Protecção de dados

Tecnologia perturba privacidade mas pode proteger dados pessoais

Depois da histeria securitária, que se seguiu ao 11 de Setembro, estamos a permitir mais facilmente invasão da privacidade?

Joana Andrade
jandrade@economica.iol.pt

Câmaras de vídeo "para sua protecção", registos informáticos sobre transacções e movimentações, 'cookies' no computador, escutas ilegais, gravação e armazenamento de dados, sistemas biométricos de identificação... O 'Big Brother' – não a versão mais mediática que aparece na televisão, mas sim o "espírito" controlador e fiscalizador que, em muitos casos, segue com atenção os passos de cada um – parece ganhar força com o desenvolvimento da tecnologia.

Mas a tecnologia pode, por outro lado, ter um papel fundamental na defesa da privacidade e dos dados pessoais, se for acompanhada por legislação uniforme dentro da União Europeia, defende uma avaliação do Centro Comum de Investigação da Comissão Europeia. O estudo, patrocinado pelo Parlamento Europeu, recomenda que as medidas invasoras da privacidade resultantes do 11 de Setembro, desenvolvidas como uma resposta imediata, devem ser temporárias e limitadas. Medidas legislativas devem ser tomadas no que diz respeito a roubos de identidade e às bases de dados do sector privado, recomendam.

A dúvida que esteve na base da realização do trabalho é clara: à luz do pós-11 de Setembro, as novas tecnologias vão proteger ou perturbar a privacidade? Em estudo três tecnologias emergentes: os serviços de gestão de identidade (serviços 'on-line' baseados na identificação do utilizador), de identificação do local (posicionamento global e trajectos do utilizador) e casas inteligentes (com recurso a equipamentos móveis, utilizados dentro e fora de casa, no carro, etc.). De acordo com o relatório, é preciso equilibrar a balança a favor da privacidade, uma vez que o uso destas tecnologias em algumas acções governamentais ou comerciais perturba a capacidade da legislação existente de proteger os dados pessoais.

«Em resposta à ameaça do terrorismo depois da tragédia do 11 de Setembro, muitos governos reforçaram os seus poderes de vigilância, mas correndo o risco de afectar a privacidade», sustenta o comissário europeu para a Investigação, Philippe Busquin. «No entanto, os cidadãos não estão preparados para deixar que a privacidade seja uma das vítimas do terrorismo», frisa.

No final deste mês entra em vigor na UE uma directiva comunitária sobre o tratamento de dados pessoais e protecção da privacidade no sector das comunicações electrónicas. O governo português aprovou recentemente em Conselho de Ministros o diploma que fará a transposição. Entre várias alterações contempladas (ver caixa), o comissário europeu das empresas e sociedade de informação, Erkki Liikanen, realça que «a informação da localização gerada por telefones móveis só pode ser usada ou passada a outros pelos gestores da rede com a autorização do utilizador, a não ser que seja uma chamada de emergência».

«Muitos governos reforçaram os seus poderes de vigilância, correndo o risco de afectar a privacidade».

A mudança principal, identificada no relatório da CE, fica a dever-se à passagem de uma protecção reactiva para uma pró-activa. Um dos exemplos dados, que carece de legislação, diz respeito à identificação de 'gadgets' por rádio frequência, através de 'chips' que são incorporados nos objectos, permitindo que se saiba onde estão, mas também identificar o utilizador.

Victor Machado

Tema: Política Nacional/Governo/AR/Partidos
Título: Protecção de dados – Tecnologia perturba privacidade mas pode proteger dados pessoais
2003/10/22 | DIARIO ECONOMICO – PRINCIPAL | Pág. 10 | Imagem: 1/3
Âmbito: n.a. | Tiragem: 21041
Temática: n.a. | GRP: 1.8
Periodicidade: n.a. | Inv.: n.a.

Tema: Política Nacional/Governo/AR/Partidos
Título: Protecção de dados – Tecnologia perturba privacidade mas pode proteger dados pessoais
2003/10/22 | DIARIO ECONOMICO – PRINCIPAL | Pág. 10 | Imagem: 2/3
Âmbito: n.a. | Tiragem: 21041
Temática: n.a. | GRP: 1.8
Periodicidade: n.a. | Inv.: n.a.

Os fins não justificam os meios

Mesmo que «na reacção aos ataques de 11 de Setembro a União Europeia tenha evidenciado solidariedade com o objectivo americano de prevenção e combate ao terrorismo», «os fins não justificam os meios», sustenta Carlos Coelho, eurodeputado social-democrata. Opondo-se à transmissão de dados «que esteja em contradição com as regras comunitárias», como indica estar a ser feita no caso da exigência de dados PNR (passenger name record) por parte das companhias aéreas, Carlos Coelho recorda que, em Março, «o Parlamento Europeu considerou inaceitável haver lugar à transmissão desses dados caso não sejam dadas garantias de um nível de protecção adequado».

Esse sistema informatizado de reserva vai mais longe na recolha de dados do que o modelo anterior, que apenas recolhia os dados necessários para atravessar as fronteiras, refere ao DE o eurodeputado. E explica que, ao fornecerem esses dados – algo a que estão obrigadas, sob pena de lhes serem recusados direitos de aterragem –, as companhias aéreas "transmitem" aos EUA informações como o nome dos passageiros, o cartão de crédito, eventuais trajectos, problemas de saúde, religião, contactos... No total são 39 dados, alguns deles «muito sensíveis». O objectivo para esta recolha «continua a não ser claro», diz Carlos Coelho.

Luís Silveira refere que o envio de grande parte dos dados exigidos não é permitido à luz do Direito Comunitário. «Porque não é proporcional», logo não se justifica, refere. Têm estado a decorrer negociações entre elementos da CE e a Autoridade Alfandegária norte-americana, porque os dados são «muito sensíveis», o período de armazenamento «é muito longo» e os dados podem ser passados a outras entidades não especificadas. **J.A.**

O que diz a directiva 2002/58/CE?

- A evolução das tecnologias obriga a novas medidas de segurança no tratamento e armazenamento de dados pessoais;
- Os prestadores de serviços de comunicações electrónicas têm de adoptar medidas técnicas e organizativas que garantam a segurança dos serviços;
- Em caso de risco especial de violação da segurança da rede, os prestadores de serviços têm de informar os assinantes;
- A legislação tem de assegurar a confidencialidade das comunicações e respectivos dados de tráfego. Têm de proibir a escuta, o armazenamento ou outras formas de vigilância, excepto em questões de segurança nacional e penais;
- Os utilizadores ou assinantes têm de ser informados caso os seus dados estejam a ser processados, podendo retirar o seu consentimento em qualquer altura;
- Os dados de tráfego devem ser eliminados ou tornados anónimos quando deixem de ser necessários para a comunicação;
- O tratamento de dados de tráfego está limitado ao pessoal que

MEDIA MONITOR

Tema: **Política Nacional/Governo/AR/Partidos**				Âmbito: **n.a.**	Tiragem: **21041**
Título: **Protecção de dados – Tecnologia perturba privacidade mas pode proteger dados pessoais**				Temática: **n.a.**	GRP: **1.8**
2003/10/22	**DIARIO ECONOMICO – PRINCIPAL**	Pág.**11**	Imagem: **3/3**	Periodicidade: **n.a.**	Inv.: **n.a.**

'Little brother' é mais intrusivo

Fala-se menos dele, mas o 'little brother' – que é usado por patrões ou empresas para fiscalizar os trabalhadores ou manter registos de clientes, por entidades públicas para verificar as horas de entrada e saída dos funcionários, mas também por pais para vigiar amas e crianças – acaba por ser mais intrusivo do que o 'big brother'. Cada vez mais empresas privadas, câmaras municipais ou mesmo cidadãos estão a operar os seus próprios sistemas de vigilância, seja através de vídeo, seja pelo recurso à biométrica. «Sorria, está a ser filmado», já se tornou num chavão, mas esse registo pode não ser legal, e deve sempre queixar-se.

Em Portugal, quem fiscaliza estes excessos e quem os pode autorizar é a Comissão Nacional de Protecção de Dados (CNPD), uma entidade que funciona na alçada da Assembleia da República. Luís Lingnau da Silveira, o presidente da comissão, refere, em declarações ao DE, que estão a surgir algumas queixas de trabalhadores quanto ao controlo de dados biométricos. A tecnologia, ainda recente, mas já relativamente barata, é usada para controlar a assiduidade tanto em entidades privadas como públicas. Recentemente, surgiu o caso do controlo da íris feito em miúdos de um infantário da Misericórdia de Oeiras. Ainda não houve decisão, mas foi aplicada uma coima pela não notificação à comissão. Para o procurador-geral adjunto, «a utilização deste sistema está claramente a generalizar-se», mas ainda não há uma leitura definitiva, mesmo a nível europeu. Só houve ainda uma decisão na CNPD, incidindo sobre o controlo de entradas de 140 funcionários do Instituto Superior de Engenharia de Lisboa – a comissão considerou a medida desproporcional. À CNPD têm também chegado queixas de clientes de bancos que não são retirados das "listas negras" de utilizadores de cheques, mesmo depois da situação ser resolvida e o pedido de acesso a dados clínicos: ou são as seguradoras, a quem é recusado o acesso, ou os familiares, a quem é permitido o conhecimento da causa de morte. E, neste momento, está em discussão a pressão das autarquias para instalar câmaras nas ruas, em virtude do Euro'2004.

O aumento de queixas na CNPD prende-se com uma maior divulgação e não com um aumento das violações da privacidade, mesmo depois do 11 de Setembro, refere Luís Silveira. «Não houve nenhuma queixa directamente relacionada com o pós-11 de Setembro», diz. Por outro lado, enquanto que no Reino Unido e Alemanha a legislação teve de ser modificada, com a introdução de legislação para controlo de dados e combate ao terrorismo, «o enquadramento legal português já chega para lidar com essas situações, desde que seja aplicado», indica.

À Comissão de Direitos Humanos da Ordem dos Advogados não é habitual chegarem queixas sobre violação da privacidade, refere Pedro Tenreiro Biscaia, secretário executivo da entidade, em declarações ao DE. Houve, no entanto, o caso de uma base de dados que o Estabelecimento Prisional de Santarém geria, sobre familiares e amigos dos reclusos, uma situação surgida há cerca de um ano, relata. Entretanto, a questão foi resolvida e a base de dados desactivada. **J.A.**

---

trabalha para os fornecedores;
- No caso de litígios, os organismos competentes podem ser informados dos dados de tráfego;
- Os assinantes têm direito a receber facturas não detalhadas e de ocultar gratuitamente o seu número, quando realizarem chamadas;
- Os dados de localização só podem ser tratados se forem anonimizados ou se houver consentimento dos assinantes;
- As chamadas automáticas, faxes ou e-mail para fins comerciais só podem ser autorizadas para assinantes que tenham dado o seu consentimento prévio;
- O envio de e-mail para fins comerciais não identificando o remetente é proibido;
- Não podem ser impostas características específicas técnicas aos terminais que possam impedir a colocação de novos produtos no mercado;
- Os Estados-membros podem tomar medidas para restringir estes direitos, para salvaguardar a segurança nacional, a defesa, a segurança pública e a repressão e investigação de crimes.