Dados Pessoais: um desafio para o seu negócio

> *"Privacy is the next business imperative. The fact is that good privacy is good business – it fosters trust, builds consumer confidence, strengthens brand recognition, increases customer loyalty and ultimately, delivers competition advantage" Privacy Commissioner of Ontario, Canada, August 2001*

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

Na verdade, se a sua empresa ou organização dispõe de dados como o nome, a morada, o telefone, endereço de email, imagens ou qualquer outro elemento relativo a pessoas individuais (sejam clientes, trabalhadores ou fornecedores), usa sistemas de videovigilância, efectua a gravação de chamadas telefónicas, utiliza *cookies*, etc independentemente do sector de actividade em que actua (banca, seguros, comunicações electrónicas e TIs, farmacêutico, prestação de cuidados de saúde, conteúdos e audiovisuais, entre outros), então interessa-lhe:

- **conhecer as regras que regulam o tratamento de dados pessoais,**
- **saber quais são os riscos de incumprimento de tais regras, e**
- **estabelecer uma política de tratamento de dados pessoais para a sua organização.**

As regras

As regras que regulam o tratamento de dados pessoais e a privacidade (*fig. 1)* têm ganho, nos últimos anos, uma importância crescente.

A nível da União Europeia assiste-se a uma crescente preocupação de articulação entre “protecção da privacidade dos cidadãos” vs “segurança”, sobretudo depois dos atentados de 11 de Setembro, de 11 de Março e 7 de Julho. Até então, a Europa assumia uma posição claramente protectora da privacidade dos cidadãos, a qual após tais acontecimentos foi posta em causa. Esta mudança de visão tem, de resto, sido patente nas discussões em torno da proposta de directiva “relativa ao prazo de conservação de dados tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis e que altera a Directiva 2002/58/CE”, não publicada (Com (2005) 438, Bruxelas, 21.9.2005) e na definição das regras de segurança pelas companhias de aviação.

O desenvolvimento da sociedade da informação, dominado pela globalização da troca de informação e pelo uso de tecnologias cada vez mais intrusivas na vida privada, tem igualmente acarretado desafios constantes neste domínio da protecção da privacidade.

O sector das comunicações electrónicas e das TIs é (talvez a par do domínio da saúde onde a problemática em torno do tratamento do dado DNA suscita, e continuará a suscitar, questões complexas) um daqueles em que provavelmente assistiremos a mais mudanças e que será alvo de maiores desafios. A tecnologia tem modificado e vai seguramente continuar a modificar a forma como se recolhe, processa e transmite os dados pessoais.

Neste contexto e porque a legislação não evolui necessariamente ao mesmo ritmo da inovação tecnológica, é fundamental que o sector se antecipe, instituindo mecanismos de auto-regulação evitando assim que cresçam as preocupações dos indivíduos em relação às novas tecnologias. Só esta atitude pró-activa do sector permitirá que as novas tecnologias se possam desenvolver, crescer e aperfeiçoar.

Algumas empresas do sector das TIs assumem claramente esta postura. Um exemplo conhecido é o da Microsoft. Para esta empresa, as questões de privacidade são uma área chave da respectiva actividade. A Microsoft possui uma equipa com enorme

experiência neste domínio produzindo, no âmbito das suas atribuições, diversos relatórios e livros brancos. No último livro branco da Microsoft, intitulado "*E.U Data Privacy in Pratice – Microsoft's Approach to Compliance"* de Julho de 2005, a Microsoft apresenta a forma como endereça, entre outros, as "*notices and information disclosures"*, o "*spam"*, os "*cookies"*, o "*spyware"*.

Os riscos

Os riscos de incumprimento da legislação de privacidade são, pelo menos em termos teóricos, elevados. Talvez sejam poucas as empresas conscientes de que o incumprimento desta legislação poderá, nos termos da lei portuguesa, acarretar responsabilidade civil, criminal e contra-ordenacional. A responsabilidade contra-ordenacional pode implicar a aplicação de coimas que podem ascender a € 29 927,87 e, no caso do incumprimento da lei que regula a protecção de dados pessoais no sector das comunicações electrónicas, até € 5 000 000.

Adicionalmente, a organização responsável pelo tratamento pode ainda ser impedida de utilizar os dados de que dispõe e ver a decisão da autoridade competente - a Comissão Nacional de Protecção de Dados Pessoais ("CNPD"), divulgada publicamente, com graves prejuízos para a sua imagem.

Mas se em Portugal não existem ainda notícias da aplicação de coimas elevadas a empresas ou quaisquer outras organizações, na nossa vizinha Espanha diversas organizações já sentiram o "peso" do incumprimento das regras de privacidade e protecção de dados pessoais (fig. 2).

Além destes impactos mais directos que podem decorrer do incumprimento das regras de privacidade, existem outros que não podem ser menosprezados. De acordo com um estudo levado a cabo pela *Privay & American Business of US Consumers*, 83% dos

consumidores americanos deixarão de fazer negócios com uma sociedade se tiverem conhecimento que a mesma não respeita as regras de privacidade.

Alguns consultores especializados têm estimado que em 2006, 20% a 30 % dos grandes grupos internacionais vão incorrer em custos que podem variar entre $ 5- $20 milhões (i.e. aproximadamente entre € 4 000 000 e € 17 000 000) em virtude do incumprimento das regras de protecção de dados pessoais (fonte: "*Legislation Defines Customer Privacy Management*", Walter Janowski, 29 de Outubro de 2003, Gartner Research).

É reconhecido que o nível de controlo do cumprimento das regras de fiscalização não é idêntico em todos os países. Mesmo na União Europeia, a avaliação que tem sido levada a cabo pelas entidades competentes tem relevado uma enorme disparidade na forma como os vários organismos responsáveis pela fiscalização têm actuado.

Em Portugal, a actuação da CNPD tem sido discreta mas, no último ano, a sua actividade de fiscalização tornou-se bastante mais visível, tendo várias organizações sido alvo de verdadeiros *raids* destinados avaliar o grau de *"compliance"* das regras de protecção de dados pessoais de forma global, i.e. envolvendo vários tipos de tratamento de dados pessoais normalmente levados a cabo pelas empresas – o tratamento dos dados relativos aos trabalhadores, de dados dos clientes, dados relacionados com a medicina do trabalho, etc.

Torna-se assim fundamental que as empresas actuem de forma preventiva para evitar o pior.

A política de tratamento

A estratégia a adoptar, passa, num primeiro plano, pela realização de uma avaliação do grau de "*compliance*" da empresa às regras de protecção de dados pessoais, i.e. as organizações devem levar a cabo uma auditoria interna, preferencialmente conduzida

por uma entidade independente, envolvendo os vários departamentos que tratam dados pessoais (é importante que estejam envolvidos no processo os departamentos de recursos humanos, de marketing, de sistemas de informação, entre outros e que a administração acompanhe de perto a auditoria) e que avalie, entre outros, os aspectos identificados na fig. 3.

Avaliado o "estado da arte", importa depois corrigir eventuais irregularidades detectadas. Esta tarefa poderá envolver, designadamente, a alteração dos formulários de recolha de dados pessoais utilizados pela empresa, os procedimentos e as regras associadas ao envio de publicidade para os clientes, a legalização de bases de dados junto da CNPD.

Finalmente e por forma a assegurar a manutenção do nível de "*compliance*", é essencial que a empresa disponha de uma **política interna de tratamento de dados pessoais**.

Em matéria de políticas de privacidade "*there is no one size fits all*". Cada organização, atendendo ao sector de actividade em que actua e às especificidades da sua estrutura, deve definir regras simples, objectivas e que sejam do conhecimento dos seus colaboradores.

Para assegurar a conservação do nível de "*compliance*" é ainda fundamental revisitar regularmente a política de privacidade e os procedimentos internos em matéria de tratamento de dados pessoais, de modo a que os mesmos estejam permanentemente adequados às exigências do negócio e das alterações legislativas

[Este artigo foi redigido pelos membros da equipa de protecção de dados pessoais e privacidade de Vieira de Almeida & Associados, R.L. : Margarida Couto, Magda Cocco, Muriel Faden da Silva, Nádia da Costa Ribeiro, Inês Nolasco, Leonor Vale e Castro e Carolina Nascimento Neves]

Fig 1

Principais regras aplicáveis ao tratamento de dados pessoais

- **Os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas e não podem ser posteriormente tratados de forma incompatível com as finalidades da recolha.**
- **Apenas podem ser recolhidos os dados adequados, pertinentes e não excessivos relativamente às finalidades da recolha.**
- **Os dados pessoais devem ser exactos e actualizados.**
- **Os dados pessoais apenas podem ser conservados durante o período necessário para a prossecução das finalidades da recolha/tratamento.**
- **A empresa terá que pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados.**
- **O responsável pelo tratamento tem de disponibilizar ao titular dos dados todas as informações relacionadas com o tratamento efectuado e dar-lhe o direito de acesso, rectificação e eliminação**
- **O tratamento de dados pessoais está, em regra, sujeito a autorização do titular dos dados**
- **O responsável pelo tratamento tem que legalizar as bases de dados junto da CNPD**

Fig 2

AEPD vs Zeppelin

A autoridade espanhola encarregue da protecção de dados pessoais (*"Agencia Española de Protección de Datos"* – AEPD) aplicou à Zeppelin, produtora espanhola que lançou o programa televisivo "Gran Hermano" (versão espanhola do programa "Big Brother"), a maior multa alguma vez aplicada, a nível europeu, no âmbito de um único processo administrativo (€ 1. 081 822).

O processo em causa foi despoletado pelo facto de "*hackers*" terem acedido, através da Internet, aos dados de 1 700 potenciais concorrentes, dados estes que, nalguns casos, continham informação relativa à respectiva saúde mental, QI e histórico de crédito.

A imposição da sanção acima descrita teve como fundamento a violação, por parte da Zeppelin, da legislação espanhola em matéria de dados pessoais, violação esta que se traduziu: (i) no incumprimento da obrigação de informação aos potenciais concorrentes, (ii) na não obtenção do respectivo consentimento para o tratamento de dados sensíveis, (iii) no incumprimento dos requisitos de tratamento de dados por terceiros e (iv) no incumprimento dos normativos em matéria de medidas de seguranças.

AEPD vs. Telefónica

A AEPD aplicou à Telefónica, operador espanhol de telecomunicações, uma multa no valor de € 420 708, por incumprimento da legislação espanhola em matéria de dados pessoais.

A Telefónica procedeu ao tratamento de dados pessoais após recusa dos respectivos titulares, tendo subsequentemente transmitido os referidos dados a um terceiro, a Telefónica Data, empresa detida pelo Grupo Telefónica, sem o necessário consentimento.

A multa imposta à Telefónica teve como fundamento o tratamento de dados para finalidades incompatíveis com a recolha, bem como a respectiva transmissão à Telefónica Data sem o consentimento dos respectivos titulares. À Telefónica Data foi igualmente imposta uma multa no valor de € 420 708, por violações semelhantes.

Fig. 3

Checklist

- ☐ **Existem bases de dados pessoais (de clientes, fornecedores, colaboradores) e/ou câmaras de videovigilância na empresa?**
- ☐ **Foi obtido o consentimento do titulares dos dados?**
- ☐ **Os instrumentos de recolha dos dados, designadamente os contratos, contêm informações detalhadas sobre a finalidade da recolha e outras informações relevantes?**
- ☐ **O tratamento foi notificado/autorizado pela CNPD?**
- ☐ **Os dados recolhidos são essenciais para a finalidade da recolha?**
- ☐ **Existe um responsável pelas bases de dados pessoais na empresa?**
- ☐ **A empresa obteve o consentimento da CNPD para a instalação das câmaras de videovigilância e tem afixados avisos que alertem para a existência das mesmas?**
- ☐ **A empresa instituiu mecanismos para garantir a segurança e confidencialidade dos dados que tem em seu poder?**
- ☐ **Antes de ceder dados pessoais a terceiros, a empresa certifica-se que tem autorização para o efeito?**
- ☐ **A empresa celebra contratos escritos com empresas subcontratadas para o tratamento de dados pessoais?**
- ☐ **Antes de proceder à transferência de dados para países fora da União Europeia a empresa confirma que está legalmente autorizada a fazê-lo?**
- ☐ **Os colaboradores da empresa que têm acesso aos dados pessoais estão informados sobre as obrigações que impendem sobre eles e a empresa?**
- ☐ **Se a empresa pretender cruzar dados de uma base com os de outra certifica-se que tal é possível?**
- ☐ **A empresa avalia regularmente o cumprimento da Lei de Protecção de Dados Pessoais?**

Esta “checklist” destina-se unicamente a auxiliar as empresas a efectuar uma avaliação preliminar e genérica sobre o grau de prossecução das obrigações e regras previstas na Lei de Protecção de Dados Pessoais (LPDP) e não pretende ser exaustiva.

Note-se que a resposta afirmativa às questões formuladas não permite por si só concluir que a empresa cumpre integralmente as disposições legais nesta matéria, não dispensando assim uma investigação aprofundada sobre a situação de cada empresa e aconselhamento jurídico concreto.