro dos aspectos considerados fundamentais pelo grupo de reflexão para conseguir a tão necessária confiança da Sociedade Civil na Identidade Digital.

Propostas

Os membros do grupo de reflexão recomendam fortemente a criação de um "Regulador da Identidade Digital" com uma postura pró-activa, que poderia ser coordenado pela Comissão Nacional de Protecção de Dados (CNPD), auxiliada por um Conselho de Gestão Consultivo em que participariam outras entidades da Administração Publica, a identificar.

Este regulador seria também responsável por promover as alterações legais necessárias referentes às múltiplas identidades digitais e pela definição de regras sobre o tipo de informação que pode ser requerido *online*.

O grupo considera que a CNPD, no âmbito das funções que lhe seriam atribuídas na área da Identidade Digital, poderia igualmente recomendar boas práticas de utilização da Identidade Digital, organizando uma "Carta do uso social da Identidade Digital"

Grupo de Trabalho - Identidade Digital
Conclusões

Identidade Digital em Portugal:

- Passaporte Electrónico Português
- Cartão do Cidadão
- Cartões bancários

Em relação a este tipo de Identidade Digital é necessário garantir a confiança do cidadão nos processos utilizados e nas diferentes formas de aplicação.

Propõe-se que se actue nos seguintes sentidos:

- Garantir a divulgação da informação prévia para discussão
- Divulgar os processos associados com a identidade digital
- Tornar os processos transparentes
- Análise por especialistas, com análise de risco e respectivas recomendações,
- Garantir a auditabilidade e rastreabilidade externa

Adicionalmente, é fundamental divulgar publicamente as reais vantagens da Identidade Digital fornecida pelo Estado:

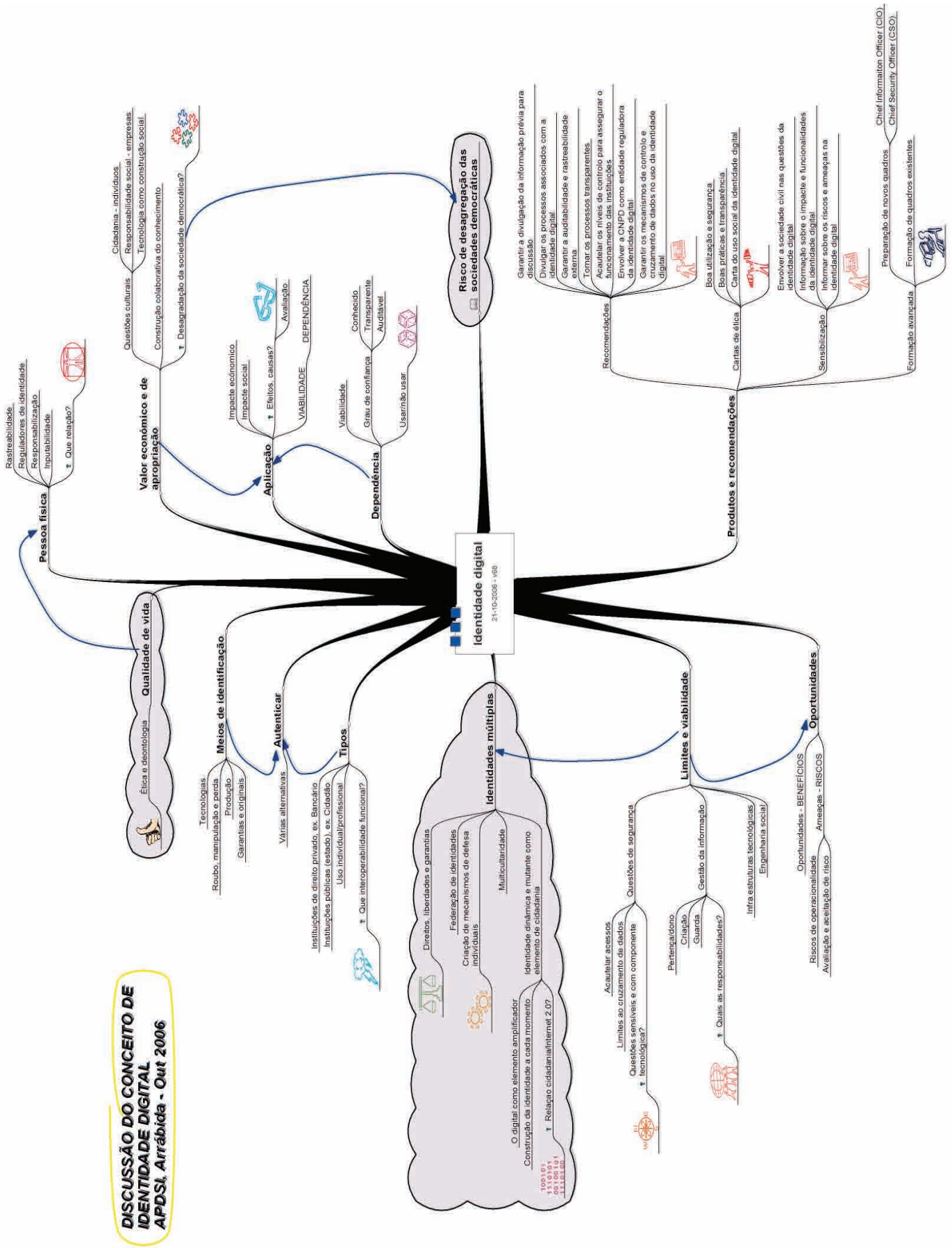
- Envolver a sociedade civil nas questões da Identidade Digital
- Informação sobre o impacte e funcionalidades da Identidade Digital
- Informar sobre os riscos e ameaças na Identidade Digital

É necessário motivar o interesse da sociedade civil e da opinião pública, propondo

- Movimento da opinião publica / cidadania que ajudem ao esclarecimento,
- Trabalho sério pela comunidade científica e tecnológica.

Recomenda-se fortemente a criação de um "**Regulador da Identidade Digital**" com uma postura pró-activa, que poderia ser coordenado pela CNPD com um Conselho de Gestão Consultivo em que participariam outras entidades da Administração Publica, a identificar.
Este regulador será também responsável por, entre outras coisas:

- Promover as alterações legais necessárias referentes às Múltiplas Identidades Digitais,
- Definir regras sobre a informação que pode ser pedida pelas empresas *online*,
- Recomendar a forma como deve ser disponibilizada informação sobre a Identidade Digital: raça, credo, … (Documento de ética),
- Recomendar boas práticas de utilização da Identidade Digital (Carta do uso social da Identidade Digital)


Identidade digital
21-10-2006 - v98
Pessoa física
Rastreabilidade
Reguladores de identidade
Responsabilização
Imputabilidade
Que relação?
Qualidade de vida
Ética e deontologia
Valor económico e de apropriação
Questões culturais
Cidadania - indivíduos
Responsabilidade social - empresas
Tecnologia como construção social
Construção colaborativa do conhecimento
Desagradação da sociedade democrática?
Aplicação
Impacte económico
Impacte social
Efeitos, causas?
Avaliação
VIABILIDADE
DEPENDÊNCIA
Dependência
Viabilidade
Grau de confiança
Conhecido
Transparente
Auditável
Usar/não usar
Risco de desagregação das sociedades democráticas
Produtos e recomendações
Recomendações
Garantir a divulgação da informação prévia para discussão
Divulgar os processos associados com a identidade digital
Garantir a auditabilidade e rastreabilidade externa
Tornar os processos transparentes
Acautelar os níveis de controlo para assegurar o funcionamento das instituições
Envolver a CNPD como entidade reguladora da identidade digital
Garantir os mecanismos de controlo e cruzamento de dados no uso da identidade digital
Cartas de ética
Boa utilização e segurança
Boas práticas e transparência
Carta do uso social da identidade digital
Sensibilização
Envolver a sociedade civil nas questões da identidade digital
Informação sobre o impacte e funcionalidades da identidade digital
Informar sobre os riscos e ameaças na identidade digital
Formação avançada
Chief Information Officer (CIO)
Chief Security Officer (CSO)
Preparação de novos quadros
Formação de quadros existentes
Meios de identificação
Tecnologias
Roubo, manipulação e perda
Produção
Garantias e originais
Autenticar
Várias alternativas
Tipos
Instituições de direito privado, ex. Bancário
Instituições públicas (estado), ex. Cidadão
Uso individual/profissional
Que interoperabilidade funcional?
Identidades múltiplas
Direitos, liberdades e garantias
Federação de identidades
Criação de mecanismos de defesa individuais
Multiculturalidade
Identidade dinâmica e mutante como elemento de cidadania
Relação cidadania/Internet 2.0?
O digital como elemento amplificador
Construção da identidade a cada momento
Limites e viabilidade
Questões de segurança
Acautelar acessos
Limites ao cruzamento de dados
Questões sensíveis e com componente tecnológica?
Gestão da informação
Pertença/domo
Criação
Guarda
Quais as responsabilidades?
Infra estruturas tecnológicas
Engenharia social
Oportunidades
Oportunidades - BENEFÍCIOS
Riscos de operacionalidade
Ameaças - RISCOS
Avaliação e aceitação de risco
DISCUSSÃO DO CONCEITO DE IDENTIDADE DIGITAL
APDSI, Arrábida - Out 2006

Segurança domina discussão plenária

No primeiro momento de discussão plenária desta 5ª Edição dos Encontros da Arrábida as intervenções marcaram a reacção ao *draft* de conclusões aí apresentado pelos grupos de trabalho. Na área da segurança mereceram comentários por parte dos participantes a falta de políticas adequadas por parte das grandes empresas para gerir os seus *assets* e a fragilidade das estratégias para estas áreas.

Os participantes discutiram ainda o que se considerou ser uma prática perigosa: o recurso a *hackers* para testar a segurança dos Sistemas de Informação empresariais, uma estratégia que já teve sucesso nos Estados Unidos e que acabou por cair em desuso mas que alguns dos participantes garantem não estar completamente posta de parte em Portugal.

Foi igualmente introduzida na discussão a falta de capacidade das agências seguradoras para gerir os prémios de seguros de forma a premiar a gestão do risco, já que a medida poderia ter um papel decisivo na implementação de medidas de segurança mais estruturadas. O ponto não mereceu, no entanto, a concordância de todos os participantes.

Introduzidas as ideias discutidas no âmbito dos temas da Privacidade e da Identidade Digital, o grupo reflectiu sobre a capacidade ou não do cidadão para exercer os seus direitos de liberdade e cidadania no mundo digital e sobre a necessidade de um maior controlo sobre os dispositivos, os serviços e as ferramentas digitais que usamos no nosso dia-a-dia, por forma a garantir a salvaguarda de identidade e de direitos.

Defendeu-se que isso só será possível com a ajuda de entidades que, pela defesa do cidadão, possam agir e informar para dar maior segurança em relação aos equipamentos que usamos.

Formar ou informar o cidadão, em que medida?

A ideia foi bem aceite pela maioria dos presentes mas fez surgir a questão: como é possível formar o cidadão para a segurança? Informar é um caminho mais fácil de traçar. Pode recorrer-se a campanhas e acções de massas que ajudem a ganhar uma consciência critica, como está aliás a ser feito em vários países da Europa. Formar é tão ou mais essencial para que a utilização das TIC não seja um risco ou motivo de desconfiança, mas implica uma acção mais directa. Será possível?

Formar nas empresas considera-se por isso um dos caminhos a seguir, pois contribuirá para que o homem não seja o elo mais fraco desta cadeia.

A formação – possível ou não - do cidadão gerou polémica na discussão e introduziu o próximo tema. Até que ponto informar o cidadão pode tornar-se uma tarefa perigosa. Formar o cidadão é dar-lhe consciência de todos os perigos e vulnerabilidades.

Que implicações teria isso na relação de confiança que este mantém com o Estado? O grupo converge na convicção de que informar é o caminho mais legítimo, assim os líderes políticos e empresariais saibam operacionalizar essa iniciativa.

Políticas públicas concretas para segurança digital precisam-se

No geral, as conclusões dos grupos de trabalho evidenciaram uma necessidade urgente: a do Estado ter uma orientação e acções

mais claras na área da segurança para o Mundo Digital, no âmbito dos seus planos públicos. Pouco visada no Plano Tecnológico, a questão é coberta pela renovada Agenda de Lisboa mas perde força na transposição para o âmbito nacional, comenta o grupo, considerando que não existem órgãos públicos com responsabilidades sérias nesta matéria. A falha, sugere-se, pode ser compensada através da acção de associações que informem o cidadão.

Sendo óbvia a necessidade de mais informação sobre a segurança no mundo digital, discute-se também a importância de passar uma mensagem positiva e sublinha-se que aplicações tão populares como a banca *online* mantêm em Portugal um nível relativamente baixo de ataques informáticos ou problemas de segurança com impactos para o utilizador, assim como o facto da tecnologia - que está na base dos perigos - ser também o veículo para controlar ameaças e ultrapassar vulnerabilidades, contribuindo para diminuir a fraude e aumentar a segurança dos sistemas bancários.

Sob a moderação de José Gomes Almeida terminou a última sessão plenária do encontro com um comentário da audiência que lembra o facto da vida ser feita de riscos que é preciso correr. Importa que sejam criados mecanismos para ultrapassar esses riscos, tirando todo o partido de uma Sociedade da Informação e do Conhecimento.

Coube finalmente a palavra a José Dias Coelho, que sublinhou a importância dos encontros até agora realizados pela riqueza de ideias debatidas, felicitando ainda todos os participantes, e principalmente os moderadores dos três grupos de trabalho, pelas conclusões produzidas. O Presidente da APDSI lembrou ainda que este trabalho será entregue a representantes de vários sectores governamentais e da Sociedade Civil para que possa transformar-se num contributo efectivo para o desenvolvimento de políticas de Segurança e Privacidade.