Jornal de Negócios Segunda-feira 29 de Janeiro 2007

CONVIDADO

MAGDA COCCO

As questões de privacidade são importantes para a sua empresa?

As questões associadas à protecção da privacidade têm hoje uma importância tal que passam a contar, pela primeira vez este ano, com um dia próprio – por decisão do Conselho da Europa, o dia 28 de Janeiro é agora o Dia Europeu da Protecção de Dados Pessoais.

Porque são importantes as questões de privacidade?

A sua empresa ou organização, independentemente do sector em que actua, dispõe seguramente de dados pessoais (tais como nome, morada, telefone, email), relativos a trabalhadores, clientes ou fornecedores. É ainda natural que proceda à videovigilância de instalações, que desenvolva acções de "marketing" directo ou que grave chamadas telefónicas recebidas ou efectuadas por *call centers*. É por isso que as questões de privacidade e protecção de dados pessoais lhe interessam!

Se a sua empresa ou organização actua em sectores que por norma tratam dados pessoais sensíveis (banca, seguros, saúde, telecomunicações, entre outros), então, não dar atenção aos aspectos de privacidade e protecção de dados pode revelar-se dramático.

São porventura ainda poucas as empresas portuguesas conscientes das consequências que o incumprimento da legislação de dados pessoais poderá ter para a actividade da empresa e para os seus responsáveis. Tais consequências são todavia bastante nefastas (embora facilmente evitáveis) – além da aplicação de pesadas s, o incumprimento da legislação de privacidade pode fazer incorrer os gestores das organizações em responsabilidade criminal, sobretudo se estiverem em causa dados sensíveis.

E são já várias as empresas que tomaram consciência da importância de cumprir a legislação de dados pessoais, da pior maneira – no final de 2006, a autoridade de protecção de dados grega aplicou uma de 76 milhões de euros a uma conhecida operadora móvel, por considerar que a empresa não tinha protegido de forma adequada a privacidade da sua rede contra "intromissões indevidas". Também no sector das telecomunicações, o então CEO da Sonera foi em 2005 condenado a pena de prisão, por violação indevida da privacidade dos seus trabalhadores. E a autoridade de protecção de dados francesa aplicou em 2006 uma elevada um Banco por ter utilizado indevidamente dados pessoais de um cliente.

Foi também em 2006 que rebentou o "Caso SWIFT", quando se descobriu que certos organismos governamentais dos EUA tinham, desde os ataques terroristas de 11 de Setembro, acesso às transacções financeiras dos clientes dos bancos europeus realizadas através do sistema SWIFT. Este caso deu origem a inúmeros processos contra bancos europeus aderentes ao sistema, por não terem informado os seus clientes da transmissão dos dados para os EUA.

Em Portugal, apesar de a actuação da Comissão Nacional de Protecção de Dados (CNPD) ser discreta, a sua acção tem vindo a intensificar-se, designadamente através de investigações de fundo no sector da saúde, dos seguros e no domínio da videovigilância. É também cada vez maior o número de queixas junto da CNPD, que desencadeiam inspecções por parte desta autoridade.

Mas, além de coimas e responsabilidade criminal, violar a lei de protecção dos dados pessoais tem outros "custos escondidos", nomeadamente de imagem, com impacto relevante junto dos clientes da empresa – diversos estudos demonstram que as empresas expostas a escândalos de violação das normas de privacidade perdem a confiança dos consumidores.

Neste contexto, percebe-se por que motivo os gestores das grandes multinacionais atribuem às questões de privacidade uma prioridade de terceiro nível no *ranking* dos instrumentos de gestão.

O que fazer para evitar os riscos?

É crucial conhecer as obrigações em matéria de protecção de dados pessoais e ter uma estratégia de actuação neste domínio.

As obrigações da empresa, enquanto responsável pelo tratamento dos dados, são diversas, mas fáceis de cumprir. Digamos que "no mínimo" a empresa deve:

- Informar o titular dos dados sobre a utilização que pretende dar aos dados e, em alguns casos, obter o seu consentimento.
- Legalizar as bases de dados (BD) junto da CNPD.

Mas, acima de tudo, importa ter uma estratégia de privacidade.

Para a definir é preciso começar por fazer uma avaliação do grau de cumprimento da lei. Avaliado o "estado da arte" importa legalizar todas as BD e perspectivar qual é a utilização que a empresa pretende dar aos dados pessoais de que dispõe. As potencialidades das novas tecnologias de localização de pessoas e/ou bens, através das redes móveis ou de RFID, não devem ser ignoradas nesta avaliação, em particular, se a empresa actua em áreas como a saúde, distribuição e logística, segurança ou aeronáutica.

Igualmente importante é a definição de uma política de privacidade da empresa, e 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 definir regras simples e objectivas que permitam assegurar que, no dia a dia, os seus colaboradores cumprem a legislação de protecção de dados pessoais.

E esta é a importância de "um dia da privacidade" no dia-a-dia da sua empresa.

Associada sénior da VdA , e
coordenadora da área de Dados Pessoais

Se a sua empresa ou organização actua em sectores que por norma tratam dados pessoais sensíveis (banca, seguros, saúde, telecomunicações, entre outros), então, não dar atenção aos aspectos de privacidade e protecção de dados pode revelar-se dramático.

Além de coimas e responsabilidade criminal, violar a lei de protecção dos dados pessoais tem outros "custos escondidos", nomeadamente de imagem, com impacto relevante junto dos clientes da empresa.

Algumas regras fundamentais

- 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 face 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.
- 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.
- A empresa tem de pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados.
- O incumprimento destas regras pode gerar a aplicação de pesadas coimas e responsabilidade criminal.