

FICHA TÉCNICA

Editor:

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Design, Paginação e Produção:

Caixa das Letras – Gabinete de Design, Lda.

Fotolitos:

Caixa das Letras – Gabinete de Design, Lda.

Impressão e acabamento:

Alves & David – Artes Gráficas, Lda.

Tiragem:

500 exemplares

Depósito Legal:

??? ???/06

LISBOA

ÍNDICE

SESSÃO DE ABERTURA

Luís Lingnau da Silveira Presidente da CNPD	9
Leonor Beza Vice-Presidente da Assembleia da República	11
António Montalvão Machado Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias	15

CONFERÊNCIA

Luís Lingnau da Silveira Presidente da CNPD <i>Protecção de dados: novos direitos para uma nova consciência</i>	21
--	----

I PAINEL – Tratamento de dados pessoais nos sectores público e privado

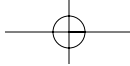
João Salgueiro Presidente da Associação Portuguesa de Bancos <i>A circulação de dados numa economia global e aberta</i>	33
Diogo Vasconcelos Gestor da Unidade de Missão, Inovação e Conhecimento <i>A modernização da administração</i>	45
Debate	57

II PAINEL – Segurança e privacidade: ponderação de interesses

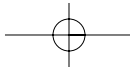
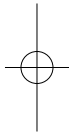
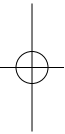
Alexandre Pinheiro Vogal da CNPD <i>A videovigilância e a protecção de dados pessoais</i>	75
--	----

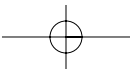
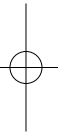
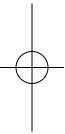
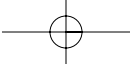
ÍNDICE

Carlos Cabreiro Brigada da Criminalidade Informática da Polícia Judiciária <i>A investigação policial e o combate ao cibercrime</i>	83
Amadeu Guerra Vogal da CNPD <i>Sistemas de informação policial – os direitos dos cidadãos</i>	91
Debate	103
III PAINEL – Tecnologias e vida privada	
Filipe Custódio Especialista em segurança informática <i>A (in)segurança da informação nas redes abertas</i>	113
Álvaro Canales Secretário-Geral da Agência Espanhola de Protecção de Dados <i>A protecção de dados pessoais na Internet</i>	123
Luís Barroso Vogal da CNPD <i>As tecnologias emergentes e a privacidade</i>	131
Debate	139



SESSÃO DE ABERTURA





Luís Lingnau da Silveira

Presidente da CNPD

A promulgação da Lei de Organização e Funcionamento da Comissão Nacional de Protecção de Dados, de 18 de Agosto de 2004, criou condições para a entrada em velocidade de cruzeiro desta entidade administrativa independente com poderes de autoridade.

Definido o enquadramento jurídico da CNPD, que já tardava, estamos em condições de dar um salto qualitativo e dotar-nos de meios humanos em sectores particularmente carenciados. A partir de 2005 procederemos à contratação de mais técnicos, designadamente nas áreas jurídica e informática.

Este colóquio oferece-nos, portanto, uma oportunidade de olhar para o futuro.

Ao colmatarmos as faltas que nos impediam de cumprir tudo o que se esperava da CNPD estaremos em condições de corresponder às expectativas e exigências da Lei.

Temos vindo a definir, como é natural, Planos de Actividade anuais e a proceder à avaliação da sua execução com a regularidade exigida.

O Registo Público, ou seja o registo de todos os tratamentos de dados pessoais, será concluído em breve. É uma obrigação da Comissão que ainda não tínhamos conseguido cumprir cabalmente. Qualquer cidadão poderá, como se impõe em matéria de registos públicos, passar a aceder a informações permitindo-lhe conhecer os tratamentos de dados que estão a ser realizados, suas finalidades e a identidade dos respectivos responsáveis.

COLÓQUIO PROTEGER OS DADOS PESSOAIS

Procedemos, igualmente, a uma renovação que cremos aceitável e boa do nosso *site* e aí disponibilizaremos informação sobre as actividades da Comissão também em inglês e francês.

O sistema de recepção de notificações por via electrónica encontra-se na fase final de ensaios.

Nos últimos tempos constatámos que a Comissão ganhou um pouco mais de visibilidade pública. O conhecimento das actividades da Comissão por parte do público, em geral, ainda não é satisfatório devido, porventura, em grande parte a deficiência nossa e por carência de meios. Contudo, é um facto que recentemente os órgãos de comunicação social têm vindo a colocar-nos um número crescente de questões e a solicitar cada vez mais esclarecimentos. Estamos em crer, portanto, que conseguimos trabalhar não exclusivamente virados para dentro, por assim dizer. Temos vindo a conseguir exercer, também, uma função externa de divulgação, uma função pedagógica.

Parece-nos, em conclusão, que a Comissão está neste momento em condições de funcionar numa normalidade satisfatória. Nunca funcionaremos em condições óptimas porque será sempre difícil alcançar tal desiderato, mas cremos estar perto do aceitável.

Impõe-se, conseqüentemente, discutir agora os novos desafios, problemas e questões que se levantam em matéria de protecção de dados.

Pretendemos discutir e apreciar aqui convosco estas novas realidades para retirar lições e ensinamentos deste Colóquio para a nossa actuação.

Leonor Beleza

Vice-Presidente da Assembleia da República

Senhor Presidente da Comissão Nacional de Protecção de Dados,

Senhor Professor Diogo Lucena,

Senhor Presidente da Comissão Parlamentar de Assuntos Constitucionais,
Direitos, Liberdades e Garantias,

Minhas Senhoras e Meus Senhores:

Agradeço ao Sr. presidente da Comissão Nacional de Protecção de Dados o convite para participar, em representação do Presidente da Assembleia da República, que está ausente no estrangeiro, na Sessão de Abertura deste colóquio comemorativo do décimo aniversário da Comissão e realizado sob o lema "Proteger os dados pessoais – Um desafio constante".

Ao longo destes primeiros dez anos, a Comissão Nacional de Protecção de Dados foi ganhando notoriedade e influência. Estão assim de parabéns a Comissão e todos os que dela fazem ou fizeram parte.

Permitam-me que felicite em particular o Senhor Dr. Luís Silveira, Presidente da Comissão, cujo empenho e capacidade conheço há muitos anos – tantos como aqueles em que tenho tido o privilégio e a satisfação de ser sua amiga, como ele há momentos quis mencionar.

Mas é necessário manter e ampliar esse prestígio e crédito alcançados. Na verdade, o papel de órgãos independentes como a Comissão Nacional de Protecção de Dados é cada vez mais importante na nossa sociedade democrática.

Com uma composição plural e equilibrada, compete-lhe, nos termos da lei, controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito pelos direitos humanos e pelas liberdades e garantias consagradas na Constituição e na lei.

O Parlamento tem sempre encontrado na Comissão – e é com gosto que nesta oportunidade o registo em nome da Assembleia da República – um importante colaborador no exercício dos seus poderes legislativos, apresentando sempre pareceres criteriosos e bem preparados relativos aos diplomas legais relacionados com a sua actividade.

Portugal foi, como se sabe, pioneiro na valorização constitucional da privacidade. O nosso quadro constitucional, que a Revisão Constitucional de 1997 estabilizou na actual redacção do artigo 35.º da Constituição, é claro e, acredita-se, suficiente. Aí se garante, nomeadamente, o acesso de todos os cidadãos aos dados informatizados que lhes digam respeito; a proibição genérica de tratamento, sem consentimento, de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica; a proibição de acesso a dados pessoais de terceiros e de atribuição de um número nacional único aos cidadãos.

A lei, por seu lado, desenvolve esses direitos e atribui à Comissão Nacional de Protecção de Dados os adequados poderes de investigação e de inquérito, bem como os necessários poderes sancionatórios.

Mas, para além das afirmações constitucionais e legais, é necessário que as entidades colocadas no terreno para garantir os direitos definidos na Constituição e na lei tenham reais condições de actuação.

Nesse sentido, e recentemente, como o Senhor Presidente já referiu, a Assembleia da República aprovou dois instrumentos – a respectiva lei de organização e funcionamento e o seu quadro de pessoal – que vieram permitir (é o que vivamente se espera!) novas condições de eficácia da acção garantística da Comissão.

E essa acção é cada vez mais importante e necessária: desde logo porque a Comissão viu fortemente ampliadas as suas competências (com a transposição

de várias directivas comunitárias, e com a aprovação de outros diplomas, nomeadamente na área da protecção de dados no sector das telecomunicações e no domínio da videovigilância), e porque a sua acção se enquadra cada vez mais numa verdadeira rede europeia de autoridades de protecção de dados.

Essa acção vai porém, e simultaneamente, exercer-se num quadro crescentemente complexo, num momento crucial na defesa dos direitos e liberdades dos cidadãos relacionados com a privacidade e a protecção dos seus dados, quer a nível nacional, quer europeu, quer mundial.

Na verdade, há hoje servidores da Internet que têm na sua posse milhões de dados das mais diversas naturezas, incluindo dados pessoais muito sensíveis.

Assistimos a uma evolução crescente do comércio electrónico.

Há hoje redes electrónicas de todos os tipos e uma massificação da sua utilização, com os efeitos positivos, mas também negativos que se conhecem: não há hoje computador que não esteja ligado a uma qualquer rede.

A protecção de dados neste novo mundo é assim de natureza qualitativamente muito diferente. Há que ter consciência desta diferença e do que ela representa como desafio.

A Comissão Nacional de Protecção de Dados terá de intervir numa vertente repressiva, mas também numa vertente preventiva e pedagógica, no quadro da qual poderia ser importante a existência de campanhas de publicidade que ensinassem os cidadãos a proteger a sua privacidade e divulgassem o direito que têm de recorrer à Comissão cada vez que suspeitem de qualquer violação dos seus direitos.

Por outro lado, os fenómenos da videovigilância, com as facilidades tecnológicas hoje existentes, exigem uma crescente acção fiscalizadora e garantista por parte da Comissão.

Seja-me permitida ainda uma reflexão final:

A actividade da Comissão é dirigida, em muitos casos, ao controlo de entidades públicas e, nomeadamente, policiais. O tratamento de dados pessoais e

COLÓQUIO PROTEGER OS DADOS PESSOAIS

sensíveis por entidades policiais levanta sempre difíceis e delicadas questões e deve ser estritamente controlado, sob pena de abusos perversos que todos conhecemos e a História nos ensina.

Mas, hoje, vivemos num quadro tecnológico enormemente desenvolvido, difundido por todos os lados e por todas as pessoas, e de muito fácil acesso, mesmo para entidades sem grande poder económico.

Ora, a consciência deste quadro aconselha-nos fortemente a perspectivar a acção da Comissão Nacional de Protecção de Dados menos preocupada, porventura, com um imaginário *Big Brother* estadual, governamental ou policial – cada vez mais hipotético, diria, nas democracias ocidentais, maduras e estabilizadas, como a nossa, onde existem suficientes instrumentos de controlo –, e muito mais preocupada com os inúmeros “pequenos” *Big Brothers* privados, ligados a grandes e pequenas corporações, que poderão hoje constituir uma ameaça muito superior à privacidade dos cidadãos.

Faço votos para que os trabalhos deste Colóquio sejam realmente úteis para os trabalhos futuros da Comissão e terei muito gosto em conhecer as suas conclusões, a que a Assembleia da República não deixará de estar atenta.

Muito obrigada pela vossa atenção.

Montalvão Machado

Presidente da Comissão de Assuntos Constitucionais, Direitos,
Liberdades e Garantias

Muito obrigado Sr. Presidente. Vou ser muito breve.

Dirijo-me em primeiro lugar, naturalmente, à Sra. Vice-Presidente da Assembleia da República, ao Sr. Presidente da Comissão Nacional de Protecção de Dados, ao Sr. Administrador da Fundação Calouste Gulbenkian. Minhas senhoras e meus senhores.

Queria, antes de mais, dizer-lhes que é com muita honra, evidentemente, que na qualidade de Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República, que participo nesta sessão de abertura do Colóquio organizado pela Comissão Nacional de Protecção de Dados, sob este título de “Proteger os dados pessoais: um desafio constante”.

Participo, natural e evidentemente, antes de mais porque é um dever institucional da minha parte, como representante da Comissão parlamentar, com quem esta entidade administrativa independente tem por definição maior ligação e relacionamento jurídico.

Mas participo, sobretudo, e queria dar conta disso aos participantes, porque tem sido e é um gosto estar junto de pessoas que de forma sempre serena e muito responsável criaram condições para trabalharmos na idealização, redacção e até no aperfeiçoamento de diplomas absolutamente fundamentais para a consistência e solidez de um estado verdadeiramente democrático.

Seria, portanto, injusto da minha parte não recordar aqui, hoje, a sempre pronta eficaz e competente resposta que a Comissão Nacional de Protecção de Dados sempre deu ao parlamento nacional, e muito concretamente à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias nessa, diria, quotidiana, incessante, e, até às vezes, lancinante tarefa legislativa que nos cumpre desenvolver.

Foi por isso, Sra. Vice-Presidente, minhas senhoras e meus senhores, que se obtiveram, em tempo oportuno, importantes pareceres, indispensáveis à idealização e redacção das leis emanados desta Comissão Nacional.

Só a título de exemplos relativamente recentes recordo o parecer emitido a propósito do projecto de lei que visou a aprovar o regime jurídico da obtenção da prova digital electrónica na Internet.

Poderia, igualmente, referir o parecer proferido no âmbito da proposta de lei que visou garantir a protecção de dados pessoais e a privacidade das comunicações electrónicas na sociedade de informação.

Indico, ainda, e até pela sua actualidade, os pareceres emitidos acerca da proposta conducente à aprovação das medidas preventivas e punitivas face a casos de manifestações de violência associadas ao desporto, bem como o parecer emitido sobre o próprio Código de Trabalho.

Tem sido este e assim deverá continuar a ser o relacionamento profícuo entre a Comissão a que honrosamente presido na Assembleia da República e esta Comissão Nacional de Protecção de Dados.

É indiscutível que a Comissão Nacional desenvolve uma actividade muito difícil. Uma actividade extremamente complexa numa área de ciência muito difícil. Está obrigada a uma tarefa de alertar tudo e todos, mas também a própria CNDP tem de estar muito alerta. É uma tarefa, como a própria lei indica, de vigilância constante, de investigação, de autoridade, mas sempre com o único fito de velar pelo cumprimento da lei em matéria de protecção de dados pessoais, em rigoroso respeito pelos Direitos do Homem e pelas liberdades e pelas garantias consagradas na constituição.

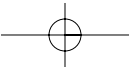
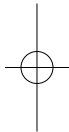
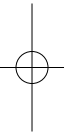
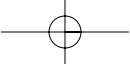
SESSÃO DE ABERTURA

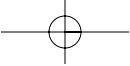
Só isto demonstra que o trabalho prestado por vossas excelências, ilustres membros da Comissão, é, sem dúvida, um verdadeiro tributo à democracia.

Considero, sem me alongar, que numa época em que o lancinante desenvolvimento da ciência informática já não constitui surpresa para ninguém e em que a descoberta de hoje nessa área do saber e da ciência representa amanhã de manhã um fóssil para o nosso conhecimento, que a CNPD não podia ter dado a este evento um melhor título do que o que deu – “Proteger os dados pessoais: um desafio constante”.

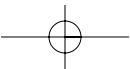
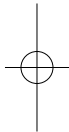
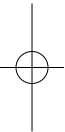
Sr. Presidente, muito obrigado pelo convite. Agradeço o convite que me foi dirigido e à Comissão a que presido.

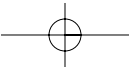
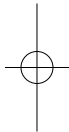
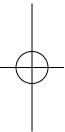
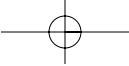
Bom trabalho e muito obrigado.





CONFERÊNCIA





Luís Lingnau da Silveira

Presidente da Comissão Nacional de Protecção de Dados

NOVOS DIREITOS - PARA UMA NOVA CONSCIÊNCIA

A) Justificação do tema

1) O direito à protecção de dados pessoais, um direito recente

O direito à protecção de dados pessoais – enquanto direito à protecção das informações relativas a pessoa identificada ou identificável – é, afinal, um direito recente.

Tal não significa, naturalmente, que este problema não tenha, desde há muito, vindo a preocupar a Humanidade, mas era considerado como integrado ou confundido no direito à privacidade, enquanto mero aspecto ou faceta deste.

Tanto assim era que até o célebre artigo de Warren e Brandeis, de 1890, que muitos consideram como a primeira proclamação do direito à protecção dos dados pessoais, se apresentou, em boa verdade, ainda na perspectiva da defesa do direito à privacidade (*“right to privacy”, “right to be let alone”*).

Em bom rigor, talvez que o direito à protecção de dados pessoais, como direito autónomo e distinto do genérico direito à privacidade, só tenha ganho carta de alforria em 1970, através da Lei de Protecção de Dados do Estado alemão do Hessen, que até, aliás, já instituía também um organismo especialmente incumbido de zelar pela sua aplicação.

A sucessiva adopção de legislações nacionais desta índole, bem como a publicação de importantes instrumentos internacionais (Convenção n.º 108 do Conselho da Europa e Linhas Directrizes da OCDE, de 1980) e comunitários (Directiva 95/46/CE), sobretudo a nível europeu, culminaram na Carta dos Direitos Fundamentais da União Europeia – posteriormente integrada no projecto de Constituição Europeia – que expressamente reconhece e regula o direito à protecção de dados pessoais como figura distinta do direito à privacidade.

Cumprе reconhecer, de todo o modo, que, mesmo no âmbito europeu, muitos cidadãos ainda não têm consciência de que são titulares deste direito, tal como o revelou, desapontadoramente, um recente inquérito promovido pela Comissão Europeia.

2) O direito à protecção de dados pessoais; um direito ainda carecido de efectivo reconhecimento universal

Se, em termos cronológicos, este é um direito recente, tal constitui, também, sob o ponto de vista espacial, uma “*novidade*” para muitos países e zonas do Mundo.

Isto, note-se, apesar de já em 1990 a ONU ter emanado Linhas Directrizes para a regulação de Ficheiro de Dados Pessoais Informatizados.

Este bem intencionado instrumento não tem tido, talvez por demasiado genérico, a eficácia desejada.

E assim é que, na recentíssima Conferência Mundial das Autoridades de Protecção de Dados, realizada na Polónia, em Setembro passado, constituiu uma dura chamada à realidade a observação de um dos participantes de que, apesar da sua pretensão universal, lá se não encontravam representados três dos maiores e mais populosos países da actualidade: China, Rússia e Estados Unidos.

Esta algo descoroçoante constatação podia mesmo valer até em relação a certos continentes: salvo algumas simbólicas excepções (Coreia do Sul e a Região Administrativa Especial chinesa de Hong Kong) poucos são os Estados de África e da Ásia que possuem legislações que reconheçam e regulem este direito. Esta dura realidade, contudo, não deve sem mais lançar no desespero os cultores da protecção de dados pessoais.

É sabido que muitos dos hoje universalmente consagrados direitos humanos – em particular na Declaração Universal dos Direitos do Homem – encontraram primeiro expressão em certos países, sobretudo da Europa, mas a sua validade e força intrínseca era tais que foram sendo progressivamente reconhecidos a nível mundial.

Só que, no tocante ao direito à protecção de dados pessoais, essa eventual expansão não está, sem mais, assegurada. Há países que adoptam a seu respeito uma posição de declarada desconfiança, se não mesmo hostilidade.

É esse o caso, nomeadamente, dos Estados Unidos da América.

A perspectiva norte-americana é a de que – ressalvadas certas áreas para as quais existe legislação protectora especial – os dados pessoais devem circular livremente para propiciar o normal funcionamento do mercado e o desenvolvimento da economia.

Segundo a visão dominante – conquanto não exclusiva, anote-se – nos EUA, as leis e instrumentos internacionais e comunitários europeus tendentes à protecção dos dados pessoais representam uma postura anacrónica da *“Velha Europa”*, afinal obstrutiva do progresso económico, e, hoje, também, do combate ao terrorismo internacional.

E o certo é que a força económica e política dos EUA já fez com que, quando contraposta com a visão europeia, em situação de conflito real, esta tenha acabado por ceder, pelo menos parcialmente: recorde-se o que vem sucedendo com o envio para aquele país de dados pessoais de passageiros e tripulantes de aviões que nele aterram ou dele partam.

3) Novas tensões e desafios

Se os dados pessoais são informações sobre os indivíduos, quaisquer novos meios ou processos de as recolher, elaborar ou divulgar suscitam a necessidade de encontrar novos modos de responder a tais desafios por forma a assegurar que não resultem agressões ou constrangimentos desproporcionados.

E, se a informação significa poder, a obtenção de mais informações sobre outras pessoas traduz-se num acréscimo de supremacia sobre estas. Uma boa parte destas novas agressões aos dados pessoais está associada a procedimentos sujeitos a rápida e constante evolução.

É para corresponder a esta realidade, aliás, que as Conferências Mundiais de Autoridades de Protecções de Dados se efectuam anualmente. Confesso que, de início, me pareceu tratar-se dum exagero, mas hoje reconheço que é essa a forma adequada de ir acompanhando as novidades nesta área.

De entre as principais novas tensões na área da protecção de dados pessoais pode, designadamente, apontar-se que:

a) A captação de imagem e/ou som mediante equipamentos electrónicos (designadamente a videovigilância) pode ter importante papel na salvaguarda da segurança, de pessoas e bens, em bancos, supermercados, farmácias, estabelecimentos de restauração e similares, mas afecta, inegavelmente, os direitos à imagem, à privacidade, à livre deslocação.

Por isso causa legítima preocupação a pretendida generalização da utilização destes sistemas em ruas, praças e outros lugares públicos como praias, bibliotecas, creches e mesmo, conforme um caso que analisámos, um cabeleireiro;

b) A Internet tem tido um estupendo efeito na liberdade de expressão, na investigação, na educação, no comércio e demais operações económicas, mas são patentes os riscos que envolve o tratamento de dados pessoais através deste meio.

Mesmo que se não entenda que ela escapa ao Direito – enquanto área de autêntico “*não direito*” – como muitos ainda hoje opinam, há que reconhecer que a Internet, pela facilidade de acesso que implica, é de por mesma um meio inseguro de tratamento de dados.

É, sobretudo, frequentemente difícil, quase impossível, fazer aplicar a lei a boa parte de tais tratamentos. Tivemos na Comissão já essa experiência mais do que uma vez em relação a imagens de índole criminal recolhidas em Portugal mas depois remetidas para os EUA, e daí colocadas na Internet, sem termos podido identificar os autores desses actos;

- c) Generalizou-se nos últimos tempos a utilização de dados biométricos – respeitantes à fisiologia ou comportamento das pessoas – resultantes da transformação em dados informáticos de informações colhidas da face, da mão, das impressões digitais, da íris, da retina...

Estes processos começam a encontrar grande aceitação por parte de entidades privadas e públicas para controlar o acesso a certos edifícios ou zonas, a assiduidade dos trabalhadores e até a frequência de cantinas escolares pelos alunos...

A CNPD, depois de longa discussão, acabou por considerar que a utilização de tais dados para controlar a assiduidade dos trabalhadores não agride, sem mais, o direito à respectiva identidade pessoal, mas nem sempre é garantida a total fiabilidade de todos os tratamentos destes tipos de dados.

E não falta quem, como a “Commission Nationale de l’Informatique et des Libertés” francesa, entenda que, em certos casos, a utilização desses dados atinge níveis de desproporcionalidade;

- d) A captação e compilação de dados genéticos tem proporcionado enormes avanços científicos no âmbito da medicina preventiva e curativa, da identificação pessoal e, até, da investigação de paternidade, mas o seu tratamento vem sempre associado ao risco de se pretenderem extrair conclusões quase determinísticas acerca da saúde e comportamento das

peçoas a que se referem para além de poderem mesmo gerar situações de discriminação.

Acresce que tais dados assumem, em regra, relevância que excede o nível do indivíduo, acabando por caracterizar toda uma família, ou mesmo grupos mais alargados;

- e) A identificação por radiofrequência (RFID) – realizada através de “chips” colocados em mercadorias, animais ou pessoas, conectados com um equipamento receptor – tem rapidamente passado do estudo à prática, em várias áreas.

A sua utilidade é indiscutível no âmbito da logística e da gestão comercial e pecuária, mas começa a parecer pelo menos problemático o seu emprego em pessoas, ainda que se trate do Procurador-Geral mexicano e seus colaboradores, com vista a permitir a sua localização em caso de eventual rapto...

- f) O sistema GPS tem trazido ingentes benefícios para localização de pessoas perdidas e de na navegação aérea e marítima.

Só que não deixa de ser questionável que ele sirva para seguir permanentemente as deslocações de pessoas, como no caso de trabalhadores de empresas.

Não pode olvidar-se, enfim, que estas várias realidades não devem considerar-se isoladamente: a sua conjugação e correlação gera um risco acrescido de intrusão na individualidade de cada pessoa nos dias de hoje.

B) Que respostas?

- 1) Para uma melhor consciência dos direitos

Importa empreender uma acção firme e regular de divulgação dos direitos relativos à protecção de dados pessoais, através de meios vários e ajustados. Este Colóquio pretende contribuir, precisamente, nesse sentido.

Esta obrigação impende, em primeira linha, sobre a Comissão que, todavia, espera e deseja uma boa colaboração, nesse sentido, dos órgãos de Comunicação Social.

A referida divulgação tem por destinatários os responsáveis pelo tratamento de dados, mas, também e sobretudo, a generalidade dos cidadãos, sujeitos principais das informações em que os dados pessoais se traduzem.

2) Para um alargamento geográfico da implementação da protecção de dados pessoais

O meio actualmente mais apropriado para conseguir o alargamento do conjunto de países preocupados com a defesa deste tipo de direitos consiste na progressiva ampliação da participação nas Conferências Mundiais de Autoridades de Protecção de Dados e na difusão das suas recomendações e outras tomadas de posição.

Sobre a CNPD recai, em especial, o dever de impulsionar a abordagem destas questões nos estados da Comunidade dos Países de Língua Portuguesa.

3) Face às novas exigências de protecção de dados

A CNPD tem procurado, em conjunto com as instituições congéneres de outros países, encontrar modos ajustados de, mantendo o critério da protecção dos dados pessoais, fazer face às novas exigências que nesta área vêm surgindo.

Assim, e nomeadamente:

- a) Cura de ponderar devidamente os objectivos sobretudo securitários da videovigilância com os direitos – à imagem, à livre deslocação, à privacidade – que esta pode atingir.

COLÓQUIO PROTEGER OS DADOS PESSOAIS

Esta preocupação foi patente, por exemplo, nas recentes deliberações, em sentido inverso, relativas à utilização deste meio para prevenção de incêndios florestais ou para acompanhamento de crianças em creches;

- b) Vem estando atenta à colocação na Internet de imagens ou outras informações que, sem o consentimento dos visados, possam afectar a sua honra ou privacidade.

Sempre que necessário e possível, ordena o bloqueamento dessas imagens ou outras informações, como o fez em relação a uma “*lista negra*” de maus pagadores ou às fotografias dos alunos duma escola;

- c) Insiste no escrupuloso princípio da obtenção do consentimento dos interessados no tocante ao tratamento de dados genéticos.

E, ademais, conforme deixou expresso no seu parecer sobre o Código do Trabalho, manifesta decidida oposição contra eventual utilização de dados genéticos preditivos com respeito à admissão ou não de trabalhadores;

- d) Enunciou um conjunto de regras gerais que devem ser respeitadas em tratamentos de identificação por radiofrequência, de entre as quais avultam a do respeito pela proporcionalidade, a da transparência e a da sujeição ao consentimento das pessoas porventura envolvidas;

- e) Trata de acompanhar a célere e, por vezes, quase estonteante evolução dos tratamentos de dados biométricos, intentando evitar que estes se revelem desproporcionados, ou que, eventualmente, venham, em qualquer modalidade, a ser utilizados para finalidades diferentes das da recolha, ou, mesmo, a afectar algum direito fundamental.

C) Qual o critério fundamental?

Na sua acção quotidiana, a CNPD deve – já hoje e cada vez mais no futuro – nortear-se por uma visão globalizante que lhe permita apreender e defrontar os novos desafios que se deparam à protecção de dados pessoais.

O seu objectivo fundamental deve ser o de propiciar, como princípio, que os indivíduos, enquanto titulares das informações que são dados pessoais, possam delas dispor em liberdade e conhecedores de todos os factores relevantes para esse efeito.

Esse é o já clássico princípio da “*auto-determinação informacional*” que exprime a ideia de que cada pessoa é dona e senhora das informações que lhe respeitem.

O exercício desta “*auto-determinação*” é uma faculdade de cada pessoa.

O primeiro e principal defensor dos dados pessoais, é, pois, cada um de nós, em relação àqueles de que é titular.

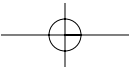
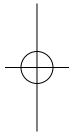
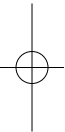
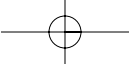
Contudo, a verdade é que, cada vez mais por virtude da sofisticação dos novos tipos e modalidades de tratamentos, cada indivíduo, por si só, não dispõe das capacidades e da força real susceptíveis de lhe assegurarem satisfatoriamente aqueles conhecimentos e liberdade de actuar.

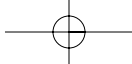
Cabe à CNPD intervir para facultar às pessoas a consecução desses requisitos, informando-as, por um lado, e, por outro, aplicando, se necessário, os poderes coercivos de que dispõe.

Estes são, no essencial, as nossas formas e critérios de actuação.

Pretendemos discuti-lo convosco e beneficiar da reacção crítica dos presentes.

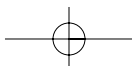
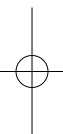
Muito obrigado.

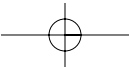
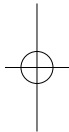
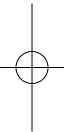
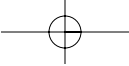




I PAINEL

**Tratamento de dados pessoais
nos sectores público e privado**





João Salgueiro

Presidente da Associação Portuguesa de Bancos

A CIRCULAÇÃO DE DADOS NUMA ECONOMIA ABERTA E GLOBAL

Gostaria de começar por sublinhar o mérito que tem esta iniciativa. Celebramos um aniversário da Comissão e estamos a assinalá-lo, como o Presidente da Comissão referiu, olhando mais para o futuro do que para o passado. Infelizmente, tal não é regra em Portugal. Infelizmente, olhamos muito, na melhor das hipóteses, para o presente e somos surpreendidos pelas consequências do que não fazemos no presente.

Também gostava de sublinhar a importância que tem tido o espírito de colaboração na análise conjunta dos problemas, conforme testemunho de vários colegas, do Banco de Portugal e outras entidades reguladoras do sector.

Porque, aliás, como o Dr. Luís Silveira nos referiu há instantes, trata-se de matérias de contornos não só difusos, como de resposta incerta. As consequências, e vimos que já ele referiu alguns exemplos flagrantes, as intenções têm muitas maneiras de se expressar e os resultados finais também não são, necessariamente, fáceis de perceber à partida.

O meu tema tinha uma componente tecnológica muito forte, mas vejo tal vertente será posteriormente abordada, e outra componente jurídica que não me atrevo a aprofundar dada a competência dos presentes.

Portanto, vou falar sobretudo do meu estado de espírito perante este problema e espero que seja útil. Pode ser, especialmente, que suscite questões para falarmos sobre elas na segunda parte desta sessão.

Nós estamos – e o tema que me é atribuído frisa-o muito bem – numa época de globalização da economia mundial. Dizemos isto, mas depois, no dia-a-dia, comportamo-nos como se as fronteiras fossem fechadas. Os casos que eu tenho acompanhado ao longo destes anos são sempre casos em que queremos regular coisas em que a regulação resiste mal à abertura internacional. Quando se impõem demasiadas regras num determinado território, a deslocalização das actividades, se for possível, anula completamente essa regulação.

Tivemos em Portugal – não tem que ver com o problema da protecção de dados – um problema em relação aos cartões de débito e crédito. O resultado foi a deslocalização para cartões estrangeiros que eram mais caros e menos controlados pelas autoridades portuguesas.

Aliás, isso já tinha acontecido quando a Dinamarca procurou impor o mesmo tipo de regulação, que veio a abandonar um ano e meio depois, porque percebeu que estava a dar resultados opostos ao desejado. Nem foi o Governo, foi o Parlamento português, que resolveu intervir no enquadramento do regime dos cartões de débito e de crédito.

Portanto, se nós admitimos a concorrência internacional – e não vejo que esteja para breve pôr em causa a livre circulação de capitais, a liberdade de circulação de mercadorias, a liberdade de circulação de informação – temos que ter a noção de que o quadro de regulação é, antes de mais, um quadro internacional. Pode haver aspectos em que a deslocalização seja duvidosa e, portanto, a regulação local tenha efeito, mas temos de ver muito bem o que está a acontecer. Atravessamos uma época de desregulação a nível mundial, porque com a queda do Muro de Berlim a alternativa entre dois sistemas e o equilíbrio geoestratégico quebrou-se e, portanto, o único modelo que temos neste momento é o da economia de mercado.

Não estou a fazer antecipações históricas. Espero que venham outros modelos no futuro, mas estamos a viver o predomínio, sem confronto, das regras do

I PAINEL

mercado e se isso apresenta consequências ao nível nacional, tem muito mais ao nível internacional.

Regular a concorrência ao nível mundial não havendo um Governo mundial não está para breve e é uma ideia um bocado complicada. Portanto, temos situações de acordos entre países e os que estão interessados em não cumprir não ratificam esses acordos, ou nem sequer os discutem, aceitam-nos, mas, depois, cumprem-nos com uma grande margem de liberdade. Isto, como sabem, acontece em vários domínios, desde as áreas militares até às financeiras, passando por muitos outros, pelo que não vale a pena desenvolver esta ideia. Se não vamos pôr em causa a lógica da globalização e da liberdade de circulação de capitais, há muitas conversas que não têm sentido.

Portugal passa todos os anos por uma crise psicológica em relação aos *offshores*. Essa crise teve um aspecto gigantesco por volta do ano 2000, quando o Governo, com uma reforma fiscal inadiável, resolveu impor algumas regras, sem considerar as consequências. Mas, na altura, tinha alguma defensabilidade, porque havia a convicção de que todos os países iriam colaborar para limitar a liberdade fiscal nos *offshores*.

Os Estados Unidos, no âmbito da OCDE, estavam a colaborar nessas medidas. Vários países europeus – que, normalmente, não colaboram – também estavam a colaborar. Quem sabe um bocado como é que isto funciona, tinha grandes dúvidas de que essa boa vontade viesse a traduzir-se fosse no que fosse.

Nesta matéria só há duas soluções: ou acabam os *offshores* todos ou quem os mantém beneficia da regulação que os outros introduzem. Isso é garantido. O grau de controlo que se pode ter, que é muito pequeno, reduz-se a zero, quando, por exemplo, se deslocalizam capitais da Madeira para outro *offshore* e a acção do Banco de Portugal de fiscalizar os bancos que estão na Madeira deixa de se poder exercer. Como não se vai proibir a livre circulação de capitais, estamos, no fundo, a encorajar quer os residentes, quer os não residentes, que trabalham com actividades financeiras portuguesas, a substituir a localização na praça financeira do Funchal por outras praças financeiras.

Os campeões da regulação – por exemplo, os ingleses – são sempre muito extrovertidos a dizer que se deve fazer colaboração fiscal, mas não se aplica a eles. Os franceses também estão sempre a dizer que se deve fazer harmonização fiscal dentro da Europa, mas quando chega a interesses franceses, não se aplica o princípio.

Como sabem, andam neste momento a lutar pela harmonização fiscal na Europa para não haver *dumping* por parte dos novos estados membros. Os países bálticos, por exemplo, têm taxas mais baixas em alguns impostos. Mas antes de ontem, contra a opinião de todos os outros parceiros da União, resolveram alterar e subsidiar a energia. Contra tudo o que estava combinado, o ministro das finanças francês, que está em campanha eleitoral para presidente, disse: “não o interesse da França é que conta; o resto não tem qualquer interesse para a França”. Bom, portanto, quando estamos a ter evidências destas de membros da União Europeia, que seria uma área de integração e transparência e de uniformidade de regras, devemos ter muito cuidado ao tentar raciocinar sobre os problemas.

Em relação às tecnologias, tenho para mim um princípio que resulta da história da humanidade. Quando uma tecnologia é capaz de dar resultados mais eficazes do que outra acaba por vencer. Acho que isso começou logo com a pedra polida em relação à pedra lascada e, depois, com o cobre e o bronze em relação ao ferro. À medida que uma tecnologia se torna mais eficaz, quem a aplica passa à frente dos outros. Se não for pela via pacífica acaba por ser por uma via agressiva.

Os Estados Unidos, neste momento, dão o melhor exemplo disso, são os mais agressivos. A China está a seguir pelo mesmo caminho. A Europa perde posições constantemente. A Europa vive ainda numa lógica de eurocentrismo que é legítima porque durante seis séculos tudo o que se passou no mundo começou na Europa.

Desde a inventiva financeira à revolução tecnológica, passando pela inovação nos sistemas políticos, nas reformas culturais e religiosas. Tudo começou na Europa desde o século XIV. Todas as mudanças. Mas desde a Segunda Guerra

I PAINEL

mundial que não é assim. Cada vez mais as mudanças não começam na Europa e não se concretizam na Europa. Nós ainda vivemos na ideia de que a Europa tem um modelo que pode impor aos outros. Pode impor-se dentro daquilo que são as regras da concorrência, mas não mais do que isso.

Veja-se o ritmo a que a Europa está a ultrapassar os seus problemas. Pelo menos já é a terceira vez que os dirigentes europeus anunciam que vamos resolver o problema do desemprego na Europa.

Foi assim com o Acto Único e o mercado interno do Sr. Jacques Delors, depois com a moeda única e agora temos o Tratado constitucional. Dizem-nos sempre que temos dezanove ou vinte milhões de desempregados na Europa – agora serão mais com os países novos –, mas que resolveremos o problema se criarmos um grande mercado, se optarmos por uma moeda única, se criarmos uma convergência política. Os desafios do desemprego e da competitividade não têm que ver com a dimensão.

Não há nenhuma regra que diga que um pequeno país é menos eficaz que um grande país. Vejamos na América Latina, na Ásia, na Europa: os que estão em melhor situação são os países mais pequenos. Portanto, o problema da dimensão não é o problema da eficácia.

Por isso, gostava de deixar estas duas componentes. É que as tecnologias vão mudando constantemente e aquilo que permitem acabar por ser feito por A ou por B. Se aceitamos a globalização europeia, não podemos deixar de ver o que se passa na porta ao lado.

Eu não queria falar do sector económico em geral, mas sobretudo da banca. No entanto, há aspectos comuns. Temos uma relação que não é muito saudável entre as autoridades e o sector privado em Portugal. Se há uma coisa que falta em Portugal é a iniciativa. O factor de que nós temos falta – e neste momento está a ser evidente – é a iniciativa. Não há empresários, os empresários não são bons, são os que temos, e ninguém quer ser empresário. Nem os advogados, nem os professores universitários, nem os sindicalistas. Ninguém quer ser empresário e não temos à porta uma fila de espera de investidores estrangeiros para virem criar empregos em Portugal. Portanto, vamos continuar com esta falta de iniciativa. E vamos pagá-la.

Devia haver uma relação de confiança, como há noutros países – em Espanha, nos Estados Unidos, na Inglaterra, em França –, uma relação de parceria entre todos os agentes económicos: o estado, os particulares, os cidadãos.

Hoje em dia, não se criam empregos sem essa relação de parceria, ou, então, é à força de dinheiro. Se não há um clima amigável para a iniciativa, a iniciativa vai instalar-se noutro sítio qualquer. E nós não temos uma atitude amigável em relação à iniciativa. Todos os anos se cria uma série de conflitos, de incidentes, que leva as pessoas a pensar se a localização em Portugal é a melhor.

O próximo Orçamento tem coisas dessas. Praticamente todas as SGPS, se o Orçamento for para a frente como está, sairão de Portugal, porque ficam na situação de não saber qual a fiscalidade que se lhes aplica. Ao mesmo tempo, outros países – como a Holanda ou a Espanha, por exemplo – estão a atrair as sociedades de gestão de participações.

Esta relação de parceria entre os agentes económicos e o estado, para criar o futuro, não é a que nós vivemos em Portugal. Temos uma tradição de séculos e justificada pela nossa história de desconfiança dos cidadãos em relação ao estado e do estado em relação aos cidadãos. Quando damos muitos poderes às instituições públicas, normalmente, os resultados são muito maus.

Eu não me queria alongar muito, mas vejamos os poderes que se deram às autarquias para controlar a qualidade do urbanismo e das implantações de habitações. Deu o resultado oposto e redundou na má qualidade da urbanização que nós temos em Portugal. Se houvesse uma regra simples e liberdade dentro dessa regra – cada um fazer o que entende e depois pagar as consequências se não cumprir a regra, que era uma coisa simples de se fazer – as pessoas saberiam quais os parâmetros. Alguém as fiscaliza, mas não é preciso autorização.

É sistema oposto ao que existia na União Soviética: se uma pessoa estava em Leninegrado e queria ir a Moscovo tinha que pedir licença três semanas antes. Depois vinha a autorização, ou não, na véspera. Nós em matéria de circulação não temos isso, mas em relação ao imobiliário contamos com coisas

I PAINEL

dessas: temos que pedir licença para tudo e para nada e acarretamos com os efeitos desse sistema.

Quando um acto administrativo tem valor acaba por ter um preço. Confiamos às autoridades autorizações para coisas que elas não têm condições para controlar. A Sra. Thatcher quando chegou ao poder reduziu para metade a taxa do imposto sobre os lucros das pequenas sociedades. Deu esta explicação ao parlamento: “Eu tenho que reduzir porque a minha administração fiscal não controla a fiscalidade das pequenas empresas.” Nos Estados Unidos aconteceu o mesmo.

Nós vivemos na ilusão de que a administração fiscal vai controlar a fiscalidade de milhões ou centenas de milhares de pequenas entidades. É claro que tal não chega a acontecer. Porque o risco de serem penalizados por não cumprirem as regras é muito pequeno. O número de casos em que a infracção é penalizada em Portugal é pequeníssimo e, portanto, compensa o risco de não cumprir as regras. Isso, aliás, acontece também nas estradas. O risco de circular fora das regras, no estacionamento, na velocidade, a probabilidade de serem penalizados é pequeníssima, portanto, é racional não cumprir.

Falando, agora, do problema da banca. A banca é um negócio de confiança; sempre foi. Não há nenhuma relação com o cliente que seja obrigatória. Os clientes entregam o dinheiro à banca para ser administrado. Os clientes pedem à banca para fazer pagamentos em seu nome. Os clientes pedem dinheiro emprestado à banca porque as condições são melhores e de maior confiança do que nos casos de empréstimos de penhor ou particulares. Portanto, é um negócio de confiança.

Os bancos que inspiram confiança têm a capacidade de se desenvolverem. Os que não inspiram confiança não têm tal possibilidade. Portanto, foi sempre central para a actividade bancária e seguradora uma relação de confiança. Tudo o que possa contribuir para que haja uma relação de confiança ajuda e permite melhores serviços aos clientes.

A relação era pessoal quando havia poucos clientes. Ainda no século XIX era tudo escrito à mão. As pessoas iam ao balcão, conheciam o gerente, tinham

uma relação pessoal. O gerente mandava-lhes os parabéns, mandava os parabéns pelo casamento do filho, pelo baptizado. Tudo aquilo se passava em termos de uma relação muito pessoal.

Hoje em dia isso é impossível porque há milhões de clientes. Os preços seriam de tal modo elevados que o negócio sairia de actividade se tentasse reverter a essa relação pessoal com cada cliente. Portanto, o que as instituições financeiras em todo o mundo mais evoluído fizeram foi informatizar todas as relações, excepto o *private banking*. Para alguns clientes que têm um grande volume de negócios continua a haver uma relação pessoal. Os gerentes de conta continuam a mandar um cartão no dia dos anos, pelo Natal, etc. Para o resto dos clientes tem que ser tudo informatizado.

Ora, a informatização deveria permitir o mesmo tipo de relação. Deveria permitir que os melhores clientes tivessem melhores condições. Devia permitir que essa relação – que, de algum modo, é impessoal – fosse tão personalizada quanto possível. E é isso que pretende. Isto implica várias coisas. Significa que, se nós, pela via informática, conseguirmos seleccionar os clientes que merecem confiança penalizamos, não só todos os outros, como estamos a penalizar aqueles que mantêm uma relação com eles em nome da banca.

Consideremos, por exemplo, o acesso ao cheque. Se não se erradica a possibilidade de um faltoso frequente e reiterado ter acesso ao cheque, não só estamos a aumentar os custos – porque esse incumprimento tem custos e esses custos têm que ser repercutidos por todos os outros clientes – como, sendo um cheque um meio de pagamento, acabamos por introduzir uma relação de insegurança nas relações que esse cliente vai ter com todas as pessoas com quem tiver negócios.

O cartão de débito é o meio mais fácil de controlar porque através dele o cliente só tem acesso aos valores que possa ter na sua conta em tempo real. Tudo bem, mas o cartão de crédito já não é assim. E, portanto, se não se conseguir manter um registo dos cartões de crédito com incumprimentos, estamos a prestar um péssimo serviço, não só aos outros clientes, como à sociedade em geral.

I PAINEL

A não possibilidade de se utilizarem registos para acompanhar a relação económica que os cidadãos têm com as várias entidades cria dois inconvenientes: o primeiro passa pelos custos que advêm para todas as pessoas que têm uma relação com o incumpridor; o segundo relaciona-se com a facilitação de comportamentos erróneos e anti-sociais.

Pela nossa experiência – e é difícil ser preciso porque não temos um serviço centralizado em relação aos cheques – deve haver umas três ou quatro mil pessoas que vivem de fraudes com cheques, mas é impossível registar as suas identidades.

Ainda que cada banco possa fazer esse registo não temos forma de comunicar uns aos outros e, portanto, o incumpridor quando tem um incidente com um banco é penalizado e fica inibido por algum tempo, mas, depois, acaba a inibição e vai a outro banco repetir a história.

São muito poucos milhares de pessoas, mas trata-se de incumpridores com um comportamento perfeitamente definido. Acho que isso se passa em todas as formas de criminalidade. É como as doenças contagiosas. Não erradicaríamos a lepra ou a tuberculose se não fizéssemos a despistagem. Ninguém acreditaria que se pudesse autorizar um alcoólico a ser piloto de um avião de carreira. Não faz sentido nenhum.

Portanto, há um certo tipo de comportamentos em que as sociedades devem ser mais ou menos exigentes – o que é que consideram comportamentos aceitáveis e inaceitáveis – e que não podemos tratar de uma forma anónima.

Outra questão tem que ver com a qualidade do serviço. É o problema do que se oferece aos clientes. O cliente é cliente global, não é cliente de cartões, ou de seguros, ou de uma actividade de *leasing*, ou de operações de bolsa. É cliente global. Qualquer pessoa dá melhores condições a um cliente que adquira, igualmente, outros serviços e bens. No caso do *private banking* isto é fácil de fazer, mas, noutras situações não é assim. Um cliente, por exemplo, pode ter prémios de seguros muito mais altos porque não se sabe que se trata de um bom cliente bancário. Acontece se não houver possibilidade de se confrontar estas realidades. Portanto, o que normalmente se tende a fazer em

todos os países é o *cross-selling*. Vender produtos de um ramo num outro ramo. Isto permite ter taxas de serviço muito mais baixas. Uma pessoa que tem um passado e um presente de cumprimento numa área é provável que tenha nas outras áreas. Portanto, pode-se oferecer melhores condições e correr mais riscos em relação a alguém que tenha um comportamento que é conhecido. A pessoa que não é conhecida é tratada pela média geral.

Ora bem, o último ponto que eu queria referir é a consequência disto. Nós não estamos em concorrência com os bancos portugueses e com as seguradoras portuguesas. Estamos em concorrência com todas as seguradoras europeias e americanas. E com os bancos europeus e americanos. Todos os nossos clientes melhores são visitados, todos os anos, pelo menos uma ou duas vezes, por representantes de bancos suíços e bancos americanos e ingleses, às vezes.

Se as nossas condições não acompanham as que eles oferecem, obviamente que deslocalizam as operações para esses bancos. A única solução é pôr bancos portugueses no estrangeiro nas mesmas condições. Na Suíça, ou em Londres, ou noutro sítio qualquer. Mas não é, digamos, uma situação muito agradável para ninguém.

Era melhor que assumíssemos as consequências daquilo que queremos. Ou queremos uma coisa ou queremos a outra. Ou vamos estar na concorrência internacional, ou pensamos que vamos ter condições específicas para Portugal.

Eu espero que possamos debater algumas destas questões e outras que têm que ver com isto. Felizmente, tem sido possível, quando se aborda – e por isto é que eu sublinhei isto no princípio – um problema muito concreto, aprofundar soluções e chegar a *modus vivendi* aceitável em termos de segurança e garantias de forma a termos de capacidade de oferecer serviços idênticos aos que outras entidades oferecem noutros países. Mas a atitude geral é um bocadinho diferente.

Acho que, se me permitem entrar em seara alheia, neste momento, os riscos maiores que os cidadãos têm em relação à protecção dos seus dados não passam pela gestão de ficheiros por entidades conhecidas e controladas. Os

I PAINEL

riscos maiores advêm do acesso a esses ficheiros por parte de entidades que nem se sabe quem são e incontroladas. Há riscos no comportamento de alguns aspectos do sector público em relação ao que está a acontecer.

Nós, neste momento, temos três grandes mudanças em curso no sector bancário. Uma que tem a ver com o *Basileia 2*. Quer dizer, as novas regras prudenciais que vão obrigar a ter tratamento diferente para os vários tipos de crédito. Seremos obrigados a ter modelos internos de *scoring* para que as condições de crédito oferecidas sejam diferentes. Isto passa a ser regra prudencial em todos os países que aderirem ao *Basileia 2*. Na prática, trata-se de todos os sistemas bancários avançados.

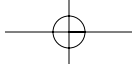
Temos a introdução das normas de contabilidade internacionais que também vão obrigar a regras uniformes e ficaremos dependentes dos auditores. São auditores internacionais e refira-se que são poucas as firmas de auditoria.

Vamos transpor para o ordenamento jurídico português a directiva de transparência sobre o pagamento de juros. Que dizer que teremos de fornecer, se a Suíça concordar, dados identificados sobre os nossos clientes ao fisco que, depois, os comunica ao fisco dos outros países onde as pessoas, porventura, estejam a residir.

Veja-se no caso dos emigrantes, por exemplo, o que isto vai implicar de confusão e, no entanto, o governo português optou por este regime quando outros que tinham gestão de poupança, como o Luxemburgo, a Bélgica e a Áustria, decidiram manter o regime anterior. Nós, singelamente, decidimos isto.

Ora, se há um confronto em matéria de rigor, eu acho que a história dos últimos trinta anos mostra isto. Nós temos tido muitíssimo poucos casos – e são todos da responsabilidade das entidades que os cometeram – de quebra de sigilo bancário. Muitíssimo poucos.

Mesmo em matérias muito mais nobres e em que a exigência devia ser maior – por exemplo, no segredo de justiça – a complicação é constante. Ora, entregar acesso de centenas de milhares de dados sobre clientes à administração fiscal e, depois, à administração fiscal de outros países torna incontrolável o rigor deste segredo. Há várias entidades que podem manipular esses dados.

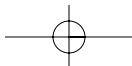
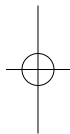
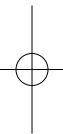


COLÓQUIO PROTEGER OS DADOS PESSOAIS

Tudo isto obriga a um grande profissionalismo e a ponderar as consequências de eventuais fraudes e desvios.

Acima de tudo, acho que é necessário penalizar os incumprimentos. Se há muitas regras, mas, depois, os casos flagrantes de incumprimento não são penalizados em tempo – se não há prontidão na penalização – os cidadãos estão muito desprotegidos.

Muito obrigado.



Diogo Vasconcelos

Gestor da UMIC – Agência para a Sociedade do Conhecimento, IP

A MODERNIZAÇÃO DA ADMINISTRAÇÃO

Muito obrigado.

Queria, antes de mais, agradecer aos Dr. Luís Silveira e ao Dr. Luís Barroso este convite. Gostaria de cumprimentar, também, o Dr. João Salgueiro e o Dr. Amadeu Guerra.

Vou aproveitar para fazer um pouco o ponto da situação daquilo que tem vindo a ser feito nesta área e de alguns projectos no âmbito dos quais tem havido uma colaboração, eu diria quase até exemplar, com a Comissão Nacional de Protecção de Dados.

A Comissão é um órgão que, no nosso entender, não só faz sentido, como, também, desempenha um papel fundamental num estado de direito que deve manifestar, obviamente, uma grande preocupação com a salvaguarda dos dados pessoais.

As questões da sociedade de informação não são questões tecnológicas, são questões essenciais para o desenvolvimento de um país e de uma comunidade. São questões para obrigar ao exercício da crítica para que Portugal seja mais competitivo. Estas questões revelam-se, ao mesmo tempo, fundamentais para a criação de uma sociedade de oportunidades. Uma sociedade em que

todos tenham capacidade de acesso e possibilidade de transformarem esse acesso em conhecimento e novas oportunidades.

Falarei de três áreas distintas.

Projectos que têm a ver com acessibilidade ao conhecimento, em primeiro lugar. No pressuposto que a inovação – uma condição crítica para a competitividade – implica o acesso ao conhecimento. Inovar é chegar à fronteira do conhecimento e, de alguma maneira, alargar essa fronteira, introduzir no mercado novos produtos e serviços, mudando as condições do mesmo.

Em segundo lugar, abordarei alguns projectos concretos no seio da administração pública que têm uma natureza transversal e nos quais temos responsabilidade.

Irei referir, por fim, de alguns projectos relacionados com o território e a grande importância das realidades locais para construir uma sociedade de informação sem discriminações, do ponto de vista geográfico, numa perspectiva de coesão económica e social.

Relativamente ao primeiro aspecto, o acesso ao conhecimento, vou falar aqui de alguns projectos em curso e que, em nosso entender, assumem um papel fundamental para mudar Portugal e criar condições completamente diferentes de acesso ao conhecimento.

A primeira das iniciativas é esta: a biblioteca do conhecimento *on-line* que lançámos no final de Março deste ano. Trata-se de um site, que está disponível em todas as cinquenta instituições universitárias e científicas que aderiram ao projecto neste primeiro ano. Esta biblioteca disponibiliza o acesso a mais de três mil e quinhentas revistas científicas de todas as áreas, do Direito às Letras, passando pela Biologia, a Engenharia, etc.

Trata-se de uma iniciativa de grande importância, na medida em que passam a estar à distância de um clique, um conjunto de milhões de artigos que posso – a partir de uma dessas instituições – aceder em texto integral, sem restrições em termos de número de *downloads*.

É uma iniciativa inovadora em termos internacionais porque não levanta restrições em termos de acesso aos estudantes. Ou seja, os alunos, os investiga-

I PAINEL

dores, os professores dentro do perímetro da universidade ou do centro de investigação gozam de acesso irrestrito. Normalmente, lá fora, tal acesso é restrito a professores, a investigadores e a estudantes de graduação.

A *Biblioteca do Conhecimento* permite, também, o acesso ao motor de pesquisa a toda a população. Ou seja, qualquer um de nós, que está aqui, mesmo que não esteja dentro de uma universidade, pode, livremente, de casa, do local de trabalho, pesquisar, em *b-on.pt*, através de uma palavra-chave ou de um autor, um determinado tema, uma determinada matéria e tem acesso, pelo menos, ao sumário.

Depois, obviamente, se quiser prosseguir essa pesquisa, poderá deslocar-se a uma qualquer universidade ou biblioteca e, munido do seu computador, ou usando o equipamento informático disponível na instituição, aceder ao texto integral e fazer o *download* do PDF ou imprimir o artigo de seu interesse.

Para terem uma ideia do impacte e da revolução que está a constituir este projecto, em termos de facilitar o acesso ao conhecimento, desde o final de Março até ao final de Julho, o número de *downloads* de artigos, cifrou-se em de cerca de um milhão e cinquenta e um mil. O número de pessoas que, em Portugal, dentro destas instituições fazem investigação, ou dão aulas, ronda as vinte mil. O número de potenciais utilizadores das instituições que assinaram estes contratos cifra-se em cerca de duzentos e cinquenta mil. Estamos, portanto, a falar de números muito interessantes, até porque, a divulgação foi feita, sobretudo, nas instituições, não foi realizada ainda uma campanha de divulgação. Há, conseqüentemente, todo um conjunto de utilizadores que ainda estão a despertar para isso, nomeadamente, os estudantes, mas a utilização é expressiva. O número de *downloads* é bastante expressivo.

O conhecimento científico expresso nestes artigos deixa de ser um exclusivo das universidades e instituições dotadas de vastas e bem apetrechadas bibliotecas e fica ao alcance de investigadores e estudantes de todos os países.

Este projecto vai continuar no próximo ano, expandindo-se o número de conteúdos de áreas que estão presentemente menos representadas. Englobará, também, conteúdos em português, nomeadamente na área do Direito, em que ainda há muito conteúdos que temos todo o interesse em disponibilizar.

Numa segunda fase, as teses de mestrado, doutoramento, etc., serão, igualmente acessíveis. A existência do motor de pesquisa, torna tudo mais fácil, na medida em que facilita, muito significativamente, o acesso ao conhecimento. Portanto, este é um projecto que nós consideramos verdadeiramente estrutural para mudar as condições de acesso ao conhecimento, em Portugal.

Um outro projecto, que nos é muito caro, e que lançámos logo no início do nosso trabalho, é os projectos dos Campus Virtuais, mais conhecido por *e-u – Electronic University (Universidad Electrónica)*, foi a marca criada para o efeito. Trata-se de dar conectividade sem fios a todas as escolas do ensino superior portuguesas. O objectivo é proporcionar condições, em articulação com um conjunto de trinta parceiros – alguns dos quais do sistema financeiro; praticamente todos os bancos portugueses – para que estudantes e professores possam adquirir em condições favoráveis equipamentos portáteis.

Em terceiro lugar, pretende-se incentivar as universidades a colocarem e a desmaterializarem toda a sua informação e serviços e a partilharem os seus conteúdos. Os conteúdos são organizados de forma *standard*, de acordo com normas internacionais, para permitir a própria troca de informação entre as várias universidades.

Este projecto foi lançado há cerca de um ano e meio. Lançou-se um conjunto de pilotos e depois uma *call*, digamos assim, a todas as universidades que quisessem participar. Todas, sem excepção, apresentaram candidaturas. A iniciativa está no terreno. As maiores universidades, como, por exemplo, a universidade do Porto – a maior do país – já têm, praticamente instalada, toda a sua rede. O seu sistema de informação, disponibilizado na *web*, já está em dezassete faculdades. O mesmo se pode dizer da universidade do Minho e da universidade de Aveiro. Até ao final do primeiro trimestre de 2005, estará praticamente concretizado, nessa componente, sobretudo a nível das infra-estruturas. A componente dos conteúdos e serviços demora mais tempo e depende, obviamente, do ritmo e da preparação, digamos assim, de cada uma das universidades.

Há uma inovação também interessante, que é a mobilidade. A possibilidade de um estudante, por exemplo do Instituto Politécnico de Bragança – que foi,

I PAINEL

aliás, o primeiro a ficar com a sua rede completamente pronta –, poder deslocar-se, aqui a Lisboa, ao Instituto Superior Técnico. Eventualmente para fazer um curso, ou para frequentar qualquer acção de formação. Esse aluno poderá ter acesso à rede, como se estivesse na sua própria escola. Portanto, há aqui um sistema de *roaming* e de mobilidade relativamente inovador e que antecipa em dois anos aquilo será feito ao nível europeu.

Gostaria de referir que é uma rede, pela sua dimensão, que é a maior, a nível mundial. Estamos a falar de duzentos *hotspots* e de mais de quinhentos postos públicos de acesso.

Um outro projecto que é fundamental para que tudo isto faça sentido, tem a ver com a oferta de condições de conectividade. A partir do momento em que se disponibilizam muito mais conteúdos, em que a necessidade de troca de informação entre a comunidade, dentro da universidade e fora, cresce exponencialmente, é necessário, de facto, criar super auto-estradas – não meras auto-estradas – que permitam um acesso mais facilitado ao conhecimento.

Para esse efeito, foi lançado, através da Fundação para a Computação Científica Nacional, um concurso público internacional para construir um cabo de fibra óptica entre os pólos académicos de Lisboa, Coimbra, Aveiro, Porto e Braga, que vai permitir larguras de banda, até agora impossíveis de imaginar, no seio universitário. O cabo de fibra óptica tem vinte e quatro pares de fibra, portanto, uma capacidade, praticamente ilimitada. Tem uma largura de banda de dez *gigabytes* por segundo. Pode aumentar, facilmente, para quarenta *gigabytes* por segundo, nesta fase, é perfeitamente razoável. Estará em testes em final de Dezembro e vai permitir um acesso aos utilizadores, ou seja, às instituições beneficiárias, de cerca de dois *gigabytes* por segundo.

Para terem uma ideia e uma comparação com o estado actual, a universidade do Porto – a maior do país, com trinta mil alunos – tem, hoje em dia, oitenta *megabytes* de conectividade e vai passar a dispor de dois *giga*. É uma multiplicação por vinte e cinco.

Deparamo-nos aqui com grandes oportunidades em termos de inovação, computação em rede, troca de bases de dados pesadas – por exemplo, na área

das ciências da vida, da Genómica, etc. – e revelam-se, simultaneamente, possibilidades novas na área do ensino à distância. À medida em que se revelar necessário a rede será alargada a outras instituições. Estas instituições, só por si, já justificam o projecto porque representam setenta por cento das instituições do ensino superior. Setenta por cento dos alunos que estudam no ensino superior, em Portugal. Trata-se de uma rede própria que vem substituir um conjunto de circuitos alugados aos operadores de telecomunicações.

Gostaria de referir que, obviamente, faz sentido investir no ensino superior, mas faz sentido aplicar recursos, ainda mais, no ensino básico e secundário.

Nesse sentido, foi, também, lançado um concurso público internacional para dotar todas as escolas do ensino básico e secundário de acesso em banda larga. É um investimento fundamental porque só a banda larga permite, de facto, criar redes em cada escola e assegura que os equipamentos dessas redes sejam totalmente ligados à Internet, com boas condições de largura de banda. Esse concurso foi um concurso público, feito como deve ser, com participação do mercado. A 1 de Outubro foi celebrado contrato e, neste momento, estão a ser equipadas cento e vinte escolas por dia. Até ao final do ano devem ficar ligadas cerca de metade das escolas prontas e o processo será concluído para as restantes antes de 2006.

Estamos a falar de cerca de nove mil escolas do ensino básico e secundário. Gostaria de dizer que, obviamente, a conectividade é importante, mas há outros aspectos, também fundamentais. Desde logo, a introdução de uma cadeira nova – de tecnologias de informação e comunicação – como parte integrante do curriculum do nono e do décimo ano. Uma iniciativa do Ministério da Educação, que vai ter um impacte, a meu ver, muito importante, na medida em que, só este ano, o nono e décimo ano contam com cento e oitenta mil alunos, que vão ter uma cadeira de uma hora e meia, no nono ano e três horas no décimo ano, de tecnologias de informação. Portanto, foram criadas cerca de mil salas de aula, perfeitamente equipadas.

Os editores de livros escolares produziram excelentes manuais, que estão, neste momento, a ser adoptados. Também no ensino básico, as autarquias

I PAINEL

foram financiadas para equiparem as escolas do ensino básico e para equiparem os quatro mil estabelecimentos do ensino pré-escolar. Portanto, os próprios jardins escola. Porque é importante, obviamente, disponibilizar conteúdos didácticos, que possam ser usados pelos professores, o Ministério da Educação está a preparar um portal de conteúdos didácticos, que será lançado no próximo ano.

Gostaria, agora, de referir alguns projectos que, a nosso ver, são bastante importantes. Têm natureza transversal. Ou seja, envolvem, normalmente, mais do que um ministério. É a nossa área de intervenção porque temos uma vocação subsidiária, relativamente às estruturas próprias, tecnológicas, dos vários ministérios. A visão aqui não é, propriamente, uma visão de que a tecnologia resolve tudo. É uma visão de que a tecnologia é capaz de ajudar à transformação e à monitorização da administração pública. Numa lógica de que ela deve servir, cada vez mais, os cidadãos.

Hoje em dia os cidadãos vivem numa economia de mercado em que a oferta faz tudo para agradar, digamos assim, aos caprichos da procura. Os cidadãos partem dessa expectativa, totalmente legítima, para exigir o mesmo a uma administração pública que tem de revelar-se, necessariamente, mais eficiente o que a obriga, claramente, a usar de forma inteligente as tecnologias de informação.

Um dos projectos mais relevantes que em investimos é o Portal do Cidadão. Trata-se de organizar todo um conjunto de serviços, dispersos por múltiplas entidades da administração pública, num portal que permita que as pessoas e as empresas saibam como resolver problemas: como aceder à informação e a serviços interactivos ou transaccionais.

Cento e dezoito entidades disponibilizaram-se para colaborar, mais do que as cinquenta que tínhamos, inicialmente, previsto. Setecentos e trinta e quatro serviços estão disponíveis, metade dos quais informativos, interactivos ou transaccionais. Os serviços informativos são importantes porque, ao contrário do que era a nossa expectativa, os estudos que fizemos revelaram que o cidadão muitas vezes não tem a quem perguntar, apesar da necessidade de aceder à

informação. Os serviços interactivos são nevrálgicos, porque as pessoas, hoje em dia, numa lógica que tem vindo a ser impulsionada pelo mercado, obviamente que pretendem recorrer a este canal como um canal alternativo, em relação aos canais físicos que, normalmente utilizam, para terem acesso à administração pública.

Um dos serviços novos refere-se à alteração de morada. Nesta primeira fase é um serviço híbrido, ou seja, posso desencadear o processo de alteração de morada num conjunto de cerca de catorze entidades e depois entregar um formulário único que é desencadeado pelo site, num conjunto de entidades públicas. Este serviço será totalmente desmaterializado já no próximo ano, mas nesta fase, punha-se desde logo a questão do tratamento dos dados pessoais são gerados por este serviço.

Estudámos este problema com a Comissão Nacional de Protecção de Dados e gostaria de agradecer a disponibilidade, a prontidão, ao contrário daquilo que muitas vezes algumas pessoas dizem, que encontrámos na Comissão Nacional de Protecção de Dados.

A Comissão revelou-se, de certa forma, até um aliado porque nos ajudou a identificar alguns problemas, a resolver de forma profilática esses problemas e isso permitiu-nos depois perspectivar formas aperfeiçoadas de desenvolver o serviço. Foi um caso em que se solicitou uma autorização à Comissão de Nacional de Protecção de Dados e cuja análise permitiu que este serviço fosse lançado sem qualquer tipo de constrangimento ao nível legal.

Gostaria de dizer que esta primeira fase foi muito importante por via da criação da rede, de engajamento de entidades públicas de criação de uma taxionomia, etc., e os resultados estão à vista. Constatam-se mais de três milhões de *page views* mensais e temos, portanto, um site crescentemente utilizado por cidadãos e empresas.

Refiro apenas a primeira fase. A segunda fase é mais complexa porque implica mudar procedimentos e, depois, colocar esses procedimentos refeitos, digamos assim, alterados, na Web, ou seja, desmaterializar de tornar de facto o serviço.

I PAINEL

Identificámos um conjunto de projectos que foram sugeridos aos vários ministérios e estamos a seleccionar esses projectos.

Alguns projectos são de grande relevância do ponto de vista económico como é o caso, por exemplo, da desmaterialização do processo da criação de empresa. É um projecto que envolve vários ministérios cuja liderança operacional caberá, obviamente, ao Ministério da Justiça, mas agregando, provavelmente, os ministérios das Finanças, Segurança Social, Ambiente e das Actividades Económicas e do Trabalho. O objectivo visa acelerar o prazo de criação de novas empresas. Este projecto será colocado a concurso ainda este ano. É um dos projectos mais complexos, mas também dos mais mobilizadores dada a sua relevância do ponto de vista da competitividade do país.

Entre outros projectos importantes destaco áreas da particular responsabilidade do Ministério da Justiça, não só ao nível do registo de pessoas colectivas, mas, sobretudo, ao nível da Direcção Geral de Registo e Notariado. O actual Ministro da Justiça tem tido um empenhamento exemplar nesta área e, portanto, irão ser anunciados em breve um conjunto de iniciativas muito relevantes no âmbito deste ministério que assume um papel fundamental em tudo o que tem haver com as políticas do chamado governo electrónico.

Gostaria de referir um outro projecto que tem, também, um impacte significativo pelas poupanças que gerou e pode gerar. Trata-se de um projecto que pode aumentar a transparência do processo aquisitivo público e dar maiores oportunidades no acesso ao mercado por parte das empresas, designadamente pequenas e médias empresa.

Este projecto, capaz de estimular a reconversão das empresas para a economia digital, é um programa mensal das compras electrónicas que está em fase de execução. O programa incorpora vinte e cinco projectos interdependentes e as poupanças que foram realizadas na fase experimental, em certas áreas de determinados ministérios empenhados na iniciativa, geraram poupanças muito significativas. A poupança média cifrou-se em vinte e sete por cento e nalguns casos registaram-se reduções de gastos de sessenta e sete por cento. Abrimos uma linha de financiamento muito recentemente que vai permitir a generalização destes projectos a todos os ministérios ao longo do ano de 2005.

Estamos, neste momento, a preparar a criação da Unidade Nacional de Compras: uma entidade que irá ter responsabilidades ao nível do *sourcing* estratégico para a administração pública em colaboração com os vários ministérios.

Uma das iniciativas mais relevantes é o Registo Nacional de Fornecedores, que também já foi discutido com a Comissão Nacional de Protecção de Dados. O concurso já foi lançado e as propostas serão entregues no final desta semana.

Este Registo Nacional de Fornecedores permitirá criar uma base de dados dos fornecedores da administração pública, facilitando a vida às empresas ao dispensar a necessidade de entrega repetida de documentação para participação em concursos. O Registo Nacional de Fornecedores prevê, também, um conjunto de ligações a outras instituições de âmbito público de modo a que certos requisitos essenciais à contratação pública sejam necessariamente respeitados. Nesta iniciativa temos vindo a contar com a colaboração da Comissão Nacional de Protecção de Dados. Ainda em Novembro será colocado em linha um site de características informativas. O site *Compras.gov.pt* disponibilizará toda a informação acerca dos concursos que vão ser lançados, sobre as melhores práticas no sector privado e no sector público, com perguntas frequentes, com explicação da legislação, etc. Pretende-se, assim, incentivar cada vez mais a utilização dos meios electrónicos no aprovisionamento público e levar o conjunto dos fornecedores actuais e potenciais do estado a utilizar este tipo de meios.

Gostaria de destacar, também, como área de colaboração com a Comissão Nacional de Protecção de Dados o projecto-piloto do voto electrónico que decorreu nas últimas eleições para o Parlamento Europeu. A questão do voto electrónico é muito controversa, mas creio que consubstancia uma iniciativa na qual vale apostar pelo potencial que poderá revelar ao nível do combate à abstenção.

Nós defendemos a deslocalização do voto, ou seja, que cada eleitor possa votar na assembleia de voto que lhe for mais conveniente, independentemente de ser aquela onde se recenseou ou não.

I PAINEL

O piloto realizado nas Eleições europeias teve como objectivo sensibilizar os eleitores, testar várias soluções tecnológicas e avaliar o impacte junto das populações. Os testes foram realizados com a participação de cerca de nove mil eleitores, registando-se uma receptividade bastante boa. Os resultados podem ser consultados no site. O site apresenta os resultados das sondagens feitas sobre satisfação do eleitor, a descrição de todo o processo e a auditoria de todas as Universidades que contratadas para o efeito. O voto electrónico contou com um acompanhamento a par e passo da Comissão Nacional de Protecção de Dados. O projecto da UMIC e do Secretariado Técnico dos Assuntos para o Processo Eleitoral teve a aprovação unânime da Comissão Nacional de Eleições. Aprecia-me registar neste particular o trabalho muito rigoroso e o grau de exigência da Comissão Nacional de Protecção de Dados relativamente à utilização dos dados, nomes e números de eleitores constantes nos cadernos eleitorais utilizados nas experiências piloto. A CNPD acompanhou *in loco* toda a experiência, disponibilizando técnicos para fiscalizar todas as fases de votação e escrutínio. Este contributo foi particularmente importante pelos dados que proporcionou sobre a salvaguarda da privacidade que será um elemento fundamental para a discussão do assunto quando a Assembleia da República vier a discutir esta matéria de sua competência reservada.

Uma palavra, ainda, sobre o apoio a projectos visando uma maior coesão social. A UMIC apoia instituições activas na área de apoio à deficiência. Utilizar as tecnologias para vencer barreiras provocadas por diversas formas de deficiência é um dos nossos desafios. Nesse sentido foram investidos cinco milhões de euros para o desenvolvimento de novas tecnologias que permitam vencer a deficiência.

Gostaria de falar, também, muito sucintamente, acerca daquilo que se está a fazer para a criação de postos públicos de acesso à Internet. O objectivo inicial de dezasseis postos por cada cem mil habitantes foi já ultrapassado graças às iniciativas que foram lançadas e à resposta do mercado. Um desses postos públicos conta-se entre os maiores da Europa. Trata-se do Parque das Nações, cuja área de cem hectares é, hoje em dia, toda ela servida por uma rede de acesso em banda larga Hi-Fi.

COLÓQUIO PROTEGER OS DADOS PESSOAIS

A questão das cidades digitais foi generalizada a todo o país com o objectivo de criar impacte ao nível da inovação da criação de riqueza. O território nacional não está todo coberto, hoje em dia, por banda larga e sem banda larga massificada não há Portugal do século XXI.

Estamos, portanto, a trabalhar no sentido de utilizar fundos nacionais e comunitários para disponibilizar infra-estruturas nas regiões onde há oferta insuficiente de modo a que todo o país venha a ter banda larga em condições competitivas. Trata-se de um pressuposto essencial para uma sociedade e uma economia baseada no conhecimento. Tal desiderato corresponde precisamente aos objectivos da famosa Estratégia de Lisboa, reiterados no Conselho Europeu de Vila da Feira.

Por último, queria, mais uma vez, agradecer a colaboração que até agora tem sido dada pela Comissão Nacional de Protecção de Dados. Outros projectos se seguirão, cada vez mais complexos e exigindo ainda um maior esforço de trabalho conjunto.

Muito obrigado.

I PAINEL

Debate

Eugénia Costa

DGEMN

Muito boa tarde. Chamo-me Eugénia Costa e sou da DGEMN – Direcção Geral de Edifícios e Monumentos Nacionais. Eu tinha uma pergunta para fazer ao Dr. Diogo Vasconcelos que tem a ver com a questão do primeiro projecto que foi apresentado. Gostava de perceber como é que foi feita, com que critérios e por quem, a escolha dos títulos das três mil e não sei quantas revistas que estão neste momento, disponíveis? Foi um processo desenvolvido pelos aderentes, por universidades? Quem é que fez essa escolha?

Muito obrigada.

Moderador

Vamos juntar talvez três ou quatro questões e depois respondermos a todas ao mesmo tempo.

Garcia Pereira

Advogado

Muito boa tarde. O meu nome é António Garcia Pereira, sou advogado e sou dos tais que não querem ser empresários.

Queria começar por fazer uma referência ao colóquio, ao papel da Comissão e à esmagadora ausência da grande comunicação social, designadamente, das televisões. Não deixa de ser significativo. Isto é, estarão os jornais, estará a rádio – a “TSF” já ouvi hoje de manhã – esteve aí, eventualmente, “O Público”. Se a Comissão Nacional de Protecção de Dados porventura se tivesse lembrado de convidar o ministro Gomes da Silva ou o Prof. Marcelo Rebelo de Sousa teria aqui uma transmissão em directo. Como está discutindo questões que são muito sérias e apelam à inteligência, à capacidade crítica e à reflexão estratégica – para a necessidade da qual o Dr. João Salgueiro chamou à atenção – falta a grande comunicação social.

De facto, no nosso país, não somos o único, predomina hoje uma cultura da frivolidade, do momentâneo, do instantâneo, do actual em detrimento do futuro e, todos aqueles que aparecem, independentemente dos pontos de vista que tenham, com a preocupação de olhar para diante e fazer uma reflexão a dez ou a vinte anos, são olhados como uma espécie de marcianos com anteninhas, porque, naturalmente, interessa muito mais saber o que é que logo à noite vai dizer a Cinha Jardim ou outro qualquer personagem da vacaria das celebridades. Bom, e saliento isto, porque falamos hoje de um problema sério.

É um problema sério, a questão da protecção de dados – e depois vou à questão –, mas este problema da protecção de dados tem que ver com um problema de cultura de cidadania, dos cidadãos e das organizações. Todas elas. Do sector público e do sector privado. E ao que hoje, exactamente, se assiste, é à demolição dessa cultura de cidadania. E à tentativa de, digamos, de desarmar as pessoas – desde logo, pela desinformação e pelo desconhecimento dos seus direitos – mas, não é apenas pela negativa. Quer dizer, esta contraposição, que eu procuro fazer aqui, tem a ver com a tentativa de criar pessoas que não pensam, que não reflectem, que não reagem, que não têm espírito crítico, que reagem apenas aos estímulos de momento.

Faz-se apelo aos instintos mais baixos, em vez de se apelar aos instintos e aos sentimentos mais elevados que todos os cidadãos – entre os quais aqueles que

I PAINEL

como nós estão aqui – têm. Eu acho que isto é uma reflexão muito séria. Isto exige, de facto, dos cidadãos que pensam; exige uma rebelião. Quer dizer, não basta resistir civicamente. É preciso rebelar-se civicamente contra este processo em curso de acarneiramento colectivo. É muito séria a questão.

Porque num Colóquio promovido por uma entidade que tem desenvolvido um trabalho de grande qualidade, como todos os intervenientes até agora salientaram, não só pelo conteúdo das suas intervenções, mas, também, pela preocupação de ser célere e eficaz. É um exemplo de equilíbrio entre, digamos, aquilo que poderia ser um excesso regulamentador e aquilo que poderia ser o *non facere* absoluto, na lógica de que aquilo que existe por si próprio está justificado só pelo facto de existir. Não é, portanto, inocente esta circunstância e não podia deixar de calar esta referência que me parece importante.

Depois, eu acho que o Dr. João Salgueiro não quis entrar numa reflexão sobre as questões jurídicas, mas, se calhar, devia ter ido por aí. Porque o direito está muito necessitado da reflexão feita de fora para dentro relativamente ao que é o seu papel no século XXI numa sociedade com as características da nossa. O facto do direito não ter feito essa reflexão tem conduzido a um problema com o qual, seguramente, a Comissão Nacional de Protecção de Dados também se tem debatido: há um número sempre em aumento de normas, cujo grau de eficácia e de operatividade é, crescentemente, menor. Portanto, há que discutir – e entre nós nunca se discutiu – os actuais poderes. Isto é um défice de reflexão da nossa sociedade no seu conjunto.

O direito, o mundo do direito, não reflectiu sobre uma circunstância que, olhando para os últimos dez anos, redundando nisto: sai hoje uma norma jurídica para regular um determinado fenómeno – económico, financeiro, social –, mas o impacto demolidor das novas tecnologias da comunicação e informação, estilhaçando as noções tradicionais de tempo e de espaço e acelerando imenso os processos de diferenciação socio-económica, leva a que a lei chega àquela realidade quando ela já não está lá. Está um quilómetro adiante e, então, a reacção instintiva do legislador é: “eu faço uma nova lei, agora, para tentar ir buscar a realidade que está lá mais adiante”. E, evidentemente, quan-

do a segunda lei sai a realidade já está ainda mais distante. Nós temos tido legisladores, ou um legislador, que actua como o perdido no deserto, sempre vendo o paraíso distante ou o oásis por detrás da duna seguinte. Com uma proliferação, pirotecnia, ou outra coisa até, que, às vezes menos agradável, se chama também legislativa...

Moderador

Precise a pergunta, por favor.

Garcia Pereira

Advogado

Sim, já lá vou, mas acho que esta reflexão é importante. Pronto!

Uma proliferação legislativa que varia na razão inversa da capacidade operativa da norma jurídica. Isto é muito importante e vou, então, direito à pergunta.

Assistimos, actualmente, a um grau muito superior de coactividade das normatividades dos poderes de facto sobre a normatividade formal dos poderes, digamos, estatais tradicionais. Hoje, normas de conduta, padrões de comportamento e regras, que nos chegam, designadamente através da Internet – e daí que alguns sustentem que isso é um campo do não direito – modelam mais comportamentos sociais do que trinta que trinta decretos-leis publicados no Diário da República.

A questão que eu coloco é: numa sociedade com as características da nossa – de Portugal, da Europa e do mundo – a posição face, digamos, à evolução dos fenómenos, designadamente na área económico-financeira, deve ser a de querer tudo regular, desconhecendo essa realidade? Deve ser a de que o direito tem que se subordinar às evoluções da economia?

Quando as multinacionais, sejam do sector da banca doutro qualquer, dizem, “aqui estão a apertar-nos muito os calos; deslocalizo-me e vou para outro

I PAINEL

lado”, a nossa reacção, enquanto sociedade politicamente organizada, deve ser a de ceder a essa chantagem? Porque hoje assistimos a uma chantagem!

Quer dizer, isto transporta, de facto, a análise para uma análise mais global, mas hoje, estamos perante um estado de chantagem permanente. Ou cedemos na desregulação a todos os níveis, designadamente na protecção dos dados pessoais, ou ficamos isolados no mundo.

Acho que há aqui um combate de cidadania que ultrapassa também as fronteiras e que deve impor uma solução diferente. É que nós temos um modelo de sociedade cujas regras fundamentais, digamos, corporizam a nossa forma de viver e de estar no mundo. Essas regras não passam pela lógica de que os fins justificam os meios. Essas regras não passam pela lógica da admissibilidade em nome do “quem não deve não teme” e outras barbaridades que seguramente a Comissão Nacional de Protecção de Dados já ouviu muito mais vezes do que eu. É uma lógica que normalmente justifica que tudo se devasse, tudo se conheça.

Quando, por exemplo, se sabe – eu não mando dizer por ninguém aquilo que tenho a dizer – que na banca algumas das instituições da associação a que o Sr. Dr. João Salgueiro preside têm, neste momento, formas de tratamento informatizado das facturações telefónicas, dos telemóveis que atribuem aos seus funcionários como instrumentos de trabalho e que parecem ser utensílios muito agradáveis.

Até ao momento em que se começa a tratar da facturação e se estabelecem programas informáticos que apuram os dez números com ligações mais frequentes e os dez números para que mais se telefonou. Cruza-se isso com bancos de dados, designadamente, os dos telefones dos escritórios dos tais advogados que não querem ser empresários, para detectar imediatamente se há um trabalhador que até comete a ousadia de telefonar para um advogado para se informar acerca dos seus direitos em matéria laboral. E quem nos defende de uma coisa deste tipo, visto que não há, neste momento, nenhuma espécie de controlo?

Eu concordo quando diz que era muito importante punir sobretudo os excessos – e punir de uma forma que não torne racional incumprir – mas, neste

momento, reina a lei da selva nessa matéria. Portanto, temos que ceder à chantagem, ou temos que nos entender quanto a regras fundamentais de cidadania, relativamente a esta matéria da protecção dos dados pessoais? Muito obrigado.

Interveniente não identificado

Há pouco ao ouvir a intervenção do Dr. Diogo Vasconcelos pensei que nem estava em Portugal. Queria felicitar a Unidade de Missão, Inovação e Conhecimento pela apresentação que fez aqui e pela situação concreta que relatou. Queria saber qual é a preocupação, neste momento da Unidade de Missão relativamente ao sem-número de cartões que nós temos: bilhete de identidade, número de contribuinte, cartão de saúde, cartão de eleitor?

Vejo com preocupação que o Ministério da Saúde fala em criar um novo cartão com dados que têm a ver inclusivamente com o rendimento das pessoas. Qual é a posição também da Comissão em relação a isso?

Muito obrigado.

Moderador

A palavra ao Dr. Vasconcelos.

Diogo Vasconcelos

UMIC

Muito obrigado. Relativamente à questão que a Dra. Eugénia Costa levantou refiro que a ideia de se criar uma biblioteca agregando as mais importantes revistas que codificam o conhecimento, ou revistas científicas, é muito antiga. É uma ideia com mais de dez anos – o que muda a realidade é a implementação, não é apenas ter ideias – e, portanto, nós achámos que se tratava de um projecto essencial e investimos muito tempo nele.

I PAINEL

Fizemos um levantamento junto das instituições académicas e científicas, um inquérito para saber o que é que assinavam e a que preço. A maior parte das instituições respondeu. A partir desses dados, feito o levantamento dos principais, digamos assim, agentes de mercado que disponibilizam essas ofertas, encetámos negociações e fizemos, depois, uma nova ronda de encontros com as instituições potencialmente beneficiárias para sabermos aquelas que, efectivamente, estariam dispostas a entrar neste projecto. Pagando metade. Portanto, o governo assumiu metade e as instituições assumiram metade o que foi uma forma expedita de avançar com o projecto.

O projecto só em si já se justificava mesmo se não houvesse envolvimento do Governo, mas, infelizmente, durante bastante tempo, discutiu-se muito e nada se fez e, portanto, nós achamos que assim era uma forma expedita de avançar. Na maior parte dos países em que existem iniciativas deste género há também um financiamento público que nós entendemos ser perfeitamente justificado porque estamos a falar de algo fundamental na sociedade do conhecimento. Falamos de dar acesso, democratizar, digamos assim, o conhecimento. Portanto, se quiserem, em última instância, fomos nós que escolhemos. Entretanto, o projecto foi lançado e criou-se através um grupo de pessoas representativas das universidades, bibliotecários, etc., que já está a trabalhar connosco no sentido de identificar, de analisar, os conteúdos actuais e novos conteúdos. Iniciaram-se já negociações com outras editoras internacionais, no sentido de agregar mais conteúdos, sobretudo, de áreas que nesta primeira fase não estão tão bem cobertas. Trata-se, portanto, de um trabalho colaborativo. Eu penso que o mais importante é que se fez. Está em linha. Melhorou significativamente as condições de acesso ao conhecimento.

Quanto à questão do cartão. Eu creio que o desafio que se lança passa por termos um sistema de autenticação que seja comum à administração pública. Esse sistema de identificação deve estar disponível em qualquer tipo de suporte. Estamos a trabalhar com o Ministério da Justiça no sentido de apoiar o lançamento de um bilhete de identidade que vai ter funcionalidades muito diferentes do actual. É um processo, aliás, que, provavelmente, vai ter que contar também com a colaboração da CNPD.

Entendemos que a melhor opção para evitar a proliferação de sistemas próprios de cada uma das entidades é reconhecer-se o registo civil como base de dados fundamental à qual todas as entidades públicas devem recorrer quando querem certificar a identidade de um cidadão nacional.

João Salgueiro

Associação Portuguesa de Bancos

Tenho que agradecer ao Dr. Garcia Pereira ter trazido à discussão um ponto mais amplo. Eu, aliás, acho que extravasei um bocadinho para uma crítica ao sistema actual de justiça que temos em Portugal. Portanto, acho que fui até ao ponto onde podia ter ido. Que é levantar o problema e algumas das suas consequências. Se começasse a dar soluções, não sei quantos advogados estarão na sala, mas, se calhar, nenhum concordava comigo. Ou as opiniões dividiam-se muito e não era o tema de hoje.

Mas falei de várias coisas, como as do incumprimento, do excesso de normas, de não haver sancionamento pronto, etc. Não posso estar mais de acordo com algumas das considerações que fez. Em relação à banca nós não temos na Associação nenhum sistema informático para ver o que os gestores da banca fazem. Não somos tão sofisticados quanto isso. Portanto, acho que a única resposta é, nesses casos, proceder. Não vejo outro mecanismo senão proceder em relação a qualquer incumprimento. Seja em que campo for, não é?! Aliás, há matérias que uma Associação não deve tocar quando envolvem aspectos que nada tenham que ver com sua actividade própria. Mas nesse caso poderíamos intervir se soubéssemos, mas não dispomos nem de registo, nem de averiguação.

Agora, a questão que põe, eu acho que é um bocadinho mais ampla e, antes de chegar à pergunta – como o nosso moderador lembrou, muito bem, tínhamos uma pergunta – mas fez considerações que acho muito pertinentes e muito amplas. Eu não acredito que uma pessoa que tem uma doença grave, se cure, normalmente, com um chá de limão. Pode ser que se cure, mas não

I PAINEL

é normal. E para nós, esses problemas que põe, têm que ver com a estrutura da sociedade, em geral, e da sociedade portuguesa, em particular. A comunicação social não está aqui porque tem padrões de desempenho que a gente conhece.

Nós temos uma sociedade em que se encoraja o consumo e o sucesso. As pessoas são educadas para serem avaliadas pelo sucesso e pelo nível de consumo. E começam logo desde a escola. O mercado, quanto mais vender, mais realiza a sua função. E os meios de comunicação social, quanto mais ajudarem a vender, mais receitas de publicidade têm. Em particular a televisão.

A televisão não informa a propósito do consumo. Uma primeira função – informar sobre um modelo novo que surgiu – que deveria cumprir, mas, de facto, não é isso que faz. Ela apresenta logo ali uma sugestão de que a pessoa tem que comprar e tenta dirigir-se directamente aos instintos da pessoa. Portanto, é uma máquina para estimular as pessoas a consumir. A política também caiu para esse lado porque o que interessa é que as pessoas votem e mais nada, que não pensem mais no assunto. De preferência que também não pensem antes para não tirem consequências. Portanto, quando um mecanismo é feito para o imediatismo, obviamente que grande parte das pessoas a tende a guiar-se por esses padrões. Agora, há condições para pôr em causa esse modelo em Portugal? Há condições para pôr em causa esse modelo na Europa? Há condições para pôr em causa esse modelo no mundo?

Eu, modestamente, com outro chapéu – agora não estou com esse chapéu – tenho tentado, também, encorajar isso, mas, sem grande sucesso, devo dizer. Pelo contrário, era mais fácil, antes do 25 de Abril, encorajar a cidadania do que hoje. Porque, na altura, havia inimigos. Era como a situação geoestratégica: quando há um inimigo determinado é muito fácil saber porque se luta. Devia lutar-se para abolir um conjunto de regras em Portugal que eram, no mínimo, obsoletas e injustas. Agora não há uma posição. Há um aliciamento através da publicidade e através desses valores. É difícil combater as mensagens televisivas ou as mensagens publicitárias. É um problema muito mais fundo. Por isso não me compete a mim. Só tenho que lhe agradecer por ter ajudado a levantar a questão.

Extravasava também um bocadinho agora. Eu penso que um papel significativo que a Comissão poderia ter, para além das questões que tem ajudado a resolver de uma forma correcta, era tentar identificar quem é que poderia desenvolver também uma acção pedagógica. Porque eu acho que as pessoas ganham mais do que essas garantias formalísticas.

É necessário que as pessoas saibam quais são os seus direitos e, por outro lado, como é que se podem defender. Porque a maior parte do fornecimento de dados é feito pelas as próprias pessoas que querem fornecer tais informações para terem acesso a determinados serviços. Portanto, os cidadãos devem ser informados – e não devia ser em letra miúda – do que é que isso representa para, depois, puderem fazer as suas opções. Está no seu direito, não é!! Tenho a impressão que alguém devia fazer isso. Não sei se tal função pedagógica cabe à Unidade de Missão ou à Comissão Nacional de Protecção de Dados, mas deveriam criar-se mecanismos para que as pessoas possam ter acesso a determinados benefícios, cedendo informações com conhecimento de todas as implicações.

Moderador

Eu queria fazer um comentário já que também a Comissão foi visada, com algumas questões. Começaria por esta última questão da informação.

Naturalmente que a Comissão gostaria muito que os órgãos da comunicação social informassem sobre o nosso papel. Mas, como devem saber, normalmente, os órgãos de comunicação social, quando se dirigem a nós, o que querem é casos. Portanto, quando nós falamos dos direitos dos cidadãos e dos aspectos da legalização dos tratamentos tais matérias ficam à margem. Podemos fazer uma referência, mas, normalmente no registo das entrevistas e declarações não passa este tipo de referências.

Possivelmente, também teríamos que caminhar para a publicitação paga como fazem colegas de outras comissões. Mas não temos orçamento para isso. Sendo uma autoridade pública independente e estamos também condicio-

I PAINEL

nados pela situação orçamental. O orçamento limita muitas vezes o tipo de actividade que se desempenha, como é evidente.

João Salgueiro

Associação Portuguesa de Bancos

Eu talvez lhe pedisse um segundo para dar uma sugestão. É que na próxima realização ponham a claro, antecipadamente, os conflitos internos que têm, dentro da comunicação. E que o Dr. Luís Silveira anuncie que vai revelar todo o conhecimento que tem desta realidade.

Moderador

Exactamente. É uma solução.

Relativamente à questão que o Dr. Garcia Pereira levanta ao dizer que o direito não tem feito uma reflexão sobre estas matérias é a pura realidade. É conflagrador como é que, em Portugal, ninguém escreve sobre protecção de dados. Pouca gente escreve e relativamente a iniciativas legislativas a Comissão tem sido uma vítima dessa situação. No dia-a-dia vemo-nos confrontados com a necessidade de actuar em inúmeras áreas.

Somos nós quem tem de regular os aspectos da biometria porque não há legislação sobre isso. Na videovigilância foi um drama. A declaração de inconstitucionalidade do decreto-lei, por parte do Tribunal Constitucional, foi um drama para nós que tivemos de arranjar uma solução. Por vezes temos de fazer de "legislador" e eu costumo dizer, e os meus colegas acompanham-me nisso, que nós não somos a Assembleia da República.

Quanto à videovigilância, a biometria, as questões da Internet e do e-mail no local de trabalho colocámos na nossa página da Internet as reflexões que fizemos sobre essas matérias. Na questão do Código de Trabalho levantámos duras críticas relativamente a algumas disposições. Não se foi tão longe quanto

se devia ir na regulação e, portanto, agora, a Comissão vê-se confrontada com essas situações.

Ainda na semana passada discutimos um assunto que tem a ver com gravações de serviços de atendimento numa empresa. Trata-se de gravações de chamadas, com vista a eventual controlo, em certa medida, dos trabalhadores. Põe-se a questão de saber se há controlo ou não. São questões muito complexas que o Código de Trabalho não resolve e a que nós, confrontados no dia-a-dia com esses problemas, temos que dar uma solução. E por isso, às vezes, tardam as soluções da Comissão.

Para dar uma decisão sobre biometria, por exemplo, ninguém faz ideia do que é que isso implica. Temos que estudar a componente técnica, as questões da codificação de uma impressão digital. Apurar se permite reversão ou não. Que consequências é que isso tem. Se a entidade empregadora fica com os perfis da nossa impressão digital ou apenas com o algoritmo codificado. São questões que nós juristas – temos uma pessoa que não é jurista na Comissão – temos sempre alguma dificuldade em equacionar, mas cumpre-nos debatê-las.

Deparamo-nos com questões tão complexas como, por exemplo, o tratamento do dado raça na área da saúde. A Comissão, por exemplo, pediu à Ordem dos Médicos um parecer sobre essa matéria e, até hoje, já lá vão cerca de cinco ou seis anos, estamos à espera do parecer. Contudo, acho que a Ordem dos Médicos era a entidade que devia ajudar nessa matéria para nos dizer em que medida é que o dado raça é fundamental para algumas patologias. Mas somos nós, que não somos médicos, quem tem de arranjar soluções no sentido de protegermos eventuais futuras discriminações. Não nos parece que, neste momento, haja discriminação de pessoas em função da raça nos hospitais. Não me parece, mas temos que prevenir o futuro e, portanto, se a informação não é necessária, não pode ser tratada.

Pergunta o Dr. Garcia Pereira que posição adoptar? Regular? Deixar andar? Ceder? Bom, a única coisa que eu posso dizer é que a Comissão Nacional de Protecção de Dados não tem cedido e temos sido acusados por causa disso.

Mesmo a nível de empresas multinacionais somos muitas vezes confrontados com o facto da nossa rigidez relativamente a colegas de outras comissões.

I PAINEL

Mas nós não nos importamos com isso. Estamos a cumprir a nossa missão, em obediência ao princípio da legalidade, e, portanto, é isso que nos preocupa a toda a hora.

No que diz respeito ao aspecto da facturação telefónica, a Comissão desconhece que isso aconteça. Isso é um tratamento, como é óbvio, passível de queixa, para a Comissão. Portanto, se isso acontecer, naturalmente que têm que ser compatibilizados, o direito da entidade empregadora, que paga o telefone, com os direitos dos trabalhadores, que utilizam o telefone, e, como é óbvio têm que ser definidas à partidas regras claras. Essas regras têm de respeitar os princípios do Código de Trabalho e da Lei de Protecção de Dados.

Uma última questão relativamente ao cartão de saúde. A única coisa que posso dizer é que a Comissão, neste momento, está a apreciar um projecto de decreto-lei do governo sobre o cartão de saúde. Chegou há pouco tempo. Não posso dizer quais as perspectivas futuras no cartão. Por acaso sou o relator do processo e, portanto, ainda não o li, não posso dizer, não sei o que lá está.

Posso dizer, no entanto, que a Comissão sempre defendeu que devia haver um cartão de saúde que identifique univocamente o cidadão. Para evitar que haja dez milhões de cidadãos e, eventualmente, doze milhões de cartões. Admitimos, com regras de segurança, que o cartão de saúde tenha alguma informação de saúde. Já o defendemos. Aliás, fomos acusados, por algumas entidades, de não autorizarmos que o cartão de saúde tivesse dados de saúde. Para mim foi uma surpresa porque fui eu o relator desses pareceres quando me disseram que não havia dados de saúde no cartão por causa da Comissão.

Posso-lhes dizer que, o que aconteceu foi que, na altura, para ter dados de saúde era necessário um *chip* – o cartão actual tem uma banda magnética e, os dados de saúde, obviamente, não cabiam nessa banda – e o *chip*, naquela altura, era extremamente caro para o Ministério da Saúde. Portanto, foi isso que aconteceu, como é óbvio. A Comissão obviamente que é favorável, desde que haja regras de segurança que impeçam que qualquer pessoa possa ter acesso ao cartão. A questão económica é mais complexa e a Comissão a seu tempo dará a sua opinião.

Diogo Vasconcelos

UMIC

Eu gostaria de sugerir à Comissão que trabalhássemos em conjunto no sentido de divulgar as questões da privacidade relacionadas com a sociedade de informação e com a utilização das tecnologias de informação.

Por um lado, para criar consciência dos direitos, na generalidade das pessoas, na opinião pública. E, por outro lado, para criar consciência das regras e dos deveres por parte das entidades, quer do sector público, quer do sector privado.

Estamos totalmente disponíveis para trabalhar com a Comissão na criação dessa consciência sobre as questões da privacidade, numa altura em que elas ganham nova acutilância com a utilização crescente das tecnologias de informação e as possibilidades de desmaterialização de informação sobre pessoas. É uma sugestão e um desafio que ficam aqui lançados à Comissão.

Da nossa parte há toda a disponibilidade para trabalhar em conjunto porque nos parece importante que, por um lado, sejam preservados os direitos individuais e que, por outro lado, não sejam prejudicados, por ignorância ou inépcia, os desenvolvimentos que é preciso fazer para transformar a economia numa economia cada vez mais digital.

João Salgueiro

Associação Portuguesa de Bancos

Eu não sei se lhes será possível, mas acho que deviam tentar num projecto que contribuísse para que os direitos dos cidadãos fossem mais salvaguardados em termos gerais.

Os direitos dos cidadãos são completamente atropelados quando os prazos legais não são cumpridos. As entidades públicas, por sistema, são useiras e vezeiras nisso. Desde as autarquias à administração da justiça, nos impostos. Este ano no Orçamento está, outra vez, a prolongar o prazo que a administração pública tem para não cumprir a lei.

I PAINEL

Portanto, eu acho que os cidadãos ganhavam muito se fosse possível haver um projecto – polémico ou não, mas era preciso começar a andar – para que ficassem registados os incumprimentos do estado.

Moderador

Uma base de dados de incumprimentos do estado não seria controlada pela Comissão, porque, possivelmente, não comportaria dados pessoais, a menos que identificasse os responsáveis da administração pública por esses incumprimentos. Aí já seria mais complicado, naturalmente.

João Salgueiro

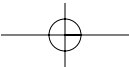
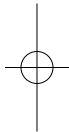
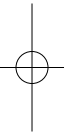
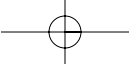
Associação Portuguesa de Meios

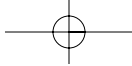
Talvez pudéssemos dispensar os dados biométricos dos responsáveis.

Moderador

Resta-me agradecer a todos, em particular aos oradores que aqui estiveram, e, também, ao público que assistiu à nossa conferência. Terminámos na hora prevista dada a vossa colaboração. Fico muito contente por isso.

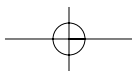
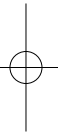
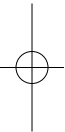
Obrigado.

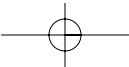
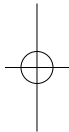
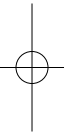
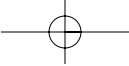




II PAINEL

Segurança e Privacidade: ponderação de interesses





Alexandre Pinheiro

Vogal da CNPD

A VIDEOVIGILÂNCIA E A PROTECÇÃO DE DADOS PESSOAIS

Na comemoração do 10.º aniversário da Comissão Nacional de Protecção de Dados, o propósito desta intervenção consiste em analisar o quadro legal e constitucional em que se desenvolve o tema da videovigilância. Trata-se de uma matéria já clássica no domínio da protecção de dados pessoais que tem justificado uma actividade profícua das autoridades nacionais de protecção de dados, de tribunais, de instâncias comunitárias e de organizações internacionais.

Importa notar que a videovigilância pode assumir-se como um mecanismo de fiscalização absoluta, dos passos de um cidadão. Portanto, como um sistema, através do qual é possível, saber tudo o que alguém faz dentro de um determinado espaço. E, nesse sentido, a videovigilância é demonizada e entendida como elemento nocivo às liberdades individuais. Portanto, aí, traz-nos à memória utopias negativas, nomeadamente, de carácter orweliano – pensamos no *Big Brother*. Através de romances e de exemplos de ficção disseminou-se a ideia de um possível controlo máximo sobre a existência individual e da sua natureza repressora.

Porém, outros exemplos demonstram a natureza positiva e bem sucedida da videovigilância. Assim, regista-se a prevenção da prática de crimes, de afoga-

mentos, evitar que alguém se precipite sobre obstáculo físico que não possa transpor. Portanto, é bom vermos a videovigilância, antes de mais, como uma fonte de informação e não necessariamente com um malefício.

A captação de som e imagem é subsumível à lei 67/98 de 26 de Outubro, nos termos expressos no art.º 4.º, n.º 4. Esta referência expressa dissipa quaisquer dúvidas sobre a aplicação da lei de protecção de dados relativamente ao tema da videovigilância. Assim, a citada lei inclui uma definição sobre dados pessoais, através da qual todas as informações de qualquer natureza e independentemente do suporte, *incluindo som e imagem*. Mais, se diz que é considerada identificada ou identificável a pessoa que possa saber-se quem é directa ou indirectamente (se for possível a identificação de um elemento, através do qual, seja identificável uma pessoa, uma matrícula, por exemplo, estamos a falar, obviamente, de videovigilância relevante para efeitos de aplicação da Lei 67/98). Relativamente ao conceito de tratamento de dados pessoais, este abrange todo o tipo de operações que vão desde a recolha até a uma eventual transmissão. Não existem, portanto, dúvidas de que a videovigilância é um dos sectores integrado no domínio dos dados pessoais.

Portanto, começando pelo quadro constitucional, pelo artigo 35.º, consideremos algumas das matérias que estão relacionadas com a videovigilância.

Importa tomar em consideração algumas das decisões fundamentais adoptadas no ordenamento jurídico sobre a videovigilância, começando com a posição do Tribunal Constitucional. Numa decisão basilar em sede de direitos, liberdades e garantias, o Tribunal considerou que *a permissão da utilização dos referidos equipamentos constitui uma limitação ou uma restrição do direito à reserva da intimidade da vida privada, consignado no artigo 26.º, n.º 1, da Lei Fundamental*. Afirmou, igualmente, que *ao autorizar a videovigilância e ao estabelecer algumas regras a que ela deve obedecer, o legislador está indiscutivelmente a tratar de uma matéria atinente a direitos, liberdades e garantias* (Acórdão n.º 255/02).

É certo que nesta decisão, o Tribunal não se pronunciou sobre elementos materiais do problema da videovigilância, mas clarificou, de forma hoje não refu-

II PAINEL

tável no ordenamento português de matéria de direitos, liberdades e garantias, sujeita, nomeadamente, à reserva de competência legislativa da Assembleia da República. Estava em causa a compatibilidade com a Constituição de algumas normas do Decreto-Lei n.º 231/98, de 22 de Julho que permitiam a adopção de sistemas de videovigilância no âmbito do exercício da actividade de segurança privada, os quais podiam estar a cargo de empresas privadas ou de serviços de “autoprotecção com vista à protecção de pessoas e bens, bem como à prevenção da prática de crimes”. O mesmo diploma determinou a obrigatoriedade de adopção destes sistemas para o Banco de Portugal, instituições de crédito e sociedades financeiras e para estabelecimentos de restauração e bebidas que disponham de salas destinadas a dança.

A jurisprudência do Tribunal Constitucional considerou que estando envolvidos sistemas de videovigilância estariam em causa restrições de direitos, liberdades e garantias – por exemplo direito à imagem, liberdade de movimentos, direito à reserva da vida privada – a lei deveria especificar se e em que medida estes sistemas poderão ser utilizados e, especialmente, assegurar, numa situação de conflito de direitos fundamentais, que as restrições se limitem “ao necessário para salvaguardar outros direitos ou interesses fundamentais”.

Dentro dos dados pessoais, concluindo nós que se trata de um dado pessoal, a videovigilância integra-se no conjunto dos dados sensíveis (artigo 35.º, n.º 3 da CRP e artigo 7.º, n.º 1 da Lei n.º 67/98). A associação das imagens recolhidas por estes processos ao bem jurídico protecção da vida privada foi enfatizada pela decisão do Tribunal. Antes já era entendido, já era tratado, de alguma forma, pela Comissão Nacional de Protecção de Dados e por autores que, sobre o tema se tinham debruçado, um dado sensível.

Assim, por força da aplicação da lei de protecção de dados, os responsáveis pelo tratamento de imagem e som estão obrigados, em particular, a notificar estes tratamentos à CNPD, a observar os princípios relativos à qualidade dos dados, a respeitar as “condições de legitimidade” e de licitude para poderem tratar esses dados e a assegurar o direito de informação. Os dados devem ser conservados por prazos limitados, cabendo à CNPD fixar o prazo de conser-

vação em função da finalidade. O Decreto-Lei n.º 35/2004, que regula o exercício da actividade de segurança privada determina, no seu artigo 13.º n.º 4, a aplicação subsidiária da Lei 67/98, designadamente em sede de “direito de acesso à informação, oposição aos tratamentos e regime sancionatório.”

É importante notar, também, que existe alguma pulverização legislativa na matéria da videovigilância. Além da lei de protecção de dados e da legislação sobre segurança privada, importa considerar o artigo 20.º do Código do Trabalho. Também se deve admitir, no mesmo contexto, a utilização destes sistemas para controlo de postos de trabalho que apresentem especiais riscos para os trabalhadores, quer pela sua especial perigosidade em relação ao contacto com certas substâncias perigosas, quer pela inacessibilidade ou especial solidão em que os trabalhadores exercem a sua actividade (por exemplo, minas, centrais nucleares, laboratórios em que se trabalhe com produtos químicos perigosos).

De acordo com a interpretação que fazemos do artigo 20.º, as câmaras não podem ser utilizadas para avaliar o desempenho do trabalhador. Por exemplo, considerou-se que, num salão de cabeleireiros, em que havia duas câmaras: uma câmara apontada para a zona de pagamentos e da caixa; e uma câmara apontada para o local onde se efectua a actividade profissional, considerou-se que a instalação desta se traduzia num tratamento excessivo e intrusivo.

Podem citar-se, também, como situações em que a videovigilância é permitida:

- A Lei n.º 38/98, de 4 de Agosto, que obrigou os organizadores de competições desportivas a dotarem os seus recintos de sistemas de videovigilância;
- O Decreto-Lei n.º 139/2002, de 17 de Maio, que obriga os estabelecimentos de fabrico e armazenagem de produtos explosivos a “estarem protegidos por um sistema de vigilância permanente que assegure a detecção de intrusos”, admitindo que uma das opções de controlo possa passar pela adopção de um “sistema de videovigilância instalado nos termos da lei geral” (artigo 22.º n.º 2 e 3 alínea b).

II PAINEL

As condições de legitimidade exigidas para esta espécie de tratamentos podem constar de “interesses vitais dos titulares”, ou para “declaração, exercício ou defesa de um direito em processo judicial”.

Estes tratamentos só são legítimos se se apresentarem necessários à execução de finalidades legítimas do seu responsável e desde que “não prevaleçam os direitos, liberdades e garantias do titular dos dados” (artigo 8.º n.º 2 da Lei 67/98). É ainda necessário, como resulta do preceito acabado de citar, que este tratamento seja autorizado pela CNPD, que verificará se foram observadas as normas de protecção de dados e de segurança da informação.

No domínio da pertinência, a CNPD tem considerado os seguintes aspectos:

- a) Definição da localização das câmaras e as modalidades de registo (registo e conservação das imagens, ângulos utilizados, escolha de “grandes planos”);
- b) Redução do campo visual em função da finalidade prosseguida ou das zonas em que “a videovigilância é efectivamente necessária, dando uma atenção particular aos casos em que as câmaras – filmando lugares públicos – permitem o registo de som e imagem em lugares privados situados na proximidade”;
- c) Recolha de imagens no estritamente necessário à finalidade prosseguida, sendo dispensáveis grandes planos ou detalhes não relevantes em função dos objectivos a que se propõe o responsável.

Como princípios fundamentais fundamentadores destes tratamentos e definidores dos seus limites apresentam-se os seguintes:

- a) O *princípio da necessidade* – O tratamento é permitido quando a finalidade não puder ser alcançada por qualquer outro meio igualmente eficaz, mas menos intrusivo para o cidadão;
- b) *Princípio da proporcionalidade* – O interesse legítimo do responsável deve prevalecer sobre os direitos e interesses do indivíduo a que dizem respeito, desde que os seus direitos fundamentais não sejam violados.
- c) Os dados recolhidos por câmaras de videovigilância devem ser adequados, pertinentes e não excessivos em relação à finalidade para a qual são

usados. Portanto, os locais onde as câmaras fixas de vídeo devem ser instaladas, bem como a forma de gravação, deve ser de maneira a que não seja gravada mais informação da que for necessária para a finalidade.

De uma forma geral, os pedidos de notificação tem como finalidade assegurar a “*protecção de pessoas e bens*”, tendo como propósito a utilização das imagens como prova das infracções criminais praticadas, em observância das disposições processuais penais. Estando em causa a prevenção de crimes, segundo a CNPD, o fundamento de legitimidade poderá ser encontrado no artigo 8.º n.º 2 da Lei 67/98, de 26 de Outubro.

Muito embora o artigo 8.º n.º 2 se refira ao tratamento relativo a “*suspeitas de actividades ilícitas, infracções penais, contra-ordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias*”, pode considerar-se que o preceito está, também, vocacionado para a recolha e tratamento de informação no contexto da *prevenção criminal*. Assim, para além de estar em causa, objectivamente, a *prevenção e dissuasão da prática de actos ilícitos* – tarefa que é desempenhada na prossecução do interesse público, em complementaridade e subsidiariedade face às competências das forças e serviços de segurança – a informação recolhida pode vir a ser utilizada como prova da infracção.

Está em causa nestes casos a utilização da videovigilância para assegurar a *dissuasão, sempre com o conhecimento das pessoas e com protecção dos seus direitos fundamentais*, bem como para registar e documentar a eventual prática de infracções. O tratamento de som ou imagem verifica-se, desta forma, a montante da eventual actividade delitual.

É importante frisar que o facto de as imagens serem recolhidas em lugares públicos e os titulares dos dados serem previamente informados da existência de tratamento e das suas finalidades contribui, substancialmente, para afastar a ideia de que existe uma captação ou utilização arbitrária da sua imagem. A sua utilização só pode dar-se com finalidades penais ou de processo penal.

No que tange ao acesso ao material recolhido através destas câmaras, existem, também, princípios que devem ser respeitados. Não há qualquer justificação

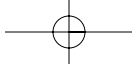
II PAINEL

para a visualização das imagens por parte das entidades responsáveis por duas ordens de fundamentos:

- a) Caso não tenha sido praticada qualquer infracção penal ou procedimento que atente contra as pessoas e bens, a visualização de imagens não tem qualquer sentido útil, sob pena de violação do disposto no artigo 5.º n.º 1 alínea b) da Lei 67/98, de 26 de Outubro;
- b) Caso tenha sido praticada infracção penal as imagens devem, necessariamente, ser canalizadas para a autoridade competente.

Para terminar, pode ilustrar-se o que tem sido exposto através de um caso concreto respeitante à decisão adoptada pela CNPD quanto às câmaras instaladas no Parque Nacional da Arrábida e que, abrangiam, como é óbvio, um espaço público, por vezes com construção de habitações próprias, e até o perímetro urbano de algumas localidades. Levantava-se o problema de saber como compatibilizar o direito à intimidade da vida privada, portanto, o interesse privado do frequentador do parque, ou de quem que vivesse numa zona abrangida pelas câmaras, e o interesse público da protecção contra incêndios. Entendeu-se o seguinte: (i) existe um interesse público que justifica uma limitação do direito individual à protecção da vida privada; (ii) pode, portanto, haver um sistema de câmaras, no parque; (iii) não se justifica que seja, completamente ignorado o direito à reserva privada de habitantes e frequentadores. Desta forma, teve que definir-se uma solução equilibrada baseada no seguinte: (i) permitiu-se a instalação de câmaras de videovigilância; (ii) quando se esteja em face de zonas habitacionais o ecrã de quem estiver a proceder à fiscalização deve ficar obscurecido; (iii) concluiu-se não fazer sentido que com a finalidade de impedir fogos se penetrasse na casa e na intimidade de outras pessoas; (iv) houve o estabelecimento daquilo que tecnicamente se designa como *blank zones*; (v) a CNPD decidiu, também, que é possível recolher a imagem do que pode estar a acontecer no Parque sem identificar os intervenientes adoptando-se uma metodologia de desfocagem.

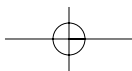
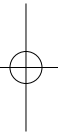
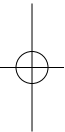
Estamos perante a aplicação do princípio da proporcionalidade que implica, em cada caso concreto, a idoneidade do meio utilizado – a videovigilância – bem como, e também, o respeito pelo princípio da intervenção mínima.



COLÓQUIO PROTEGER OS DADOS PESSOAIS

O princípio da intervenção mínima obriga, necessariamente, que, em cada caso concreto, se pondere entre a finalidade pretendida e a necessária violação de direitos fundamentais, aqui concretamente o direito à privacidade e à imagem.

Assim termino. Muito obrigado.



II PAINEL

Carlos Cabreiro

Brigada da Criminalidade Informática da Polícia Judiciária

A INVESTIGAÇÃO POLICIAL E O COMBATE AO CIBERCRIME

Antes de mais, muito boa tarde.

À pessoa do Dr. Luís Silveira, presidente da Comissão Nacional de Protecção de Dados, pelo convite que foi formulado à Polícia Judiciária, para estar aqui presente, o meu obrigado.

Permitam-me a utilização desta barricada e desta muleta do PowerPoint. Pertencendo à secção de criminalidade informática, dificilmente me consigo livrar desta muleta.

Irei falar pouco, e já que a dicotomia e a ponderação que nos é solicitada, neste tema, irei optar pela segurança. Sou polícia e irei falar pelos interesses que existem na investigação. Com um levantamento muito genérico sobre as dificuldades de prova em ambiente digital. Com a abordagem de um tema que, por sorte, hoje é muito actual. Porque está a ser discutido, ao que sei, no Conselho de Ministros uma proposta de lei relacionada com a obtenção de prova digital. Iremos falar, em concreto, do que deveremos fazer e qual o entendimento da Polícia Judiciária, relativamente aos dados dos operadores de telecomunicações.

Antes de mais, iria começar, então, por estas dificuldades genéricas da investigação criminal. Considerando as características da prova e, tendo ela que ser

admissível, autêntica, precisa e completa, à Polícia Judiciária e, também aos tribunais ou à investigação, coloca-se, afinal, esta grande questão: como lidar com prova que assume um carácter tão temporário, fungível e de grande volatilidade? Outras questões, mais complicadas ainda, que a informática nos coloca têm a ver com questões relacionadas com a incriptação, a recuperação do e-mail, as características do e-mail, as características do correio, o que é a correspondência e o que é o circuito de comunicação que permite a nossa comunicação por e-mail. Problemas relacionados com a simples recuperação de ficheiros, que nós pensamos, ou eles pensam que têm apagados e que, eventualmente, podemos vir a recuperar.

A possibilidade de eu ter um local autorizado para realizar uma determinada busca e aperceber-me, no momento, que essa informação, afinal, não está naquele local, mas, através de uma comunicação de PC's remotos, num outro local eliminado a possibilidade urgente de a aceder directamente.

Acresce sempre, algo que é normal falar em seminários e conferências, tem a ver com a cooperação. Cooperação é, normalmente, o tema de encerramento de todas as intervenções. Diz-se sempre que a cooperação, além de internacional, tem que ser interna. Porque, afinal, antes de falarmos com os outros países, temos que falar cá dentro, porque nós não nos entendemos muito bem com os operadores, não nos entendemos muito bem, na definição que temos sobre determinados conceitos.

Desde que estou na Polícia Judiciária a questão da cooperação é essencial, mas, no entanto, pouco se tem avançado nessa matéria. É a minha opinião.

A Internet veio aqui baralhar um pouco as contas desta questão relacionada com a prova informática, complicar os problemas com os dados que podem circular livremente.

A Internet é já um meio desvirtuado, na nossa opinião, e preferencial de comunicação. Porque primeiro que nós chegou a este tipo de comunicações vital quem a utiliza para a prática criminal. É, por isso, um instrumento privilegiado das redes organizadas, para a prática de crimes, armas, drogas, terrorismo, branqueamento. A exploração sexual de crianças é apetecível para a

II PAINEL

utilização deste meio poderoso de comunicação. A Internet tornou-se, por isso, um palco preferencial para estas práticas.

Queria começar por alguns exemplos relacionados com a nossa actividade. Vão perceber qual o interesse dos dados dos operadores de comunicações. Eu não irei referir todas estas interrogações, mas são situações que, de alguma forma, se nos colocam no dia-a-dia. Algumas reportadas a situações reais e que até podem ser do conhecimento público. Irão perceber a necessidade de possuímos tudo o que são dados dos operadores de telecomunicações.

Nesta cooperação interna que tem de existir entre os operadores e a justiça, mas com a necessidade de definição clara do que é que os operadores podem, devem preservar, e dar às autoridades, sejam elas policiais ou judiciárias. Perante estas situações que aqui vêem, estamos a falar, tão só, de uma primeira necessidade em termos de investigação. Que é a obtenção dos dados, que estiveram na base da comunicação que só aos operadores diz respeito e que só eles possuem.

Estamos a falar, por isso, acerca de dados gerados numa comunicação em rede ou sistema informático, por exemplo, a Internet. São dados que estão, obrigatoriamente, na posse dos operadores. Constituem, em muitos casos, a peça única e, quando não única, a primeira peça para que se comece a investigar um caso relacionado em que intervenham estas novas tecnologias e que envolva os dados provenientes dos operadores de comunicações.

Posso-vos dizer que cerca de 20% dos casos da SICIT – SICIT é a Secção de Investigação de Crime Informático – estão a ser concluídos por não possuímos, ou por os operadores não poderem fornecer, os elementos relacionados com aquela prática criminosa e que, eventualmente, nos poderiam levar ao local – e atenção que não estou a falar de autor – da prática do crime.

Dentro da perspectiva da proposta de legislação, em que a Polícia Judiciária colaborou, interessa, por isso, na nossa opinião, saber que tipo de dados e quais os vários tipos de dados de que estamos a falar. Saber qual a sua natureza, quem pode aceder e quem pode fornecer tais dados. Encaro, também, uma previsão de imposições de regras para os operadores na preservação destes

dados; inexistente de momento. Acrescento a imposição de alguma regra relativa aos denominados fornecedores de serviços de acesso às redes de comunicações.

Decifro-vos já esta quarta hipótese. E, pensem, tão só, num cibercafé. Neste momento pode estar a ser utilizado por qualquer pessoa para a prática de um crime sem que surja a hipótese da sua identificação. E não estamos a falar de coisa diferente, de, por exemplo, uma biblioteca, ou de um hotel, onde entro e tenho a obrigação de me identificar.

Quanto à tipologia – e, apesar da grande proliferação de conceitos nesta área – tivemos em conta os vários conceitos que existem em instrumentos internacionais, em instrumentos nacionais e no entendimento que existe ao nível das operadoras de comunicações. Considero uma subdivisão de dados das operadoras de comunicações – e já vão ver o porquê – em dados de localização, em dados de tráfego, em dados de base e em dados de localização.

Dados de tráfego, digamos em termos gerais, são os dados, eminentemente técnicos, relacionados com uma comunicação. Que nos dá, entendam, a origem, o destino e indicam se, pelo meio, houve algum reencaminhamento de uma comunicação. Quando estou a falar de origem, não estou a falar de pessoas, estou a falar, eventualmente, de uma morada.

Refiro, eventualmente, um IP. São dados meramente técnicos que não identificam pessoas e que, por isso, na nossa opinião, não bulem, não mexem com a privacidade das pessoas.

Numa definição um pouco mais completa, baseada em algumas recomendações do Conselho da Europa, os dados de tráfego assumem esta definição. Quanto aos dados de localização devido às novas tecnologias – redes *wireless*, sem fios – torna-se premente falar, também deles.

Neste momento, no cômputo de práticas de crime – peço desculpa pela insistência de só estar a referir a parte da segurança – é tão usual alguém praticar um delito dentro de uma viatura estacionada junto à praça Marquês de Pombal como junto da sua residência desde que o instrumento utilizado seja, por exemplo, um computador com acesso à Internet. Eu tanto posso divulgar foto-

II PAINEL

grafias de pornografia infantil na residência, dentro de um carro, num autocarro, utilizando redes *wireless* que, neste momento, começam a proliferar. Daí, a necessidade, também, de fazer esta distinção entre dados de localização.

Este tipo de dados é vulgar associarem-se às intercepções telefónicas. Os operadores sabem isso porque há eventual possibilidade de localizar o equipamento. Mas teremos que estender isto não só à intercepção telefónica, mas também à utilização de um simples portátil que, neste caso, não está ligado por rede sem fios, mas que é possível a alguém localizar aqui neste salão, na fundação Calouste Gulbenkian.

Dados de base são os dados que toda a gente conhece, quando as pessoas não optam pela confidencialidade. Os dados de base, serão os dados constantes da lista telefónica, quando as pessoas decidem não utilizar o regime da confidencialidade. No entanto, nesta ponderação de interesses entre privacidade e segurança, deve associar-se, também, a facturação detalhada. A facturação detalhada nunca deverá ser de acesso directo, excepto mediante solicitação da autoridade judiciária.

Dados de conteúdo são os dados relativos ao conteúdo de uma comunicação que associamos directamente à equiparação que é feita às intercepções telefónicas. Terá que seguir, necessariamente, o mesmo regime.

Razões para este escalonamento? Vimos que dados de tráfego, dados de localização, são elementos meramente técnicos. A sua identificação proporciona a informação do local e dos elementos, diria, algoritmos, de uma comunicação. Não estamos a falar de localização, não estamos a falar ainda de número de telefone. Referimos um dado, por exemplo, ao nível da Internet, estamos a falar de um IP. Estamos a falar do percurso que essa comunicação percorreu. Eventualmente, um servidor em Portugal, com a utilização de um servidor na América e que, depois regressou a Portugal é o rasto de um possível crime. Estamos a falar do local do delito, cuja identificação é essencial à investigação.

Quanto ao regime de acesso aos dados de tráfego e localização e, com base no que referi, considero puderem ser solicitados directamente pelas autori-

dades de polícia criminal ou autoridades judiciárias. Os operadores devem facultar este tipo de informação, sempre que solicitado e sempre que estejam obrigados a preservá-los. Presentemente, os operadores não têm o dever de preservação deste tipo de dados para além do período normal de facturação, ou, em casos excepcionais, para efeitos de investigação.

Ora, alguém tem definir se, de facto, tais dados serão necessários à investigação. Quanto aos dados de base, como referi, se estão sujeitos ao regime da confidencialidade, naturalmente que só através da autoridade judiciária se poderá aceder a este tipo de elementos.

Situação diferente acontece se estes dados de base – o nome, a morada – forem públicos. Porque as pessoas podem optar pela confidencialidade de determinados números nas listas telefónicas nacionais em que se associa o nome, a morada e o número. Se estiverem sujeitos ao regime da confidencialidade, isso sim, terá que fazer intervir a autoridade judiciária. Vale o mesmo em relação à facturação detalhada. E porque é que, embora sendo dados de base, nós consideramos que devem ser solicitados pela autoridade judiciária?

Porque, primeiro, indevidamente na minha opinião, se lhe chama facturação detalhada quando se reduz, de facto, a uma lista discriminativa de chamadas efectuadas e recebidas. Se fosse só facturação referencial que a chamada X ou Y, custou X e custou Z. Tal listagem, além da facturação, permite a interligação de dados que são, além dos meus e do meu número de telefone, indicativos de quem ligou para quem, de para onde é que eu liguei. E vêm identificados os números. Daí, que consideremos que, nestes moldes, esta informação só pode ser solicitada pela autoridade judiciária.

Quanto aos dados de conteúdo, julgo que não existe dúvida se deve fazer uma equiparação total ao regime das intercepções telefónicas. Porque estamos, apenas, a falar de um diferente meio de comunicação, cujo conteúdo tem que ser protegido. A própria extensão do art.º 190 ao correio electrónico é já o seu reflexo. A nova proposta de revisão do Código do Processo Penal, refere até que o disposto nos artigos 187, 88 e 89 seja aplicado às conversações ou comunicações transmitidas por qualquer meio técnico, diferente do telefone.

II PAINEL

Uma questão terá de ser resolvida. Os operadores devem preservar e por quanto tempo este tipo de dados? Não está claro para os operadores que devem preservar este tipo de dados. Eventualmente, até podem vir a incorrer na prática de ilegalidades, quando os tenham preservado, ou quando os não tenham preservado, durante o período de facturação.

Daí que a Polícia Judiciária defenda – e julgo que é esta a tendência de grande parte das legislações da Europa – que os operadores de comunicações sejam obrigados a conservar pelo período de um ano a informação relativa aos dados de localização, de tráfego e de base.

Os dados de base já são preservados porque é do interesse do operador ao terem índole meramente contratual e constarem do contrato. São dados que vivem e morrem durante a vigência de um contrato, com as constantes actualizações que podem ser efectuadas. Solicita-se, conseqüentemente, que os dados de tráfego e os dados de localização sejam preservados durante um ano. Actualmente os operadores estão isentos desta obrigação. Assiste-lhes o poder de preservar dados exclusivamente para o período de facturação.

Quais as razões para este prazo? Vou colocar uma hipótese muito simples. Num crime semi-público – e estamos a falar de quase todos os crimes, por exemplo, da área informática – as pessoas podem queixar-se num prazo de seis meses.

Imaginando que só se queixam ao sexto mês, com um período razoável de funcionamento das polícias e dos tribunais, vejam a impossibilidade, que pode ser criada à justiça, de investigar um caso que tenha por base e em que o único suporte consista neste tipo de dados. Acho que este exemplo é ilustrativo da necessidade deste prazo.

Falei há pouco destes fornecedores de serviços de acesso à rede de publicações e que, de facto, na nossa opinião, são uma parte branca e sem controlo. Sabendo eu, no entanto, que existem preocupações por parte de quem abra, por exemplo, um cibercafé, em saber que tipo de precauções é que pode tomar, para que os dados dos utilizadores – e reparem, nós já não estamos a falar aqui dos dados das comunicações, estamos a mencionar os dados dos

COLÓQUIO PROTEGER OS DADOS PESSOAIS

utilizadores – sendo indiferente, na nossa opinião, que aquilo seja um chamado livro de merceeiro, ou seja uma base de dados legalizada para o efeito. Daí que tenha que haver, na nossa opinião, alguma intervenção nesta matéria.

O que fazer? Mencionei casos reais de dificuldade extrema de investigação e, para outra oportunidade, deixarei a questão da ciberconvenção que pode vir a ser um instrumento legislativo importante, para a uniformização de legislações. Mas, o tempo urge e terminava por aqui.

Muito obrigado.

Amadeu Guerra

Vogal da CNPD

SISTEMAS DE INFORMAÇÃO POLICIAL – OS DIREITOS DOS CIDADÃOS

I. Introdução

O Dr. Carlos Cabreiro acabou de focar alguns aspectos relativos ao tratamento de informação policial que eu me propunha evidenciar. Por isso dispensar-me-ei de os abordar.

A Directiva Parlamento Europeu e do Conselho n.º 95/46/CE ⁽¹⁾ salienta que os sistemas de tratamento de dados devem “respeitar as liberdades e os direitos fundamentais das pessoas singulares e contribuir para o progresso económico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos” (ponto n.º 2 dos considerandos).

O documento estabelece, igualmente, os parâmetros uniformes de protecção das liberdades, dos direitos fundamentais e da vida privada, proibindo aos Estados-membros qualquer restrição à livre circulação de dados pessoais (cf. art. 1.º n.º 2). São permitidas “derrogações” aos Estados quando, nomeadamente, esteja em causa o tratamento de dados relativos à “segurança pública, à defesa, segurança do Estado e às actividades no domínio do direito penal” (art. 3.º n.º 2 e 13.º).

⁽¹⁾ Directiva de 24 de Outubro de 1995 (in JO n.º L281 de 23/11/95, pág. 31 e ss.).

Daí que, no âmbito do tratamento de informação policial, se note nos estados membros uma diversidade de regimes em que a cooperação policial, a recolha de informação de diversas fontes ou o tempo de conservação podem apresentar certas especialidades em função da sua cultura, da especificidade ou natureza de criminalidade que têm, bem como da definição das políticas de prevenção ou investigação criminal de cada estado.

A nova realidade criminal – onde assume particular realce o crime organizado e transnacional, com utilização de meios sofisticados de organização e comunicação – obriga os órgãos de polícia criminal e as autoridades judiciais a adoptar novas metodologias de investigação, de cooperação policial e formas mais expeditas e eficazes de obtenção de dados, que podem constituir meios de investigação e de prova decisivos.

Quem conhece os sistemas de informação policial pode constatar que houve uma evolução significativa nos últimos dez ou quinze anos em matéria de sistematização e tratamento automatizado de informação policial. Tenho a sensação, porém, que ainda há muito a fazer no domínio da disponibilidade de meios tecnológicos e de “circulação da informação” entre as várias polícias. Estas limitações podem decorrer, nomeadamente, de uma insuficiente abordagem legislativa em matéria de cooperação policial e troca de informação entre os vários “órgãos de polícia criminal”.

II. O direito à privacidade como direito fundamental

1. Para responder aos perigos evidenciados pelas novas tecnologias e pelo armazenamento massivo de informação, o nosso ordenamento adoptou medidas efectivas que visam impedir que o tratamento de dados pessoais possa afectar as liberdades e os direitos dos cidadãos, em especial a sua “vida privada”.

Dois preceitos da Constituição da República, integrados no título dos direitos, liberdades e garantias, devem ser evidenciados:

- a) O artigo 26.º n.º 1 estabelece que a todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à reserva da

II PAINEL

intimidade da vida privada e familiar e à protecção legal contra qualquer forma de discriminação. Acrescenta o número 2 que “a lei estabelecerá garantias efectivas contra a utilização abusiva, ou contrária à dignidade humana, de informações relativas às pessoas e famílias”. O n.º 3 atribui à lei o papel de garantir a “dignidade pessoal e a identidade genética do ser humano, nomeadamente na criação, desenvolvimento e utilização das tecnologias e experimentação científica”;

- b) O artigo 35.º⁽²⁾ consagra os direitos fundamentais em matéria de tratamento de dados pessoais. Começa por reconhecer a todos o direito de acesso, rectificação e o conhecimento sobre a finalidade a que se destinam os dados, cabendo à lei definir as suas condições (n.º 1). Atribui à lei, nos termos do n.º 2, a incumbência de definir o conceito de dados pessoais, as condições aplicáveis ao tratamento automatizado, bem como a sua transmissão e utilização. O n.º 3 refere que a informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação”.

2. Tal como os demais direitos fundamentais, o direito à privacidade face à informática não é absoluto. Em qualquer tratamento estão em causa:

1. Os interesses dos titulares dos dados (vg. prestação de cuidados de saúde, a transferência de um risco na celebração de um contrato de seguro ou o direito a não ver devassada a sua privacidade);
2. Outros interesses de carácter geral como sejam a participação na vida pública, o direito à saúde e à protecção da saúde pública, a preservação da segurança interna, a prevenção criminal e administração da justiça.

Isto é, o desenvolvimento da actividade económica e o estabelecimento de relações entre os particulares e o estado pressupõe, necessariamente, o tra-

⁽²⁾ De uma forma mais genérica, o artigo 18.º 4 da Constituição espanhola confere à lei a missão de delimitar o “uso da informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercício dos seus direitos”

tamento de dados pessoais e, em algumas situações, a compressão de alguns direitos como forma de compatibilizar interesses conflitantes.

Daí que a doutrina ⁽³⁾ saliente que:

- a) O princípio da proporcionalidade deve assumir um “papel muito importante no controlo da actuação policial”;
- b) A vida em sociedade implica “limitações aos direitos e liberdades individuais em nome do respeito aos direitos e liberdades dos outros” – o que fundamenta o direito de polícia – sendo certo que “estas restrições impostas pela actividade estatal de polícia também estão limitadas, para que não ocorram excessos ou abusos”;
- c) É necessário estabelecer, por via legislativa, um equilíbrio entre os interesses em presença;
- d) A própria Constituição – no seu artigo 272.º – estabelece que “as medidas de polícia não devem ser utilizadas para além do estritamente necessário” (n.º 2) e que “a prevenção de crimes...só pode fazer-se com observância das regras gerais sobre polícia e com respeito pelos direitos, liberdades e garantias dos cidadãos”.

III. O tratamento de dados policiais

1. Condições de legitimidade

1. O artigo 8.º n.º 2 e n.º 3 da Lei 67/98, de 26 de Outubro, estabelece as condições de legitimidade dos tratamentos.

O tratamento de dados policiais obedece à verificação dos seguintes requisitos cumulativos:

- a) Os tratamentos devem apresentar-se como necessários à execução de finalidades legítimas dos responsáveis;

⁽³⁾ Lúcia Maria de Figueiredo Ferraz Pereira Leite – “O princípio da proporcionalidade nas medidas de polícia” in “Estudos de Direito de Polícia”, Vol. I, 2003, pág. 363.

II PAINEL

- b) Devem limitar-se ao necessário para prevenção de um perigo concreto ou repressão de uma infracção determinada ⁽⁴⁾;
- c) Deve ser realizado no exercício de competências previstas no respectivo estatuto orgânico ou noutra disposição legal ou convenção internacional;
- d) Carece de autorização da Comissão Nacional de Protecção de Dados (cf. artigo 8.º n.º 2 da Lei 67/98) ⁽⁵⁾;
- e) Deve respeitar as normas de protecção de dados e de segurança da informação.

2. A recolha de dados. Os princípios da adequação e da pertinência

1. O tratamento de dados policiais, tal como acontece em relação a todos os tratamentos, deve processar-se em estrita adequação e pertinência, não devendo os dados ser excessivos em relação à finalidade que determinou a recolha ou o tratamento posterior (artigo 5.º al. c) da Lei 67/98).

Conforme a natureza e os contornos de um crime – os procedimentos de análise criminal necessários à prevenção e repressão de uma infracção ou a complexidade e “ramificações” da actividade delituosa (v.g. crime organizado, para além das fronteiras nacionais, com recursos a sofisticados sistemas de comunicações) – pode ser diversificada a informação a coligir. A abordagem e apreciação da “pertinência” em relação a uma investigação em concreto nem sempre é evidente, razão pela qual essa análise deve ser cautelosa e ponderada. Efectivamente, uma informação que – à primeira vista – se apresenta como irrelevante pode, quando relacionada com outra informação, vir a revelar-se útil a uma investigação.

2. A informação policial assume contornos particulares, desde logo, em relação à natureza e grau de fiabilidade.

⁽⁴⁾ Corresponde à previsão do ponto 2.1. da Recomendação (87) 15.

⁽⁵⁾ Nos termos do ponto 1.1. da Recomendação (87) 15 cada Estado-Membro deve dispor de uma autoridade de controlo independente e externa à polícia, encarregada de controlar o respeito pelos princípios enunciados nessa recomendação. Os ficheiros devem ser declarados a essa autoridade (ponto 1.4.).

A informação pode ser ⁽⁶⁾:

1. Confirmada ou de elevado grau de confiança, quando constatada pelo próprio investigador ou quando deriva de fonte credível;
2. Pode ser meramente especulativa ou opinativa, quando não foi sujeita a qualquer investigação ou confirmação;
3. Pode, ainda, ser “protocolada” quando advém de fontes externas de elevado grau de fiabilidade.

A investigação criminal é feita com base em diversas informações de natureza muito diversificada:

1. A par de uma “informação ou denúncia anónima” – que precisa de ser confirmada quando se assume com algum grau de credibilidade – podem surgir informações avulsas que não contêm dados pessoais ⁽⁷⁾ mas que, mais tarde, podem ser ligadas a pessoas;
2. Os acompanhantes de suspeitos ou arguidos (habituais ou ocasionais) podem ver-se envolvidos em procedimentos de investigação ou passar a integrar a base de dados pelo simples facto de terem sido relacionados com a pessoa do suspeito;
3. Se é verdade, por outro lado, que há dados pessoais que são únicos (v.g. o nome, a filiação o n.º de BI), no domínio da investigação criminal é possível que esses dados não se apresentem como tal: os suspeitos podem apresentar diversas identidades (nome, filiação, data de nascimento, nacionalidade, vários números de BI todos eles falsificados).

Os dados deixam de ser pertinentes quando se revelarem excessivos em relação à finalidade (investigação criminal) e quando perderam a sua actualidade.

⁽⁶⁾ O artigo 2.º n.º 2 do DL 352/99, relativo aos tratamentos da PJ, estabelece que “as diferentes categorias de dados recolhidos devem, na medida do possível, ser diferenciados em função do grau de exactidão ou de fidedignidade, devendo ser distinguidos os dados factuais dos que comportem uma apreciação sobre os mesmos”.

⁽⁷⁾ *Modus operandi*, fisionomia do suspeito, meios utilizados, tipo de veículos utilizados, zona de actuação.

II PAINEL

Nestas situações impõe-se que sejam tomadas as medidas adequadas para assegurar a sua rectificação ou eliminação. Os dados devem ser eliminados, nomeadamente:

- Quando sejam consideradas injustificadas as razões que levaram à sua inserção;
- Logo que tenha sido extinto o procedimento criminal;
- Logo que concluída a conclusão de uma investigação sobre um caso específico ou uma decisão judicial definitiva ⁽⁸⁾, em especial de absolvição.

3. Derrogações aos princípios de protecção de dados

1. A Directiva 95/46/CE e a Convenção n.º 108 do Conselho da Europa admitem a possibilidade de os Estados fazerem, no seu direito interno, derrogações em matéria de cumprimento de alguns princípios de protecção de dados.

O artigo 13.º da Directiva admite a adopção de medidas legislativas destinadas a restringir as obrigações relativas:

- Aos princípios da “qualidade dos dados” (da adequação, pertinência e actualização);
- Ao direito de informação;
- Ao direito de acesso;
- Ao princípio da “publicidade dos tratamentos”.

Para além destas derrogações a Convenção 108 permite, ainda, que a lei interna do Estado Parte estabeleça limites ao tratamento de categorias especiais de dados (v.g. origem racial, opiniões políticas, convicções religiosas ou outras, dados relativos à saúde e à vida sexual e condenações penais).

2. A nossa lei foi sensível a algumas derrogações. Não fez qualquer derrogação ao cumprimento dos princípios da qualidade dos dados (artigo 5.º), em

⁽⁸⁾ Veja-se o artigo 9.º n.º 3 dos Decretos Regulamentares n.º 2/95, 4/95 e 5/95 relativos, respectivamente, às bases de dados da GNR, SEF e PSP. Em relação à Polícia Judiciária veja-se o disposto no artigo 11.º do DL 352/99, de 3 de Setembro.

relação à publicidade dos tratamentos (cf. artigo 31.º n.º 1) nem em relação ao tratamento de dados sensíveis (cf. artigo 7.º).

Estabeleceu derrogações em relação ao direito de informação (artigo 10.º n.º 5) e ao direito de acesso (artigo 11.º n.º 2 e 4).

O artigo 10.º n.º 5 da Lei 67/98 permite a dispensa do direito de informação quando resulte de “disposição legal ou deliberação da CNPD, por motivos de Segurança do Estado e prevenção ou investigação criminal”.

O tratamento de dados da responsabilidade da GNR, PSP e SEF – objecto de regulamentação no domínio da vigência da Lei 10/91 – limita o direito de informação e acesso quando, nos termos do artigo 27.º da Lei 10/91 e artigo 5.º n.º 1 da Lei 65/93, o exercício daqueles direitos comprometa o segredo de estado e segredo de justiça (cf. artigo 10.º dos respectivos Decretos Regulamentares).

Com a publicação da Lei 67/98 mantêm-se em vigor as derrogações relativas ao direito de informação. Isto é, os responsáveis só devem assegurar o direito de informação quando não for colocado em causa o segredo de estado ou o segredo de justiça.

Já em relação ao direito de acesso deve entender-se que as disposições dos respectivos Decretos Regulamentares, supra citados, se devem considerar revogadas pela Lei 67/98⁽⁹⁾.

A Lei 67/98, por inspiração no direito francês, consagrou o direito de acesso por “intermediação da CNPD” ou de “outra autoridade independente”.

O acesso deverá ser requerido por escrito à CNPD, a quem compete fazer a respectiva verificação no sistema de informação do órgão de polícia criminal. A CNPD – em face dos dados inseridos e da fase e natureza do processo – delibera em que medida a divulgação de dados prejudica ou não a segurança de Estado, a prevenção ou a investigação criminal. Caso considere que a comunicação de dados ao titular prejudica a segurança de estado, a preven-

⁽⁹⁾ Em relação à Polícia Judiciária estabelece o artigo 15.º do DL 352/99 que o direito de conhecer o conteúdo do registo dos seus dados pessoais é feito nos termos do artigo 11.º da Lei 67/98.

II PAINEL

ção ou a investigação criminal deve limitar-se a “informar o titular dos dados das diligências efectuadas” (cf. artigo 11.º n.º 3).

Caso conclua que não há perigo para o segredo de estado ou de justiça deve assegurar o direito de acesso aos titulares ⁽¹⁰⁾.

De qualquer modo a CNPD deve sempre diligenciar, junto do responsável, pela rectificação, actualização ou eliminação dos dados quando se verificar que são inexactos, incorrectos ou não actualizados, nos termos dos artigos 11.º n.º 1 al. d) e 23.º n.º 1 al. g) da Lei 67/98.

4. *Decisões da CNPD*

1. Em geral, admite-se a comunicação de dados não sensíveis aos órgãos de polícia criminal no contexto do “dever de colaboração” a que todas as entidades se encontram vinculadas.

No contexto destes princípios podemos evidenciar, entre outras, as seguintes decisões da CNPD:

- Devem ser prestadas todas e quaisquer informações constantes da base de dados do recenseamento eleitoral, quando solicitadas pelas polícias, enquanto “órgãos de polícia criminal” ⁽¹¹⁾.
- O acesso da Polícia Judiciária a bases de dados não sensíveis e para mera identificação complementar de determinada pessoa (já identificada ou identificável) não carece de uma decisão de intermediação da CNPD ⁽¹²⁾.

2. Quando estiver em causa acesso a dados sensíveis ou da intimidade da vida privada – e porque afecta direitos, liberdades e garantias – esse acesso deverá ser feito nos termos de Lei da Assembleia da República ou Decreto-Lei auto-

⁽¹⁰⁾ Não se verificando qualquer das situações previstas no n.º 4 do art.º 11 da Lei n.º 67/98, de 26 de Outubro, nada impede que se dê à requerente do acesso aos dados pessoais sobre ela registados do ficheiro da PJ – Deliberação n.º 39/2000, de 17 de Outubro (in Relatório de 2000, pág. 105).

⁽¹¹⁾ Deliberação n.º 41/96, de 11 de Julho (Relatório de 1996, pág. 244) e Deliberação de 25 de Junho de 2002 (Proc. n.º 324/2002).

⁽¹²⁾ Deliberação n.º 59/98, de 9 de Julho (Relatório de 1998, pág. 109).

rizado ou mediante despacho da autoridade judiciária competente. Podem ser enunciadas, a título de exemplo, as seguintes decisões:

- Só por despacho das autoridades judiciárias – e não a iniciativa de qualquer órgão de polícia criminal – podem ser requisitadas as informações constantes em “documentos automatizados” (VIA VERDE) em poder da Brisa. A “liberdade de movimentos” deve ser preservada contra intrusões que não estejam legalmente autorizadas ⁽¹³⁾.
- Em relação à obrigação de fornecimento da documentação clínica às autoridades policiais (Policia Judiciária, PSP, GNR) entende-se que não existe disposição expressa que legitime uma obrigação de fornecimento da informação de saúde. O estatuto orgânico destas entidades policiais – pela natureza e formulação demasiado genérica das disposições relativas à “obrigação de colaboração” e às suas competências – não permite concluir que tenha sido objectivo do legislador vincular os serviços de saúde a revelar dados clínicos dos utentes.
- O acesso a “dados de tráfego” por parte dos órgãos de polícia criminal sem intervenção da autoridade judiciária, no âmbito das comunicações electrónicas, viola as disposições do artigo 34.º n.º 4, 18.º n.º 2, 26.º e 272.º n.º 3 da Constituição da República ⁽¹⁴⁾.
- Tal como acontece no regime da Lei 5/2002, só por despacho das autoridades judiciárias – e nunca por iniciativa de qualquer órgão de polícia criminal – podem ser requisitados dados pessoais sobre a situação tributária dos contribuintes ⁽¹⁵⁾.

IV. Sugestões para o futuro

A regulamentação dos tratamentos da responsabilidade dos órgãos de polícia criminal encontra-se desajustada à nova realidade.

⁽¹³⁾ Deliberação n.º 1/96, de 6 de Fevereiro (Relatório de 1996, pág. 177).

⁽¹⁴⁾ Parecer n.º 27/2004, de 8 Junho.

⁽¹⁵⁾ Parecer n.º 7/2002, de 18 de Setembro. Anota-se que, na sequência deste Parecer, a Lei n.º 93/2003, de 30 de Abril, veio estabelecer as condições de acesso e análise, em tempo real, da informação pertinente para investigação dos crimes tributários pela Policia Judiciária.

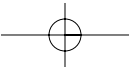
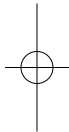
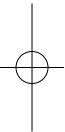
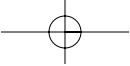
II PAINEL

À exceção da Polícia Judiciária, que adaptou um novo regime de tratamento depois da Lei 67/98, todos os órgãos de polícia criminal continuam a reger os seus tratamentos por Decretos Regulamentares em que se aplica subsidiariamente a Lei 10/91. Mesmo em relação à Polícia Judiciária foi sentida a necessidade de introduzir alterações aos respectivos tratamentos, modificações que foram operadas ao abrigo do artigo 8.º n.º 2 da Lei 67/98, de 26 de Outubro, através de “autorização da CNPD”.

Seria desejável que uma “Lei de enquadramento” regulamentasse aspectos fundamentais – aplicáveis a todos os órgãos de polícia criminal – no domínio do tratamento de dados para fins de investigação policial, nomeadamente nas seguintes matérias:

- Dados a tratar (v.g. possibilidade de tratamento de dados sensíveis – etnia, ADN);
- Delimitação dos contornos dos princípios da pertinência e da proporcionalidade em matéria de investigação policial;
- Limites específicos do direito de informação dos titulares e procedimentos relativos ao direito de acesso;
- Âmbito e limites da cooperação policial entre os vários órgãos de polícia criminal;
- Tempo de conservação de dados e regras observar para actualização de dados;
- Procedimentos de segurança que devem ser adoptados.

Esta solução, para além de clarificadora em relação às condições de tratamento, tem a vantagem de fixar os parâmetros gerais do tratamento de dados policiais e, desse modo, contribui para evitar a aprovação de diplomas específicos para cada um dos órgãos de polícia criminal, que são confrontados com a necessidade de fazer alterações legais sempre que pretendam fazer modificações às condições de tratamento.



Debate

Moderadora

Ana Luísa Gerales

Vogal da CNPD

Temos pena que não esteja aqui ninguém que possa veicular directamente esta sugestão feita pelo nosso colega no âmbito dos sistemas de informação policial sobre uma lei de enquadramento, uma lei-quadro para todas as polícias. Penso que no futuro, talvez mais próximo do que seria imaginável, poderemos ter uma lei nesta matéria que satisfaça a Comissão no âmbito da protecção de dados pessoais.

O Dr. Amadeu Guerra deu-nos vários exemplos de situações que temos tratado e das preocupações na Comissão em relação a esta área.

Quando chegámos ao fim deste painel apercebemo-nos que, de uma forma geral, quer quando se fala da videovigilância, quer quando se fala da investigação policial e do combate ao cibercrime, há sempre a necessidade de ponderar em que medida é que, perante o caso concreto, devemos considerar que a situação se justifica, ou não, se o tratamento é ou não proporcional. Devemos, sobretudo, fazer esse contraponto entre a segurança, por um lado, e a preservação da privacidade e do direito à reserva da vida privada, por outro.

Vamos abrir de seguida o debate. Quem quiser colocar as suas questões, faça o favor. Temos aproximadamente dez minutos.

Sónia Machado

TMN

Gostava só de deixar aqui duas notas. Primeiro, desconhecíamos que este diploma de que falou o Dr. Carlos Cabreiro estivesse já em discussão no Conselho de Ministros. Temos pena que assim seja porque gostávamos de participar na sua discussão. Porque vejo dois problemas: se o diploma prever que os dados de tráfego têm que ser guardados durante um ano pelos operadores de telecomunicações isso implica que os dados de tráfego respeitantes às chamadas recebidas que não estão na definição tenham que ser apagados logo após a conclusão da chamada. A Polícia Judiciária vai ter a vida ainda mais dificultada do que tem hoje. Esse é o primeiro ponto.

O segundo ponto tem a ver com a falta de sensibilização que diariamente notamos, quer na Polícia Judiciária – na brigada do Dr. Carlos Cabreiro obviamente que não, porque são pessoas que estão muito envolvidas no conhecimento dos sistemas de informação e das telecomunicações – quer em termos de justiça, em geral.

Quando digo justiça, refiro-me aos magistrados judiciais em geral e às próprias polícias que não estão especializadas neste campo. Notamos, de facto, um desconhecimento absoluto da realidade das telecomunicações. Não se sabe o que é um dado de tráfego. Desconhece-se quais as obrigações dos operadores. Ignoram-se em absoluto estas matérias. É um desafio que lanço não só à Comissão Nacional de Protecção de Dados, mas, também, à Polícia Judiciária nesta parte da especialização. E mesmo aos operadores. Já nos disponibilizámos muitas vezes para uma acção de sensibilização das magistraturas e das polícias, para que todos possam contribuir para uma melhor investigação criminal, não só mais rápida, mas, também, com maior qualidade, nesta matéria dos dados de tráfego.

E, por último, queria só deixar mais uma nota.

Cinco dias para cumprir um ofício vai obrigar a que todas as empresas de telecomunicações – e neste caso em particular a TMN – venham a ter uma direcção com 30 pessoas para responder a estes ofícios. Convém notar que, no ano de 2003, a TMN recebeu dezenas de milhares de pedidos de informação para identificação de cidadãos que são clientes da empresa e dados de tráfego.

II PAINEL

Onde está, então, a protecção da intimidade da vida privada quando um diploma vem prever que qualquer entidade pode pedir dados de tráfego, facturação detalhada, identificação de dados de base? O que se passa quando estamos a falar de números desta dimensão? Tivemos milhares de pedidos no ano passado.

Concluindo, gostava de receber alguns comentários do Dr. Carlos Cabreiro e da Comissão.

Carlos Cabreiro

Polícia Judiciária

Dra. Sónia, ainda bem que aceitou a provocação. No âmbito da Polícia Judiciária fizemos, de facto, um projecto. Como sabe, a secção que coordeno tem contactos privilegiados com os operadores de comunicações. Há em consideração os temas e conceitos que levam, naturalmente, ao parecer das operadoras sobre a grande necessidade que existe no tratamento deste tipo de dados. Eu também sinto a necessidade de os operadores serem ouvidos nesta matéria. Porque também vos posso referir que algumas questões relacionadas com os operadores de comunicações tratadas noutros países passam – e, atenção, vou falar de dinheiro – passam pelo pagamento por parte dos tribunais aos operadores de comunicações por cada informação solicitada. E não estamos a falar de pouco. Não é!!!

Quanto ao volume, não percebi muito bem a questão da Dra. Sónia, relativamente aos dados de base e em relação à facturação. Se não se importa de repetir a questão.

Sónia Machado

TMN

A definição de dados de tráfego se é a mesma que consta da lei que está a ser discutida em Conselho de Ministros não vai permitir que os operadores de telecomunicações tratem e conservem os dados das chamadas recebidas

durante um ano. Porquê? Porque os dados das chamadas recebidas não são necessários, adequados e pertinentes, para a actividade de um operador de telecomunicações. A informação da chamada recebida só serve para tratar quem faz a chamada, a facturação, o consumo, e não quem recebe a chamada. Ou seja, o número e a identificação do dado recebido pela definição que ali está e pela conjugação com a lei n.º 67/98 e, agora, com a lei 41/04 vão ter que ser pagos por nós.

Carlos Cabreiro

PJ

Já entendi. Mas, atenção, que a facturação detalhada, nos moldes em que a Dra. Sónia está a falar, não se engloba naquela definição de dados de tráfego, mas está sim, nos dados de base. Porque é preciso distinguir o que são os resultados de uma comunicação – os dados técnicos de uma comunicação, que considero que são, tão só, os gerados pelo sistema de comunicações – e o que são elementos referentes à facturação. Estes são muito úteis à investigação, mas, na nossa opinião, porque não são gerados automaticamente pela comunicação em si, não devem ser considerados dados de tráfego. Isto não invalida que incida sobre eles a protecção da privacidade e que só possam ser solicitados pela autoridade judiciária.

Sónia Machado

TMN

Neste ponto, provavelmente, vamos precisar da Comissão Nacional de Protecção de Dados, mas, segundo esta interpretação – e mantenho o meu ponto de vista – na medida em que não posso, nos termos da lei 67 e da lei 41/04, tratar dados de chamadas recebidas também não os vou poder fornecer à Policia Judiciária, porque serei obrigada a apagá-los, após a conclusão da chamada. Mas, agora, trata-se de um desafio para a interpretação.

II PAINEL

Amadeu Guerra

CNPD

Em primeiro lugar, acho que, eventualmente, o legislador aqui não clarificou bem os conceitos. A própria Comissão no parecer que deu chamou a atenção para isso. Isto é, há um parecer da Procuradoria-Geral que tem sido seguido e relativamente ao qual a Comissão tem o mesmo entendimento, sobre a distinção entre o que são dados de base, dados de tráfego e de conteúdo. Chamámos a atenção para a possível confusão que pode ser gerada. Na sequência do parecer que demos houve um ajustamento ao diploma em que, apesar de ter sido mantido o conceito, acrescentou-se mais qualquer coisa ao diploma, para dizer “bom, são os dados de base, ou tráfego, mas não estes nem aqueles”. Portanto, acho que há aqui, em termos doutrinários, uma alteração de conceitos.

Há três diplomas que devem manifestar um equilíbrio.

Antes da Comissão intervir – porque também tem muito onde intervir – vamos ver se no balanceamento destes três diplomas há ou não dúvidas. Eu penso que é capaz de haver, mas não se aceitou na totalidade aquilo que a Comissão pretendia, apesar de, depois, num segundo parecer, termos considerado a solução satisfatória. Penso que os conceitos se deviam manter, mas alterarem-se os conceitos de dados de tráfego, conteúdo, e, essencialmente, os de base e de tráfego. Na minha óptica, estes conceitos não são precisos, mas isto também se relaciona com definições, com o Conselho da Europa, etc. Relaciona-se, ainda, com definições de outros diplomas, noutros países e, nomeadamente, a nível quer da União Europeia, quer a nível do Conselho da Europa.

Moderadora

Mais alguma questão?

Carlos Cabreiro

PJ

Só para dizer que estas definições beberam, essencialmente, dos instrumentos internacionais. Nomeadamente, a ciberconvenção, que tem a ver com a tentativa de uniformização de legislações relativas a crime informático.

Eis uma situação em que os dados de tráfego e os dados de base são distinguidos desta forma. Acrescentando nós, nesta posição, os dados de localização e os dados de conteúdo. Como perceberão, têm outro significado e outra actualidade.

Jorge Silva

KidsNanny

Eu sou o gestor de um projecto que se chama <http://kidsnanny.com> e segui muito atentamente a palestra do Dr. Alexandre Pinheiro.

De facto, particularmente, esta semana surgiu a informação sobre um parecer negativo quanto à colocação de câmaras de videovigilância em infantários e creches. O que eu gostava aqui, de facto, de tentar obter, e porque isto é um tema bastante polémico, era algum tipo de informação e algum tipo de reacção, face a alguns argumentos que passo a explicar.

Tanto quanto me apercebi, o parecer teve um carácter negativo na medida em que considerou violar-se a privacidade das pessoas que trabalham nesses locais e das crianças por serem sujeitos a uma videovigilância, à utilização de meios mecânicos. No entanto, gostava de salientar duas situações.

Actualmente, a mobilidade tem um carácter essencial para o dia-a-dia das pessoas. Cada vez mais, a tecnologia e a maneira como a empregamos é, de facto, o elemento chave, como muito bem disse e frisou o Dr. Alexandre, e pode ser encarada sob um aspecto negativo de controlo.

No entanto, a meu ver, há uma situação particular que surge quando colocamos um filho num infantário. Neste caso estamos a solicitar um serviço que não temos forma de controlar. Aqui entra uma questão de direito de consumo.

II PAINEL

Solicitamos um serviço e queremos que seja prestado de acordo com determinadas expectativas. Colocar uma criança num infantário relaciona-se com a educação de um filho e esse âmbito é um aspecto que, a meu ver, parece ter ser ignorado

Por outro lado, hoje em dia as creches, os infantários, têm uma política de porta aberta. Qualquer encarregado de educação, qualquer pai, pode aceder à informação do filho ou ver o que se passa nas instalações. Ora, isso é inconcebível e até prejudicial porque a presença do pai ou da mãe num infantário provoca, naturalmente, a distração e desatenção das crianças.

Moderadora

Eu ia pedir para sintetizar a sua intervenção, por favor, porque estamos já com falta de tempo. Temos outro painel. Muito obrigado.

Jorge Silva

KidsNanny

No fundo a questão é esta: no estado democrático verificam-se situações em que são obrigatórias as câmaras de videovigilância para protecção de pessoas e bens. Estou-me a lembrar, por exemplo, de uma discoteca, um estádio de futebol.

No caso de um infantário e considerando o imperativo de protecção das crianças não será do interesse público que os pais, e estamos a referir apenas os pais, tenham acesso à informação, às imagens das crianças, a dados sobre o seu bem-estar?

Alexandre Pinheiro

CNPD

Muito obrigado pela pergunta. É de facto uma das matérias mais sensíveis que a Comissão tratou nos últimos tempos não só no campo da videovigilância, mas, também, em geral.

Os argumentos incidiram sobre a privacidade das crianças e a avaliação do desempenho profissional do educador durante todo o tempo. Tratava-se de um sistema que seria disponibilizado *on-line* a todos os encarregados de educação, de um sistema contínuo. Ora bem, o que é que nos pareceu?

Pareceu-nos que se tratava de um sistema abusivo, excessivo que punha em causa a privacidade do menor, que não pode prestar o seu consentimento. O sistema envolvia o consentimento dos envolvidos e, nesse sentido, talvez a decisão seja mais polémica.

No entanto, mesmo assim, entendeu-se, e a decisão é muito discutível, entendeu-se que há um direito à privacidade por parte de menores que deve ser tutelado. O menor não pode agir em relação a quem tem o direito do poder paternal, portanto aqui a acção é injuntiva e, por outro lado, entendeu-se que, inevitavelmente, haveria uma fiscalização do desempenho. Já houve casos em que outras comissões, congéneres da Comissão Nacional de Protecção de Dados, nomeadamente a comissão francesa, apreciaram e autorizaram casos em que havia um período ao longo do dia de observação, mas não se tratava de observação em contínuo.

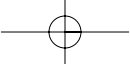
Agora, a sua última referência é bastante interessante. Haverá alguma coisa mais importante do que a segurança e o bem-estar dos nossos filhos? Nesse porque não recorrer às câmaras de vigilância? Ora bem, aqui reflecte-se mais uma vez o binómio e o ponto de tensão entre liberdade e segurança.

É obvio que é importante a existência de elementos que garantam a segurança. É obvio que as câmaras são um elemento que pode contribuir de uma forma muito expressiva para a garantia de segurança, mas não podemos através deste elemento de fiscalização, de observação por câmaras, desfazer outros bens que devem ser protegidos. A decisão é polémica, isso é verdade. Era isto o que tinha a dizer.

Moderadora

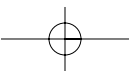
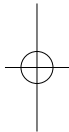
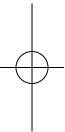
Temos pena de não prolongar o debate, mas, de facto, neste momento estamos com o nosso tempo esgotado. Espera-nos outro painel com vários oradores e vamos ter que interromper aqui.

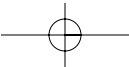
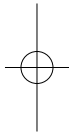
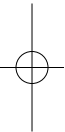
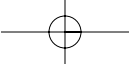
Muito obrigada pela vossa presença.



III PAINEL

Tecnologias e Vida Privada





Filipe Custódio

Especialista em segurança informática

A (IN)SEGURANÇA DA INFORMAÇÃO NAS REDES ABERTAS

Boa tarde, quero agradecer à Comissão Nacional de Protecção de Dados o convite que me foi endereçado.

Nesta apresentação vamos falar essencialmente sobre tecnologia no que respeita à segurança da informação e das questões especificamente relacionadas com a protecção da informação do indivíduo, com a protecção de dados pessoais.

Vou começar por falar sobre a informação que guardamos nos nossos computadores para sabermos até que ponto está protegida. Vou aqui falar, essencialmente, sobre os nossos computadores lá de casa que, muitas vezes, não é o enfoque da maior parte das reflexões sobre segurança.

Fala-se muito sobre a segurança dos dados nas empresas, segurança da informação de negócio, mas penso que é muito urgente e importante, também, começarmos a pensar sobre a protecção da informação que temos nos nossos computadores caseiros. Ou seja, se calhar, há cinco/seis anos atrás, a maior parte das pessoas, tinha a sua informação privada em papel, as suas fotografias em rolos fotográficos, as primeiras gravações áudio dos filhos em cassetes áudio.

Hoje em dia, temos cada vez mais fotografias digitais, documentos Word, folhas Excel com o orçamento da família, contas de acesso à Internet, de *home-*

banking, ou seja, muita informação nos habituámos a guardar em suporte digital. Penso que na maior parte dos casos poucas pessoas sabem o risco a que essas informações estão sujeitas.

Irei referir apenas algumas ameaças, mais no sentido de alertar para o tipo de risco que existe e, respondendo ao repto deste Colóquio, dar alguns conselhos. Neste caso, ao contrário dos painéis anteriores, não estou a falar de conselhos a nível legislativo, de orientações para o país, estou a dirigir-me às pessoas em concreto.

O que é que podem fazer para se proteger no século da informação, o século XXI, que, apesar de ter começado há poucos anos, está a mudar muitas coisas nas nossas vidas para melhor, na maior parte dos casos. O reverso implica, precisamente, lidar com os riscos dessa mudança.

Não vale a pena falar sobre o quê é a Internet, acho que já toda a gente nesta sala sabe, mas vou só relembrar um pequeno detalhe. Se tivermos um computador, algures na Europa, algures em Portugal, algures em Lisboa, ligado à Internet através de banda larga estamos apenas a uns segundos de uma ligação feita, por exemplo, a partir do Brasil, de alguém que queira aceder aos nossos ficheiros. A globalização da Internet significa que os ataques são completamente globais. Não há qualquer diferença de custo entre atacar a partir da Malásia, da Europa de Leste ou do Brasil. Aliás, surgiram umas estimativas que diziam que a maior parte *dos hackers* mundiais são do Brasil, portanto temos aí alguma afinidade cultural, não sei.

É preciso ter atenção porque quando pensamos viver num país à beira mar plantado, num país de brandos costumes, o facto é que a maior parte dos criminosos informáticos, segundo este estudo, pode ser discutível obviamente, fala a nossa língua, consegue ler os nossos ecrãs de *homebanking*, tem alguma afinidade com os portugueses, gosta de gozar com os portugueses. É só um alerta para os perigos que andam por aí.

Falando em concreto, muita gente exclama quando falo desta história da segurança informática: “mas tu és paranóico, mas o que é que é isso! O quê que alguém pode querer do meu computador lá em casa? O que tenho lá é meu e ninguém quer saber disto”.

III PAINEL

Por isso vou mencionar alguns artigos disponíveis na imprensa *on-line* para mostrar que, actualmente, não só toda a gente está em risco como ainda todos são atacados mesmo que o ignorem.

Um estudo feito por um instituto norte-americano em 2003 e 2004 chegou à seguinte conclusão. Em 2003 ligaram à Internet um PC vulnerável, um computador acabadinho de vir da loja, instalado sem utilizações de segurança, sem *firewall*, sem anti-vírus. Em quarenta minutos foi comprometido. Em 2004, demorou vinte minutos. Podemos admitir que a situação tenda a agravar-se.

Isto significa que ninguém sabia que aquele computador estava ligado à Internet, mas que existem hoje em dia ferramentas de ataque generalizado e automatizado que procuram sistematicamente todos os sistemas vulneráveis do mundo e atacam-nos.

Com certeza se lembram do ataque do *Blaster*. Em Agosto de 2003, o *Blaster* demorou apenas cerca de quinze a vinte minutos a atacar todas as máquinas vulneráveis do Mundo. Ainda na parte da manhã falamos nos links de dez *giga-byte* e até me surpreendeu que já tivéssemos isso cá em Portugal, mas o reverso da medalha é que quanto mais rápidas as comunicações mais fulgurantes os ataques.

Consideremos, agora, o *spyware*, o *software* que ninguém pediu para instalar na máquina. Muita gente não sabe que lá está. De vez em quando dizem: “eh pá, o meu *Explorer*, às vezes, abre assim uns sites de pornografia, eu nem sequer os queria ver”. Ou dizem assim: “eh pá, o meu computador está lento, está esquisito, o que é que será isto?”.

Na maior parte dos casos é o chamado *spyware*, *adware*, há muitos nomes. Isso, basicamente, é *software* que instalado sem se saber com outro *software* gratuito que se puxou da Internet.

Ou a pessoa foi visitar um site qualquer na Internet, apareceu um daqueles *pop-up's* a dizer “tem a certeza que quer correr isto?”. A pessoa carregou *enter*, *yes*, e pronto, já está! É um problema que está a crescer. Já vou dizer, daqui a pouco, porque é que isso está a crescer. Um estudo concluiu que nos Estados Unidos 80% das máquinas têm este *spyware* instalado. Este estudo foi financiado por uma empresa que vende ferramentas *anti-spyware*.

Eu diria que 60% é uma boa estimativa. Mesmo assim, é interessante o número. Porque é que estas máquinas são comprometidas? Porque é que gangs organizados de crime informático atacam sistemas de pessoas individuais que não têm nem negócios nem bens que justifiquem um ataque?

Em primeiro lugar, porque uma máquina com acesso a banda larga, ligada todo o dia, tem um valor comercial. Outro artigo constata já existirem negócios no mercado negro de venda e aluguer de redes de máquinas comprometidas. É um problema que tem a ver com o *spam*, o correio electrónico não solicitado.

Os Estados Unidos, que não eram muito agressivos em relação a esse de envio de correio não solicitado, também já aprenderam, tal como a Europa, que se trata de uma praga da Internet e começaram a legislar para acabar com o *spam*. Só que, naturalmente, os atacantes evoluem e tentam fugir à lei.

Como é que o fazem? Alugam à hora redes de máquinas comprometidas e o próximo correio electrónico não solicitado, em vez de ser enviado de um servidor qualquer de uma empresa que pode ser obrigada a desligá-lo, passa a ser enviado da vossa casa. E isso é uma das razões pelas quais estes PC's têm valor comercial.

Outro aspecto reside nos ataques de negação de serviço, usados para crimes de extorsão. Um criminoso telefona para uma empresa e diz assim: "ou vocês me pagam X ou o vosso site vai abaixo". Quando o site vai abaixo o ataque não provém de um determinado ponto do globo, mas é antes um ataque vindo de milhões de máquinas de todo o mundo. Os tais 80% de máquinas que têm o *spyware* instalado podem estar a participar hoje, sem que os seus donos o saibam, em redes de ataque e para cometer crimes informáticos.

Outra informação que tem muito valor, é o próprio – e falando agora de dados pessoais – endereço de correio electrónico. Deixem-me só fazer aqui um pequeno parêntesis.

Acho que as pessoas só sentem realmente esta questão da privacidade quando lhes toca na pele. Uma das vezes que isso me tocou na pele foi quando recebi um daqueles correios electrónicos não solicitados em casa. Achei curioso

III PAINEL

porque provinha de uma empresa nacional. E pensei: “ah, ah! Já vou conseguir fazer alguma coisa”.

Ora, mandei um mail educado para esses senhores a dizer assim: gostaria de saber onde é que obtiveram o meu e-mail, gostaria de saber quem é o responsável da vossa base de dados porque, é assim, eu também já li a Lei de Protecção de Dados Pessoais. E que me responderam? “É pá, olha, desculpa lá. Sabes o que é que é? Comprei um CD onde estava o teu mail”.

Nesse momento fiquei assim: “mas como é que o meu e-mail foi parar a um CD que anda à venda por aí?” Depois de investigar um pouco apurei que, afinal, o meu e-mail vale muito pouco. Consegue-se comprar um CD com 250 milhões de endereços por dois dólares. Portanto, este é o nível de perigo em que estamos.

Passemos a outra questão. A fraude da banca electrónica assumiu, este ano em particular, uma importância muito grande a nível mundial e os bancos portugueses também não estão a salvo disso. O problema com os ataques de *fishing* começa muitas vezes no acto da compra de um computador pessoal.

Quando a pessoa compra o computador na loja, a máquina vem insegura por omissão, ou *by default*, em inglês.

Quando se compra um computador e se instala em casa a máquina muitas vezes não traz os últimos serviços, *packs*, ou os sistemas operativos mais recentes. Ainda há portáteis à venda com o *Windows 98*. É um sistema muito inseguro face aos ataques de hoje em dia. Muitos computadores não vêm com anti-vírus ou dispõem de anti-vírus que têm um limite de 90 dias. E a pessoa pensa assim: “espera aí, mas eu agora vou ter que pagar a uma empresa qualquer para o meu computador não ser atacado? Acabei de pagar 200 ou 300 contos pelo meu computador e agora vou ter que pagar mais para não ser atacado?”

O computador não vem com *firewall* pessoal e isso é um problema. Se, no passado recente, o tipo de equipamento consistia no computador que era ligado directamente à Internet, hoje em dia, com o ADSL, com a Netcabo, etc., cada vez mais se recorre a um *router*, uma caixinha que se compra na loja e se liga à rede.

Esse equipamento tem como missão ligar-nos à Internet e proteger-nos dos ataques. Normalmente tem pequenos aplicativos de *firewall*, nada de muito especial, mas oferece alguma protecção. O que acontece é que esses equipamentos também vêm mal configurados. Vêm com as *passwords* de administração que podem não ser alteradas e trazem os interfaces de administração disponíveis na Internet.

O que é que eu quero dizer com isto? Quero dizer que, casualmente, navegando na minha ADSL *neighbourhood* – ou seja, os outros utilizadores que estão ligados na mesma rede em que eu estou – rapidamente consegui aceder, via *web*, a um site de administração de um desses *routers*.

Tinha *password by default* e se eu quisesse podia, sem grande custo, usar este *interface* de configuração para desviar o tráfego e, permitir-me a mim, se fosse um atacante, chegar à rede interna de determinada casa, ou também, usar este *router* com reencaminhador de tráfego. Um eventual ataque seria feito a partir desse utilizador incauto e não do atacante real.

Um outro exemplo reporta-se às interfaces de Telenet, também abertas. Portanto, é preciso chamar à atenção para as pessoas que montam equipamento de comunicações em casa, mesmo que não tenham os conhecimentos para tal, para solicitarem aos operadores que procedem no sentido de efectuarem instalações minimamente seguras. Além disso, colocar uma *password* num equipamento é algo que demora 30 segundos. Não demora mais que isto.

No caso do *wireless* ainda é pior. Com um programa que basicamente detecta os *access points* disponíveis num determinado local mesmo um portátil como uma antena muito pequenina que só apanhe os que estão muito próximos é possível aceder a sistemas não-protegidos. É possível usar o *access point* alheio, cometer actos ilícitos e os *logs* apontam para a máquina deixada desprotegida.

Nos casos de *fishing* é importante assinalar que nenhum banco envia um mail solicitando que se aceda a um *link* para certos efeitos e muito menos que sejam indicadas as credenciais do cliente.

Os ataques diários em que um criminoso rouba a *password* de acesso à banca *on-line* e transfere o dinheiro para outra conta não atingem de momento gran-

III PAINEL

des proporções e, enquanto os ataques forem poucos, se calhar os bancos até, para não prejudicar a sua imagem, repõem o dinheiro e fazem de conta que nada aconteceu.

Acontece, no entanto, que no caso de um banco que tenha uma cláusula que diga ser eu o responsável pela protecção das minhas credenciais e, conseqüentemente, ocorrer um roubo através do furto das minhas credenciais, sou, portanto, responsável e resta-me assumir a responsabilidade.

Ou seja, os bancos podem até – porque não querem estragar a sua imagem – optar por repor o dinheiro, mas não têm obrigação de o fazer. Pelo menos face ao contrato que eu tenho. Não sou jurista e, portanto, não faço a mínima ideia se estou certo ou não. É preciso ter muito cuidado com isto. É necessário ter cuidado com o *software* que se instala nos PC's, os sites a que se acede e a quem se dão as credenciais de *homebanking*.

Voltando ao *spyware*. Tipicamente, o *spyware* visava apenas obrigar as pessoas a consumirem publicidade. O primeiro sintoma de *spyware* surge quando estão muito bem na vossa máquina e o *Explorer* abre com uma página qualquer. Pronto, isso é um sintoma típico de *spyware*. Mas já existe *spyware* que, agrega informação sobre a pessoa: onde é que pessoa vai, o que faz, etc., e transmite-a para fora, para um servidor central. Desvia o acesso a determinadas páginas. Imaginem que têm um negócio *on-line*, concorrente com outra empresa e querem ter mais acessos que o concorrente. Contratam um *hacker* russo qualquer – acho que eles são baratos – para fazer um *spyware*, espalhá-lo pela Internet e, sempre que alguém escrever o endereço do vizinho do lado, vai à vossa página. Portanto, isto é real.

Uma referência ao roubo de informação. No ano passado ocorreram uns ataques em Portugal de *keyloggers* que capturam as teclas de acesso à banca. A banca adaptou-se, mudou o sistema de acesso, mas não anulou o problema. O problema é que, enquanto as credenciais de acesso ao *homebanking* forem algo que eu digito apenas no teclado é possível capturá-las. Este roubo de informação é cada vez mais frequente.

Outra questão muito importante prende-se com o facto da informação que é roubada muitas vezes ir parar à Internet. Consultas a bases de dados (*queries*)

permitem obter informações de cartões, mesmo que cancelados, obter números de telemóvel que se pretendiam confidenciais. Deparamo-nos com situações em que uma pessoa, tem uma assinatura num mail com o número do telemóvel, participa numa *mailing list* qualquer e a *mailing list* é arquivada, é posta *on-line*. A informação vai para a Internet e é quase impossível tirá-la de lá. Por muita vontade, até legal, que haja, de remover uma informação, há *caches*, há *mirrors*, a informação pode estar disseminada por montes de sítios. Ainda hoje consigo descobrir os mails que mandei para uma *mailing list* quando estava no Técnico há uma década. Portanto...

Outra questão relativa às fotografias digitais. Hoje em dia quase toda a gente tem uma câmara digital. É uma revolução que está, realmente, a tomar conta da nossa sociedade. Existem sites para partilhar as fotografias com os amigos, mas outras pessoas podem igualmente aceder a esse site. É possível indexar essas fotografias. Há *queries* que obtêm fotografias com simples busca do DSCN, o prefixo do ícone usado nos ficheiros, ou do JPEG, tal como existem programas que recolhem endereços de correio electrónico para depois fazer os tais CD`s de venda no mercado negro.

Em conclusão: como é que nos devemos proteger?

É imperativo proteger o computador. Toda a gente deve ter, no mínimo, um anti-vírus, uma *firewall* pessoal, fazer as actualizações do *software*, usar o *software* mais seguro que consiga, ou seja, face a duas opções, usem a mais segura – pelo menos a que vos disserem ser a mais segura – e usar *software* de *spyware*.

Relativamente aos *routers* é preciso serem bem configurados. Não é preciso ser um grande especialista para o fazer e pelo menos as pessoas que vos instalam os *routers* em casa devem ter estes cuidados.

Em relação ao *homebanking* nunca se deve seguir quaisquer links comunicados por mail e em caso algum fornecer as credenciais de acesso, seja a quem for. A *password* de acesso ao *homebanking* é informação estritamente pessoal e intransmissível.

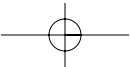
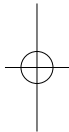
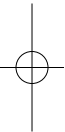
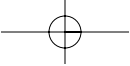
A Internet não deve ser utilizada para acesso a sites sensíveis e toda a informação dispensada através de formulários electrónicos deve restringir-se ao mínimo indispensável.

III PAINEL

Cautela na replicação de fotos. O *Peer-to-Peer*, *Emule*, *Kazza*, etc., são muito bons a indexar todos os ficheiros do vosso disco e a disponibilizá-los a todo o mundo mesmo que vocês não saibam.

Finalmente, fazer com regularidade uma pesquisa pelo vosso nome na Internet às vezes dá resultados interessantes.

Muito obrigado.



Profesor Álvaro Canales Gil

Secretário-Geral da Agência Espanhola de Protecção de Dados

A PROTECÇÃO DE DADOS PESSOAIS NA INTERNET

Boa tarde.

Antes de mais quero felicitar a Comissão Nacional de Protecção de Dados pelos seus dez anos de actividade na defesa dos direitos pessoais dos cidadãos portugueses.

Desejo, ainda, endereçar a todos os presentes calorosas saudações em nome do director da Agência Espanhola de Protecção de Dados, Dr. José Luis Piñar, que, por motivo de ausência no estrangeiro, não teve oportunidade de corresponder ao convite para assistir a este Colóquio patrocinado por uma Comissão irmã com quem mantemos relações muito estreitas e cordiais.

Ao olhar mais uma vez para o cartaz que anuncia este Colóquio deparo com as palavras: "Um desafio constante". Ao escutar a explicação técnica do meu companheiro de painel Eng. Filipe Custódio e, tal como afirmou o moderador, torna-se evidente que o tema da Internet desperta preocupação universal e gera intranquilidade quando damos conta que a nossa vida privada, não apenas a nossa intimidade, mas, até o património pessoal, a situação financeira, não estão de forma alguma a salvo de possíveis agressões externas.

Nesta comunicação vou, de forma sucinta, levantar uma série de problemas, identificar presumíveis responsáveis e apontar soluções possíveis na base da

experiência da Organização para a Cooperação e o Desenvolvimento (OCDE) e da Agência Espanhola de Protecção de Dados. Terei, igualmente, em linha de conta os ensinamentos sobre combate ao *spamming* proporcionados pela *Federal Trade Commission* dos Estados Unidos com quem mantemos relações de cooperação recíprocas.

Como ponto de partida creio ser necessário não perder de vista os princípios gerais e definir uma premissa necessária.

Em primeiro lugar, existem dois modelos antagónicos e duas abordagens sobremaneira divergentes em relação ao direito fundamental da protecção de dados.

Por um lado, temos o modelo norte-americano que considera a protecção de dados de carácter pessoal e os dados pessoais dos cidadãos como um aspecto, um factor de mercado, e não como direito fundamental e, por outro lado, o modelo europeu que define tal protecção como direito fundamental.

O modelo europeu é partilhado por Portugal e Espanha por via da transposição para as respectivas legislações nacionais da Directiva 95/46 e de outras Directivas que referiremos sobre telecomunicações.

Revela-se, portanto, necessário reconhecer que a doutrina sobre dados pessoais comporta uma importante influência de modelos jurídicos, além das suas vertentes de ordem económica.

Os dados pessoais dos cidadãos não apresentariam qualquer valor acrescentado se estivéssemos a considerar apenas de perfis, estatísticas ou outras formas de recenseamento de informação sem valor económico intrínseco. Temos, conseqüentemente, bens jurídicos absolutamente diferentes em função dos modelos adoptados.

Em relação à Internet gostaria de referir um aspecto.

A Internet, *grosso modo*, foi concebida como uma ferramenta útil de efeitos benéficos óbvios. Assim, generalizando, os fabricantes e, inclusivamente, os provedores de acesso, partem do princípio que uma ferramenta útil de efeitos benéficos óbvios deve ser divulgada de forma coerente e uniforme para que a maior parte das pessoas possa aceder à informação.

III PAINEL

Tal situação obriga-nos a considerar os problemas que levanta o uso indevido da Internet. Os problemas que a própria rede cria devido à sua utilização por interesses financeiros, empresariais, à ocorrência de fraudes, ao impacte sobre o consumo, à exploração por terroristas, etc., etc.

As duas premissas que pretendia tivessem em linha de contas são as seguintes: os diferentes modelos jurídicos e os diversos interesses envolvidos, por um lado, e a utilidade e efeito benéfico inerentes à criação da Internet, por outro. Quem pretende usar a ferramenta Internet para fins malévolos aproveita-se, obviamente, desta situação.

Basicamente e de forma muito sintética deparamo-nos com dois modelos jurídicos sobre protecção de dados: o norte-americano, considerando-a um dos factores de mercado, e o europeu, entendendo-a como direito fundamental. Temos, ainda, um terceiro modelo, o chamado modelo *habeas data*, criado ou adaptado por países que estiveram tradicionalmente na área de influência do modelo norte-americano e que visa integrar o direito fundamental ou determinados direitos dos cidadãos em matéria de protecção de dados.

O *habeas data*, que não possui em muitos países uma expressa tradução constitucional, tem-se imposto por via da jurisprudência. Em regra, os cidadãos vítimas de prejuízos por uso indevido dos seus dados pessoais recorrem, se assim o entenderem, aos tribunais para uma acção civil.

Este modelo encontra-se ainda muito longe do modelo europeu em que uma autoridade de controlo independente derime as controvérsias entre o cidadão e o responsável pelo tratamento dos seus dados pessoais.

Representa uma fase intermédia para que esses países possam reconhecer a pouco e pouco esse direito e actuem no sentido de evitar usos abusivos.

Assim, quando falamos da posição do cidadão e do seu direito fundamental deparamo-nos com um triângulo dado que o responsável das bases de dados tem de estabelecer uma interconexão com tal direito e respectivas implicações e, ao mesmo tempo, não desperdiçar os benefícios que as tecnologias de informação e comunicações apresentam para tratamento de dados, em geral, e de dados pessoais, em particular.

É uma situação conhecida. Todos os dias a figura jurídica “dados pessoais” incorpora novos conceitos e novos aspectos porque ela implica, por definição, todo e qualquer dado que permita a identificação do cidadão.

Surgem novos conteúdos. Temos o IP, o endereço de determinado computador, e o endereço de *e-mail*. Temos o número de cliente e/ou de utilizador, mas com uma matiz porque no direito espanhol o cliente é a pessoa em nome de quem está firmado o contrato e o utilizador pode ser qualquer membro da unidade familiar. Podemos considerar o caso da matrícula automóvel. Temos os casos de certos parques que registam a hora de entrada do veículo e, por via indirecta, a matrícula e, conseqüentemente, a identidade do proprietário, ainda que surja a questão de identificar o condutor.

Sem necessidade de referir o endereço postal e tantos outros dados, o facto é que a sociedade de informação produz constantemente novos elementos que nos identificam como cidadãos.

As tecnologias de informação de comunicações servem, naturalmente, para tratar esses dados que podemos abordar segundo três pontos de vista:

- o responsável da base de dados pode utilizar suportes electrónicos;
- o responsável da base de dados pode utilizar redes de telecomunicações;
- o responsável da base de dados pode utilizar a Internet, essa ferramenta tão poderosa e valiosa de benefícios inegáveis, mas que coloca, também, problemas acrescidos.

Dou-vos o seguinte exemplo que envolve os registos em publicação oficial. Em Espanha quando o Conselho de Ministros indulta um cidadão tal acto administrativo, um Decreto Real, é publicado no “Boletín Oficial del Estado”.

Houve casos em que alguns cidadãos expressaram o desejo de não ver o seu nome publicado no “Boletín Oficial del Estado”. O governo tem nos termos da lei a prerrogativa de tornar público os seus decretos por tal meio, mas se alguma página da Internet, um prestador de serviços, incorporar essa informação os dados desse cidadão passam a estar permanentemente disponíveis ao escrutínio público. Já não é a questão de ter o nome e apelido publicados

III PAINEL

em determinada edição do “Boletín Oficial del Estado”, mas esses dados podem, por exemplo, ser incorporados em permanência a uma base de dados sobre indultos oficiais anuais. É uma situação penosa. É uma situação diferente da colocada pela publicação de um indulto no “Boletín Oficial del Estado” e que comporta um tratamento de dados pessoais.

É um exemplo, entre muitos.

O que acontece quando o responsável das bases de dados utiliza as redes de comunicações?

Pode utilizar o fax, recorrer a serviços de localização, de tráfego e facturação, a mensagens SMS ou MMS, incorporando som e imagem.

Temos, ainda, a questão preocupante do *wireless* que permite aceder à Internet a partir dos mais diversos locais, dispensado a infraestrutura tradicional de cabo. O utilizador de WIFI pode ver as suas ligações desviadas para sistemas onerosos de comunicações ou ser vítima de furto de dados. Coloca-se o problema de se, por exemplo, criar um sistema WIFI na Agência Espanhola de Protecção de Dados, poder ficar vulnerável a captações de informação do exterior. Apesar de existirem limitadores nada me garante que as radiofrequências não permitam o acesso a quem está fora do edifício. Deparo-me, portanto, com uma falta de garantias adequadas de segurança.

No caso da Internet coloca-se, também, o problema dos *cookies*. Estas parcelas de informação armazenadas pelo *browser* no disco rígido do computador estabelecem critérios de navegação e recuperação de informação que podem ser utilizados pelo prestador de serviços.

Os *dialers* representam, por sua vez, um sistema informático que à revelia do utilizador, do cidadão, remetem automaticamente ao aceder a certas páginas para uma determinada linha de valor elevado, o 906 no caso de Espanha.

Como identificar, então, os responsáveis por estes ilícitos?

No caso dos *cookies* trata-se do prestador de serviços solicitados que através desses ficheiros apura os meus hábitos de navegação.

Os prestadores de serviços de acesso respondem pelo sistema de marcação automática e os perfis implicam os serviços de facturação e tráfego. O opera-

dor telefónico será o responsável no caso de interpretação e tratamento de tais dados. Os ilícitos nos casos de envio de informação por fax serão da responsabilidade do emissor tal como o *spamming* por *e-mail*, SMS ou MMS.

Em matéria de Directivas contamos com a Directiva 2002/58 sobre telecomunicações e a Directiva de Protecção de Dados e, em Espanha, a legislação de telecomunicações e a própria legislação sobre Protecção de Dados de Carácter Pessoal.

No caso do *spamming* os modelos são, outra vez, muito diferentes. O modelo norte-americano ao não assumir a protecção de dados um direito fundamental e ao considera-la um factor de mercado e consumo acarreta duas consequências lógicas: estabelece o sistema de *opt out* que permite o envio de correio electrónico de teor comercial excepto nos casos em que o destinatário recuse expressamente a recepção de determinados emails comerciais. Dado que a opção sobre a aceitação de correio electrónico comercial recai sobre o cidadão esta matéria não é tutelada por uma entidade de protecção de dados, mas por um órgão de regulação do consumo, a *Federal Trade Commission*.

O modelo europeu considerado sinteticamente, salvo questões de pormenor, que o correio electrónico pessoal indesejado não pode ser recebido pelo cidadão a não ser que exista uma prévia relação jurídica entre o emissor e o receptor.

Tal opção levanta problemas e em Espanha o combate ao *spamming* é incumbência da Agência Espanhola de Protecção de Dados.

Quais as soluções?

São de dois tipos: preventivas, implicando cooperação de diversas entidades nacionais e internacionais, ou correctivas.

O grupo de reflexão sobre o *spamming* da OCDE, quer no encontro da Coreia do Sul, quer na reunião recente em Londres, definiu uma série de critérios que, logicamente, realçam a cooperação internacional e, também, as acções educativas e a formação dos utilizadores da Internet.

Em Espanha, a influente "Asociación de Usuarios de Internet" criou, designadamente, uma base de dados específica sobre *spamming*.

III PAINEL

Contamos, ainda, com soluções de carácter técnico.

O correio electrónico pode ser filtrado através de etiquetagem que permita e identificação clara de mensagens comerciais, apesar de existirem algumas dificuldades.

É possível elaborar listas brancas e negras de correios electrónicos.

Os provedores de serviços podem bloquear o envio maciço de mensagens que apresenta um custo baixíssimo para os responsáveis pelo *spamming*.

Seria igualmente muito importante a alteração dos protocolos de transmissão para salvaguardar a identidade dos cidadãos. Isso implicaria que fossem facultados dados reais, residência, por exemplo, para confirmar registos prévios.

É possível, ainda, recorrer a solução de índole económica onerando o envio de mensagens e avançar na via da autoregulação do sector para obviar aos aspectos negativos que podem apresentar as *firewalls*, os *cookies* ou os sistemas de *wireless*.

Quais as soluções correctivas?

Está em voga a instituição de autoridades com capacidade de *enforcement*, ou seja capacidade de fazer cumprir a lei. A questão é complexa porque, como já foi referido neste Colóquio, é possível a um servidor em Portugal fazer circular uma mensagem entre o Brasil, a Coreia do Sul e as ilhas Cayman e retê-la de volta. Há problemas de coordenação e âmbito de aplicação, mas a solução correctiva passa pela capacidade de aplicar uma sanção pela prática de um delito.

Que técnicas de solução correctiva foram postas em prática?

Foram duas: a chamada solução de reversão em que no caso de recepção de uma mensagem electrónica indesejada de teor comercial se identifica o remetente e se apura se cumpriu ou não as normas de etiquetagem.

Acontece que tal solução provou ser totalmente ineficaz porque é muito fácil falsificar os remetentes e os provedores de serviços de correio electrónico não têm capacidade, nem interesse, em conservar por um prazo superior a 20 dias

– definido pelos próprios provedores – os imensos registos de actividades do sistema, os chamados *logs*.

A solução oposta à reversão tem-se, no entanto, mostrado mais eficaz.

Nos Estados Unidos a *Federal Trade Commission* mantém, recorrendo ao seu próprio orçamento, contas correntes abertas de forma a conhecer as reais dimensões das fraudes. Como um dos muitos hipotéticos clientes a Comissão pode apurar os sistemas de pagamento e seguindo a pista do dinheiro identificar quem está por detrás destes tipos de actividades fraudulentas.

Termino aqui a minha comunicação e, propositadamente, não apresento quaisquer conclusões. Como dizia no início estamos perante “um desafio constante” e seria mera presunção avançar com conclusões face aos problemas actuais e às questões que o futuro nos reserva.

Muito obrigado.

III PAINEL

Luís Barroso

Vogal da CNPD

AS TECNOLOGIAS EMERGENTES E A PRIVACIDADE

Muito boa tarde.

Esta minha intervenção baseia-se nos problemas colocados pelas tecnologias emergentes. Propositadamente, não escolhemos o nome novas tecnologias porque estas tecnologias que vão ser aqui referidas estão muito longe, algumas delas, de serem novas. Pura e simplesmente, devido a alguns desenvolvimentos tecnológicos, estão agora na ordem do dia.

Por exemplo, não é de hoje que se fala de videovigilância, mas, agora, os problemas da videovigilância colocam-se com maior cuidado. Não é de hoje que falamos dos problemas das consultas cruzadas, mas, actualmente, há dispositivos, há técnicas que se apoiam em tecnologias que possibilitam ou, se quiserem, potenciam os eventuais perigos que podem advir da sua utilização.

O Grupo da Protecção de Dados Pessoais no plano europeu discutiu já este ano, no mês passado, alguns temas que têm a ver, directamente, com aquilo que nos traz a este ponto da ordem do Colóquio. Trata-se, precisamente, da preocupação e necessidade de acompanhar e de monitorar os desenvolvimentos em curso. Foram referidas designadamente algumas dessas tecnologias que deveriam merecer mais atenção e despertar maior preocupação aos comissários de protecção de dados europeus: a radiofrequência; as ferramentas próprias para na Internet, ou com o auxílio de meios electrónicos, poder

fazer-se prova da propriedade intelectual; a localização, serviços de localização, utilizando diferentes tipos de tecnologia. Ou seja, desenvolvimentos específicos que foram pensados e começaram a ser aplicados e testados, como aqui foi referido pelo Dr. Diogo Vasconcelos por via de algumas experiências implementadas em Portugal.

Uma questão que se levanta de alguns anos a esta parte, mas que, agora, começa a assumir uma maior acuidade diz respeito aos tratamentos de dados envolvendo dados genéticos e dados biométricos. É impossível num quarto de hora abarcar esta panóplia de tecnologias e os respectivos diferentes desenvolvimentos. Assim sendo, vou apenas focar alguns dos aspectos que, em princípio, merecem a preocupação e a atenção das autoridades de protecção de dados no contexto europeu. Depois, espero que reste algum tempo para podermos debater os aspectos que vou referir e as demais vertentes que, porventura, achem pertinentes.

Começo por algo que já foi referido no nosso Colóquio e que tem a ver com a generalização dos meios de videovigilância e, também, de audiovigilância. Julgo que a assistência tem presentes os perigos reais que as tecnologias de videovigilância e audiovigilância podem acarretar, mas queria alertar para alguns aspectos particulares.

Primeiro, abordemos a vigilância dissimulada do som, das conversas. Dissimulada ou não esta vigilância existe. Eu sou professor, além de ser vogal da Comissão, há já largos anos na universidade e não é uma nem duas vezes que um aluno vem ter comigo – geralmente estrangeiros do projecto Erasmus – pedindo para gravar aula. Eu importar, importo-me. Sinceramente que me importo. Uma pessoa fica sempre menos à vontade, mas disponibilizo-me para ele gravar a intervenção e, depois, em casa, ou no seu país, ou onde quiser, poder estudar melhor aquela matéria. O aluno teve, no entanto, um cuidado prévio: pediu-me o consentimento. E eu dei-lhe. Mais ou menos contrariado mas, certamente, com boa vontade de o ajudar, concedo que ele grave a minha intervenção. O meu problema – a minha intervenção ou a minha aula – surge quando essa gravação ocorre sem eu ter dado o consentimento ou,

III PAINEL

outras vezes, quando digo explicitamente que não admito qualquer gravação e essa gravação ocorre.

De vez em quando vemos nalgumas televisões estrangeiras reportagens que nos alertam para este tipo de problemas. Infelizmente, não é só no estrangeiro que estes problemas acontecem. Em Portugal temos também presente o perigo de se proceder à audiodivulgação sem serem cumpridos os requisitos indispensáveis para qualquer tratamento de protecção de dados, nomeadamente a notificação à Comissão Nacional de Protecção de Dados, e, depois, os restantes procedimentos: o livre consentimento do titular dos dados, o direito de informação, de oposição, etc.

Todos nós já ouvimos falar de mensagens multimédia e, eventualmente, a generalidade dos presentes já utilizou mensagens MMS. Julgo que também já todos os presentes já ouviram falar da 3.^a geração – que não é para amanhã, é para hoje – dos telemóveis. Por vezes pensamos estar a falar do futuro, mas, não, o futuro é hoje.

Os sistemas de MMS são o mais vulgar possível. As minhas filhas usam o MMS como eu nunca pensei utilizar algum dia. Noutro dia uma filha minha contou-me uma coisa que me fez pensar. Quando dois colegas dela estavam a debater se determinado rapaz tinha dito algo sobre certa moça, uma rapariga – mais inteligente do que as restantes ou mais esperta, se quiserem – por sua livre iniciativa deixou a amiga ouvir aquilo que o outro rapaz tinha dito sobre ela na sua ausência. Como? Como um telemóvel semelhante a este, normalíssimo, que, sem qualquer aviso prévio, permite que seja feita gravação de conversas, de imagem, ou, então, capturar a imagem.

Ora, esta preocupação não é só nossa. A nossa congénere australiana já debateu este problema. Em Itália surgiu um caso num tribunal que tem a ver com a divulgação de imagens via MMS. Na última reunião que houve do Grupo Internacional das Telecomunicações, em Abril passado, na Argentina, voltou a ser debatido este problema. Houve sugestões simples para tentar ultrapassar a questão da privacidade. Algumas nem seriam boas sugestões, mas facto é que se pensou e debateu o assunto.

Qual foi a sugestão? Já não sei qual foi o país que propôs o alerta de bip. Cada vez que eu quisesse gravar uma imagem ou um som soava um bip. Resolvia o problema, mas criava outros. Julgo que a utilização desse som, desse aviso sonoro, pode levantar problemas. Por exemplo, se eu estiver num local onde esses sons não são permitidos. Há países que foram mais longe do que aquilo que foi proposto nessa reunião do Grupo Internacional de Telecomunicações. O Japão, por exemplo, já tem legislação sobre o assunto que determina o número máximo de decibéis que o som a ser emitido pode ter. Já falámos de audiovigilância.

Noutro nível, num plano global, a vigilância por satélites espões já não é exclusivo, nem de perto nem de longe, dos governos ou das autoridades públicas. Há empresas comerciais envolvidas no negócio. Ainda ontem um familiar meu começou a dizer que o *Google* já se envolvera no negócio de uma empresa de satélites. Hoje em dia, os satélites que existem disponíveis na Internet para consulta, para treino, para demonstração, permitem no limite, se aproveitarmos todas as suas potencialidades, identificar endereços específicos, em áreas onde esse levantamento já foi executado. O *Keyhole Pro* é, por exemplo, um *software* que utiliza uma rede de satélites já bastante antiga, nem sequer é muito moderna. Em Portugal, não temos esta informação carregada, mas noutros países, como, por exemplo, nas áreas urbanas dos Estados Unidos, essa informação é de fácil acesso.

Se alguém quiser ver com que velocidade se consegue localizar um determinado ponto no globo terrestre – qualquer que ele seja – pode tentar pesquisar na Internet algum produto similar. Ficará com uma ideia aproximada, se quiser entrar no negócio que envolve bastante dinheiro, das potencialidades em termos de espionagem sem grande custo. Isto levanta interrogações.

Lidamos diariamente com processos que envolvem a videovigilância, tentamos – e, julgo eu, com bastante sucesso – regulamentar essa actividade, impondo as normas que se têm de cumprir. Por vezes, pura e simplesmente proibimos certas práticas que consideramos despropositadas ou atentatórias da liberdade e privacidade dos cidadãos, dos titulares dos dados, mas ficamos sempre aquém daquilo que, eventualmente, a nossa missão exigiria.

III PAINEL

Ficamos sempre aquém, mas não é por isso que pensamos seguir no mau caminho. Não, estamos a tentar regulamentar aquilo que no plano nacional pode ser regulamentado. Temos ainda presente que este tipo de dificuldade, de obstáculo à privacidade, tem que ser sempre abordado e resolvido no plano global. Não por acaso está aqui também o nosso colega da Agência Espanhola de Protecção de Dados e que o presidente da Comissão Nacional de Protecção de Dados ainda há pouco referiu que se pensava antes que era muito uma reunião por ano de âmbito internacional agora tem claro que é necessário cada vez mais olear estes mecanismos de âmbito internacional. Temos, portanto, consciência dos limites da nossa actuação.

Gostaria, ainda de deixar como tópico para discussão o *Electronic Numbering*. O ENUM, sucintamente, algo que vai juntar num só número, ou se quiserem, numa só cadeia de caracteres, o nosso número telefónico e o nosso e-mail. Se o meu número de telefone for 123456789 e o e-mail for cnpd.pt, por exemplo, qualquercoisa@cnpd.pt, o nosso ENUM será algo que, em vez de ser 123456789, será 987654321 incluindo o nosso domínio no mail.

O ENUM permite a comunicação entre utilizadores de serviços de comunicações electrónicas de diferentes tipo, através de diversos meios, como voz, fax, e-mail, etc., tendo como referência para comunicação e acesso apenas os números de telefone. É muito útil, mas também tem muitos perigos.

Reparem que, hoje em dia, já há resoluções de âmbito europeu e de âmbito internacional, por exemplo, para vigiar a utilização dos dados que estão nas listas de endereços da Internet, as chamadas *Wise databases*. Existe regulamentação própria e normas específicas para gerir a informação constante das listas telefónicas públicas, nomeadamente as listas telefónicas electrónicas que permitem a consulta cruzada. Isto é, eu posso nalguns casos indicar um determinado número de telefone e obter informação sobre o titular da conta, o dono desse telefone, e colher alguma informação anexa.

Uma tal base de dados não pode ser regulamentada no plano nacional, é impossível. Isto é, tem de existir um ponto único em todo o globo que agregue a informação, embora, depois, distribuída pelos vários países, sobre todos os

cidadãos que sejam subscritores do Enum. Isto é, todos os cidadãos que tenham número de telefone e um endereço electrónico.

Só para não dizerem que eu estou a ser um bocadinho faccioso, que só estou referir os perigos, indico algumas vantagens que tem este serviço. Por exemplo, com o mesmo número fico a poder ser contactável no meu móvel, no meu telefone do trabalho, no meu telefone de casa. Se quiser recebo as chamadas para os telefones da minha mulher num telefone portátil. As chamadas para os telefones da universidade, do meu trabalho, naquele telefone específico que está na minha secretária e por aí fora. As vantagens são consequentemente boas, mas existem muitos perigos.

É sobre esses perigos, para já, queria que pensássemos um pouco porque se faço o reencaminhamento das chamadas posso saber, também, onde é que está um determinado telefone, qual o paradeiro do utilizador dum determinado endereço electrónico.

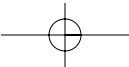
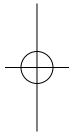
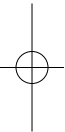
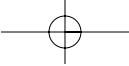
Uma referência, ainda, à radiofrequência. Presentemente, é possível através de dispositivos emissores seguir por todo o mundo um qualquer objecto, animal ou pessoa. Enquanto forem só objectos isolados, nada a objectar. Por exemplo, empresas como a *Benetton*, a *Marks & Spencer*, seguem o trajecto de determinado artigo desde até à sua ida para armazém, posterior comercialização no supermercado, na loja. É assim possível saber quando determinado produto chegou ao armazém, a data de venda, e gerir as existências. Surgem outras potencialidades como frigoríficos ligados à Internet que permitem, quando os produtos têm agregada tecnologia de radiofrequência, automatizar o processo de gestão das existências.

O tempo escasseia para as questões tão vastas que levantam as convergências de todas estas tecnologias, como a radiofrequência, a videovigilância, o número electrónico único. Isto é, os perigos da tecnologia de informação combinados com os perigos da biotecnologia, com os perigos da nanociência que trabalha num grau de miniaturização microscópico impossível de captar a olho nu. A conjugação de todas estas tecnologias eleva à potência muito alta os perigos que enfrenta, hoje em dia, a privacidade dos cidadãos.

III PAINEL

Concluo com uma ideia. A segurança e a privacidade podem ser complementares e podem ser concorrentes. Podem ser complementares porque para garantir a minha privacidade tenho, por vezes, de adoptar medidas de segurança. Esteve aqui um especialista na área de segurança que explicou essas medidas. Por outro lado, se as medidas de segurança inibirem ou puserem em causa a minha liberdade ou a minha privacidade, aí, tenho que pensar duas vezes.

Dou lugar ao debate.



III PAINEL

Debate

Moderador

Eduardo Campos

Vogal CNPD

Creio que depois deste painel fica mais compreensível a existência de zonas de não direito de que se falou hoje de manhã. Mas, se por acaso, sobretudo aos juristas, poderá custar admitir zonas de não direito, creio que este painel foi eloquente acerca da necessidade de conceber novos paradigmas de direito, diferentes dos paradigmas clássicos.

Em resposta às três intervenções poderia deixar uma pista no sentido de que esse novo paradigma de direito, diferente do paradigma clássico, englobasse o direito normativo, a actuação do estado, a actuação das empresas, a sua responsabilidade com a comunidade e o aprofundamento da cidadania.

É um tema muito longo vasto e, passemos, portanto, às questões.

Paula André

Instituto Nacional de Engenharia, Tecnologia e Inovação

Boa tarde, sou Paula André do INETI.

Os sistemas de informação são úteis, de facto, não há dúvida nenhuma, mas levantam perigos problemas. Uma questão levantada pelo Dr. Luís Barroso

prende-se, precisamente, com os sistemas de informação geográfica. São úteis, estão associados a bases de dados. É, portanto, inquestionável, a sua utilidade. Agora deixo aqui uma pergunta acerca da protecção de dados pessoais. Diversas empresas públicas, e não só, têm sistemas de informação geográfica muito bem montados, portanto, é matéria actual, em termos nacionais. Depois, isso está integrado dentro de sistemas de informação geográfica europeus e, devido à globalização, de todo o mundo. Pergunto, portanto, se a Comissão está a proteger esses dados quer pessoais quer geográficos? Qual é o papel da Comissão nessa fundamental protecção de dados?

Moderador

Muito obrigado. Não sei se alguém pretende colocar alguma questão conjuntamente com esta ou interligada?

Interveniente não identificado

Consideremos o seguinte exemplo: na Inglaterra não recolhem dados sobre pessoas que não trabalhem, não paguem impostos, mas é importante recolher informação mesmo que alguém esteja ilegal num determinado país e, depois, decidir juridicamente o que fazer.

Não se trata de expulsar pessoas em situação ilegal. Trata-se de recolher dados sobre toda a gente e o importante é ter essa informação segura.

Achei interessante a observação do Dr. Álvaro Canales de que quando a Internet foi construída se partiu do princípio de que os seus utilizadores seriam pessoas honestas, afinal, tratava-se de cientistas. Na verdade os protocolos não evoluíram, portanto, não há certificados de autenticação, por exemplo, só agora começam a surgir, mas a tecnologia não evoluiu para compensar esse ponto.

Outra coisa ponto em relação à privacidade da informação. Se me roubam a minha identidade, se roubam o meu cartão de crédito em casa e gastam di-

III PAINEL

nheiro, estragam-me o historial de crédito e não posso modificar, não posso corrigir o meu historial. Eu não tenho controlo sobre a minha informação, mesmo que esteja errada, não a posso corrigir. Isso é ainda mais grave.

Terceiro ponto. Foi referida a falta de segurança dos computadores nos dois lados, questão deveras importante. O meu computador é inseguro porque vem inseguro da *Microsoft*. Eu não tenho controlo sobre isso. Não é? O *software* não é meu, não fui eu que o fiz. O computador receptor também não é seguro, não tenho nenhuma garantia que seja seguro. Portanto, a não ser que haja níveis de segurança – e os Estados Unidos têm níveis de segurança para computadores do máximo ao mais baixo – a única coisa que tenho por segura é a comunicação entre os dois computadores.

É uma questão que vai ter repercussões mesmo em termos comerciais. O consumidor vai perder a confiança no computador porque não é a ligação do computador a outro que é vulnerável é o seu próprio computador que se encontra vulnerável. Pode até acontecer que reserve um bilhete de cinema, utilizando um cartão de crédito, e que seja roubado porque o computador a que acedi para a compra está vulnerável. Que certezas posso ter sobre os níveis de segurança?

Moderador

Muito obrigado.

Interveniente não identificado

Achei muito interessante uma observação que foi feita no sentido de realçar que se pode alertar as pessoas, expor-lhes a informação necessária, mas que é bem mais difícil alterar atitudes culturais. É, pois, necessário investir nessa área.

Moderador

Muito obrigado. Dou a palavra ao professor Canales.

Álvaro Canales

Agência Espanhola de Protecção de Dados

Os cidadãos têm dificuldade em compreender as condições em que os operadores telefónicos oferecem os seus serviços. Provavelmente porque desconhecem que o telefone móvel é um sistema de localização. Quando se apercebem desta circunstância ficam apreensivos pelo facto de poderem ser localizadas através das redes móveis, mas o mesmo ocorre com as radiofrequências.

Ao comprar um sistema de radiofrequência pretendo garantir a segurança de um veículo e não que tal serviço venha a ser utilizado para outras finalidades como o escrutínio dos meus hábitos de consumo ou dos padrões de gastos da minha família.

Ora, prosseguindo o raciocínio, os operadores telefónicos não devem utilizar os dados de localização – necessários à prestação do serviço – para finalidades distintas das que foram contratadas e autorizadas pelo cliente. É essa a razão porque a legislação espanhola penaliza o operador telefónico pela localização sem consentimento do cliente não só pela Lei de Protecção de Dados, mas, também, em virtude da Lei Geral de Telecomunicações.

O conceito genérico cinge-se a isto: o contrato do cliente com um operador de telecomunicações, o uso do telemóvel, tem a ver exclusivamente com os termos da prestação do serviço. Ao facultar a terceiros os dados da localização do titular do telemóvel sem sua expressa autorização o operador está a infringir a lei e sujeita-se a penalizações.

Luís Barroso

CNPD

Obrigado pelas perguntas que colocaram. Vou responder à questão relativa à utilização da informação geográfica. É um tema que deve ser também discutido a nível internacional e que gostava de ver debatido na próxima reunião em Abril, no nosso país do Grupo Internacional de Telecomunicações. Cada

III PAINEL

país sugere temas para discussão e Portugal vai propor, precisamente, a questão do tratamento de informação pessoal em bases de dados de informação que conjugam esses dados pessoais com bases de dados geográficas.

Moderador

O Eng.º Filipe Custódio vai prestar alguns esclarecimentos.

Filipe Custódio

Especialista em segurança informática

Respondendo a uma das questões que penso que aqui foi colocada gostaria de dizer que na minha apresentação, naturalmente breve, não quis deixar a ideia que vivemos num mundo muito inseguro e que o melhor é pôr-nos todos debaixo de uma pedra e escondermo-nos.

A segurança é como a qualidade: nunca há suficiente e nunca é total. Portanto, o facto dos computadores terem, muitas vezes, uma segurança fraca face a um referencial que devia e pode ser melhor, é uma advertência. Aliás, neste aspecto da segurança acredito no mercado. Os problemas de segurança, relativamente aos computadores pessoais já existem há muito tempo, mas só começaram a assumir relevância pública como os números preocupantes divulgados nos últimos dois, três anos. Ainda é cedo, portanto, e o mercado vai responder se tiver condições para funcionar.

Ou seja, por hipótese, se a *Microsoft* não faz sistemas operativos mais seguros, então as pessoas mudam para *Macintosh*. Caso a *Apple* não tenha, também, o mesmo cuidado, as pessoas mudam para *Linux*. Se o *Linux* continuar a ter problemas, as pessoas usam outro tipo de dispositivos para aceder à Internet. Se o *Internet Explorer*, por exemplo, ainda tem problemas de segurança, foi porque, durante muito tempo, a *Microsoft* não deu atenção suficiente a essas questões. O que é que aconteceu? Há dois anos o *Internet Explorer* tinha 98% de *share* nos *browsers*. Era o domínio absoluto. Dominaram a *Netscape*. Con-

COLÓQUIO PROTEGER OS DADOS PESSOAIS

seguiram colocar a *Netscape* fora do mercado. Ora, essa situação alterou-se e em matéria de navegadores o *Netscape Navigator* recuperou quota de mercado. Porquê? Porque os consumidores estão alerta e quando deparam com um produto que não lhes dá garantias de segurança escolhem outro mais seguro.

Moderador

Muito obrigado. Não havendo mais nenhuma questão, nem mais nenhuma observação, gostava só de lembrar que as conclusões deste colóquio serão apresentadas no site da Comissão Nacional de Protecção de Dados. Queiram fazer o favor de o consultar.

Muito obrigado e muito boa tarde.