VIEIRA DE ALMEIDA
& Associados Sociedade de Advogados, R L

JANEIRO 2008

NEWS

PRIVACIDADE E DADOS PESSOAIS

Índice

PRIVACIDADE

Na agenda da sua empresa?

Actualmente, qualquer organização deve ter em consideração a legislação que regula o tratamento de dados pessoais e a privacidade.

Sempre que uma empresa dispõe de dados como o nome, a morada, o telefone, endereço de e-mail, imagens ou qualquer outro elemento relativo a pessoas individuais (sejam clientes, trabalhadores ou fornecedores), usa sistemas de videovigilância, efectua a gravação de chamadas telefónicas, etc, independentemente do sector de actividade em que actua (banca, seguros, telecomunicações, farmacêutico, cuidados de saúde, conteúdos e audiovisuais, entre outros), então é essencial conhecer as regras que regulam o tratamento de dados pessoais, saber quais são os riscos do seu incumprimento e estabelecer uma política de tratamento de dados pessoais.

As questões relacionadas com o tratamento de dados pessoais e a privacidade têm ganho, nos últimos anos, uma importância crescente. Contudo, algumas empresas não estão ainda conscientes das consequências que o incumprimento da legislação de dados pessoais poderá ter para a sua actividade e para os seus responsáveis. Tais consequências, embora facilmente evitáveis, são bastante nefastas – além da aplicação de pesadas coimas, o incumprimento da legislação de privacidade pode fazer incorrer os gestores das organizações em responsabilidade criminal, sobretudo se estiverem em causa dados sensíveis. Mas não ficamos por aqui: violar a lei de protecção dos dados pessoais tem outros "custos escondidos", nomeadamente de reputação e imagem, com impacto relevante junto dos clientes da empresa.

O Núcleo de Privacidade da VdA tem vindo a trabalhar com diversas empresas, dos mais variados sectores de actividade, avaliando o nível de *compliance* da empresa e prestando aconselhamento jurídico especializado que permita evitar (ou reduzir substancialmente) os riscos de incumprimento da lei.

O *know-how* e o *track record* da equipa têm sido uma mais-valia na definição de regras de *compliance* que estejam em linha com o modelo de negócio de cada cliente. De facto, neste domínio, *"there is no one size fits all"*. Cada organização, atendendo ao sector de actividade em que actua e às especificidades da sua estrutura, deve assim definir regras adequadas que permitam assegurar que, no dia a dia, os seus colaboradores cumprem a legislação de protecção de dados pessoais.

Neste contexto, vimos igualmente prestado aconselhamento jurídico na "estruturação" de projectos em que as bases de dados assumem uma importância fundamental, contribuindo assim para acrescentar valor aos projectos desta natureza.

Temos, deste modo, trabalhado para que os clientes coloquem na sua agenda as questões de privacidade, reduzindo o risco de incumprimento da lei neste domínio.

Esta *newsletter,* que terá uma publicação semestral, procura ser mais um contributo nesse sentido.

Margarida Couto, Magda Cocco, Muriel Faden da Silva, Leonor Pimenta Pissarra, Patrícia Sousa Lima, Inês Antas de Barros, Leonor Vale de Castro, Mónica Chambre e Joana Almeida e Sousa membros do Núcleo de PRIVACIDADE da Vieira de Almeida & Associados.

O "BIG GOOGLE" DA INTERNET

Grupo 29 preocupado com os dados recolhidos pelos motor de busca

Índice

O Grupo de Trabalho de Protecção de Dados do Artigo 29 ("GT do Artigo 29"), composto pelas comissões de protecção de dados pessoais dos diversos Estados Membros, remeteu, em meados de 2007, uma carta ao responsável pela privacidade do motor de busca Google, alertando para o facto de a política de privacidade desta empresa não respeitar a legislação aplicável em matéria de protecção de dados pessoais.

Em particular, o GT do Artigo 29 considerou que o período de conservação, pelo Google, de informação sobre as pesquisas efectuadas pelos internautas é excessivo, sobretudo tendo em consideração que o Google mantém tais dados por tempo indeterminado.

Esta posição surge numa altura em que o Google foi considerado, num estudo publicado pela *Privacy International*, como "hostil em relação à privacidade", ocupando um dos últimos lugares do *ranking*.

Perante tal alerta, o Google admitiu rever a sua política de privacidade, nomeadamente através do estabelecimento de um período máximo de conservação dos dados relativos às pesquisas efectuadas pelos utilizadores do motor de busca. O Google referiu ainda que apenas guarda tais dados para melhorar a qualidade dos serviços, manter a segurança e evitar fraudes.

A guerra aberta contra o Google, tendo como pano de fundo a (falta de) protecção da privacidade, assumiu tal dimensão, que levou esta empresa a disponibilizar recentemente um vídeo *on-line*, no qual explica a sua política de privacidade. Este vídeo poderá ser acedido em http://googleblog.blogspot.com/2007/09/search-privacy-and-personalized-search.html.

A polémica está, no entanto, longe de estar resolvida, aguardando-se que a Comissão Europeia tome uma posição a qualquer momento em relação a este *big brother* da Internet.

O que quer que venha a ser decidido nesta matéria, afectará não apenas o Google, como todos os motores de busca que armazenem dados relativos às pesquisas efectuadas pelos internautas, pelo que os desenvolvimentos desta novela são aguardados com expectativa pela ciber-comunidade.

"PRIVACY BREACH"- COMO AGIR?

Índice

Os casos de divulgação não autorizada de dados pessoais (*privacy breach*) têm sido uma realidade crescente nos últimos anos. Estes casos são fruto tanto de acidentes, como de acções dolosas de colaboradores das empresas ou de terceiros. Nos anos recentes, no Reino Unido, 20% dos bancos, 18% das empresas gestoras de cartões de crédito, 13% dos organismos da administração pública e 9% das empresas de saúde comunicaram casos de desvio ou de divulgação indevida de dados pessoais.

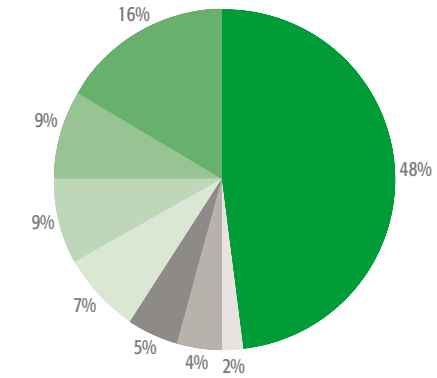
Em Portugal, não há números oficiais, mas a realidade poderá não ser muito diferente. É assim essencial que as empresas adoptem medidas que permitam evitar os casos de acesso indevido ou de divulgação de dados pessoais, definindo regras de segurança sobre o acesso aos dados, a utilização de computadores portáteis, a armazenagem de dados pessoais em *pens* e CDs, ou sobre o seu envio para o exterior. Mas, quando a prevenção falha e ocorre uma situação de acesso indevido, importa ter um segundo nível de protecção, que permita controlar ou reduzir os danos, nomeadamente os de imagem, de difícil reparação. E assim, sempre que uma situação de *privacy breach* é identificada, há que adoptar medidas que permitam controlá-la.

O primeiro passo é a realização imediata de uma auditoria, que permita avaliar a situação, sem contudo destruir provas relevantes para o apuramento dos factos. Essa avaliação deverá ter em conta, designadamente, os dados pessoais envolvidos, a causa da violação, as pessoas afectadas e os danos que podem decorrer da violação. A designação de um responsável, que controle, nomeadamente, a comunicação com os *media* e com as pessoas afectadas pela violação, é também fundamental.

A notificação da ocorrência às entidades competentes pode ser vantajosa e em alguns casos é mesmo obrigatória. Importará também avaliar se as pessoas afectadas devem ser notificadas. Tal decisão deve ter em consideração diversos factores, tais como a existência de obrigações contratuais de notificação e a possibilidade de os eventuais afectados evitarem ou atenuarem os potenciais danos.

Uma coisa porém é certa – se nem sempre é possível evitar a ocorrência de uma situação de *privacy breach*, a existência de uma política de *damage control* poderá fazer toda a diferença numa situação de crise.

PRIMARY CAUSES OF A PRIVACY BREACH



Fonte: "2007 Annual Study: U.S. Cost of a Data Break", November 2007– "The Ponemon Institute, LLC"

OUTSOURCING

Os dados dos seus clientes e colaboradores estão em boas mãos?

Índice

É cada vez mais comum as empresas recorrerem ao *outsourcing* de algumas das suas actividades, em regra, aquelas que não correspondem à sua área *core*. O recurso ao *outsourcing* permite às empresas centrar a sua atenção no desenvolvimento do seu negócio, sem desperdiçar recursos em áreas que não são prioritárias.

A opção pelo *outsourcing* traz benefícios óbvios para a empresa cliente (i.e. a empresa que "externaliza" a sua actividade), nomeadamente em termos de eficiência económica. Mas a verdade é que também pode ter associados alguns riscos, que nem sempre evidentes. Com efeito, o recurso ao *outsourcing* envolve frequentemente o acesso e tratamento, pela empresa que passa a assegurar os serviços, de dados de colaboradores e clientes da empresa que decide "externalizar" a sua actividade. É o caso, por exemplo, de diversas modalidades de *Business Process Outsourcing* (BPO) como o *outsourcing* de gestão de sistemas de informação, de serviços telefónicos de atendimento ao público que operam através de *call centers* (ou mesmo de *contact centers* com formas de contacto mais sofisticadas, como Internet ou e-mail) e cuja gestão implica o acesso a dados pessoais, por vezes de natureza sensível, por parte da empresa que presta o serviço. É inegável que a informação pessoal tem um enorme valor e consequentemente é um "bem apetecível" que deve ser protegido em qualquer circunstância e em particular no âmbito do recurso a serviços de *outsourcing*.

É conhecida a história de um banco inglês que viu dados dos seus clientes (relativos a cartões de crédito e contas bancárias, entre outros) serem vendidos por um trabalhador de um *call center* situado na Índia, a um jornalista do "*The Sun*". Neste caso de venda de dados, a autoridade de protecção de dados pessoais do Reino Unido – o *Information Commissioner's Officer* (ICO) – determinou que as empresas que recorrem ao *outsourcing* são responsáveis pela escolha do prestador de serviços que contratam e permanecem responsáveis por falhas de segurança no tratamento da informação. O ICO recomendou igualmente que fossem realizadas auditorias regulares aos prestadores serviços contratados, por parte das entidades responsáveis pelo tratamento de dados.

Também face à lei portuguesa a responsabilidade pelo tratamento de dados pessoais permanece na empresa, em particular quando, como é regra, é esta que define as finalidades e os meios de tratamento dos dados ou no interesse de quem os dados são tratados. Nesta perspectiva, a empresa que presta o serviço será uma mera "subcontratada", já que tratará os dados por conta e sob as indicações da empresa cliente. Ora, porque as obrigações legais aplicáveis ao tratamento de dados, incluindo a responsabilidade última sobre o tratamento, recaem sobre o responsável pelo tratamento – em regra a empresa cliente – convém conhecer o quadro legal aplicável e assegurar o seu cumprimento.

Desde logo, para além do consentimento dos titulares para o tratamento dos respectivos dados pessoais, a empresa que recorre ao *outsourcing* deve assegurar o cumprimento de uma série de formalidades, incluindo, por exemplo, (i) a legalização do tratamento junto da Comissão Nacional de Protecção de Dados (podendo a legalização corresponder a uma mera notificação ou a um pedido de autorização, consoante, por exemplo, os dados a tratar sejam sensíveis ou não sensíveis ou haja ou não operações de interconexão de bases de dados), (ii) no pressuposto de que a empresa que presta o serviço é uma mera subcontratada, deve ter-se o cuidado de se prever no contrato de *outsourcing* regras detalhadas sobre o tratamento de dados pessoais, incluindo, por exemplo, a proibição de tratamento dos dados para outros fins que não os previstos no contrato e (iii) pode ser ainda importante prever no contrato de *outsourcing* que a empresa que presta o serviço será responsável perante a empresa cliente caso venha a tratar dados em violação do previsto no contrato, de forma a que, em caso de quebra de procedimentos de segurança, a empresa cliente possa exigir da empresa que lhe presta o serviço uma indemnização pelos danos incorridos com a violação das normas relativas ao tratamento de dados pessoais.

É conhecida a história, de um banco inglês que viu dados dos seus clientes (relativos a cartões de crédito e contas bancárias, entre outros) serem vendidos por um trabalhador de um call center situado na Índia a um jornalista do "The Sun".

Importa ainda não esquecer que existem algumas limitações à transferência de dados pessoais para países situados fora da União Europeia, em particular para países que a Comissão Europeia não considera que asseguram um nível de protecção adequado em matéria de privacidade. Se a empresa que presta o serviço estiver situada num país considerado "inseguro" em matéria de privacidade, a transferência de dados só poderá realizar-se caso seja obtido o consentimento inequívoco da pessoa a quem os dados respeitam. Como alternativa, poderão ser reflectidas no contrato de *outsourcing* as cláusulas aprovadas pela Comissão aplicáveis à transferência de dados pessoais para subcontratados estabelecidos em países terceiros. Estas são apenas algumas das medidas necessárias para garantir o cumprimento da lei em matéria de dados pessoais e minimizar os riscos de responsabilização das empresas que decidem recorrer ao *outsourcing*. A indiferença face às mesmas pode resultar em prejuízo financeiro (decorrente da aplicação de coimas) e até mesmo em responsabilidade criminal, para além de poder repercutir-se negativamente na reputação da empresa e acarretar a perda de clientes, por quebra de confiança no serviço. Aqui aplica-se a máxima "mais vale prevenir que remediar" !

Índice

Retenção de Dados – quem paga a factura?

Foi no passado dia 4 de Janeiro aprovada no Parlamento a Proposta de Lei que transpõe para a ordem jurídica portuguesa a Directiva que impõe a conservação dos dados gerados nas redes de comunicações electrónicas, conhecida por "Directiva Retenção". A partir da publicação da Lei, os prestadores de serviços de telecomunicações (incluindo os operadores móveis e os ISPs), serão obrigados a "reter", durante um ano, um volume imenso de informações relativas às comunicações efectuadas através das suas redes.

EUA e UE ...ainda o efeito "Bin Laden"

Desde o 11 de Setembro que os EUA e a UE têm mantido negociações sobre a transferência de dados pessoais contidos nos registos de identificação dos passageiros aéreos com destino ou origem nos EUA. Nos termos de um novo acordo recentemente alcançado, a UE deverá assegurar que as transportadoras aéreas que efectuem voos internacionais de passageiros com destino ou origem nos EUA disponibilizem ao Departamento da Segurança Interna dos Estados Unidos (DS) os dados dos registos de identificação dos seus passageiros.

Obrigatório limpar o disco!

Um estudo desenvolvido por um grupo de investigadores da Universidade de Glamorgan (País de Gales), no âmbito de um projecto de recuperação de discos daquela instituição, descobriu que um significativo número de discos rígidos vendidos em segunda mão, em feiras de informática e sites de leilões, continham dados pessoais e informação confidencial. Os investigadores afirmam que é possível encontrar em circulação um alarmante nível de informação confidencial, não tendo ainda as empresas adoptado procedimentos destinados a assegurar que a mesma é efectivamente removida antes de os discos rígidos serem postos à venda.

Controlo de e-mail e Internet

O controle do uso da Internet e de envio de e-mails pelos trabalhadores é uma preocupação cada vez maior no seio das empresas, as quais optam pela instalação de sistemas cada vez mais sofisticados. Alguns hospitais norte-americanos instalaram sistemas que analisam o conteúdo dos e-mails antes de estes serem efectivamente enviados. Assim, cada vez que um colaborador envia um e-mail, a mensagem é reencaminhada para uma aplicação instalada no sistema central do hospital. Este software analisa o conteúdo do e-mail, procurando informação confidencial e dados sensíveis, sendo as mensagens reencaminhadas para o administrador de segurança.

Controlo de e-mail provoca despedimento ilícito

Num acórdão recente, o Supremo Tribunal de Justiça (STJ) considerou ilícito o despedimento de um trabalhador, em virtude de o empregador ter acedido a mensagens de correio electrónico do trabalhador, de natureza pessoal. O STJ considerou que ao aceder ao e-mail do trabalhador, que se encontrava de férias, o empregador violou o direito de reserva da intimidade da vida privada e a confidencialidade da sua correspondência, tendo condenado a empresa a pagar uma indemnização e a reintegrar o trabalhador no seu posto de trabalho.

Escândalo no Reino Unido

Quando o Governo do Reino Unido foi forçado a admitir terem sido extraviados dados pessoais sensíveis (incluindo números de contas bancárias) de mais de 25 milhões de cidadãos britânicos, pertencentes ao departamento do governo responsável pela colecta de impostos (*Her Majesty´s Revenue of Customs*), rebentou um escândalo sem precedentes que danificou gravemente a imagem do Governo e provocou demissões ao mais alto nível. Os dados, que foram enviados sem encriptação, por correio, até à data não foram localizados, podendo o seu extravio pôr em perigo a segurança das contas bancárias dos ingleses e ameaçar a sua privacidade.

Coordenadora do Núcleo de Privacidade da VdA recebe prémio

Magda Cocco foi um dos sete advogados portugueses distinguidos pela Iberian Lawyer na primeira edição do "*Forty under Forty Awards*" da Iberian Lawyer, na qual foram eleitos os melhores 40 advogados com menos de 40 anos, a trabalhar na Península Ibérica. A VdA foi a única firma Portuguesa em que dois advogados receberam esta distinção, tendo o outro prémio sido atribuído ao líder da área de fiscal, Tiago Moreira.

Vieira de Almeida & Associados - Sociedade de Advogados, RL | www.vda.pt
Av. Duarte Pacheco, 26 - 1070-110 Lisboa - Portugal | lisboa@vda.pt
Av. da Boavista, 3433 - 8º - 4100-138 Porto - Portugal | porto@vda.pt
Calçada de S. Lourenço, 3 - 2º C - 9000-061 Funchal - Portugal | madeira@vda.pt