CISION

negócios

negocios.pt

ID: 77263574

18-10-2018

Meio: Imprensa
País: Portugal
Period.: Diária
Âmbito: Economia, Negócios e.

Pág: 18
Cores: Cor
Área: 25,70 x 32,00 cm²
Corte: 1 de 1

OPINIÃO

SOFIA RIÇO CALADO
Advogada da SRS, especialista em protecção de dados

Dados roubados, trancas à porta

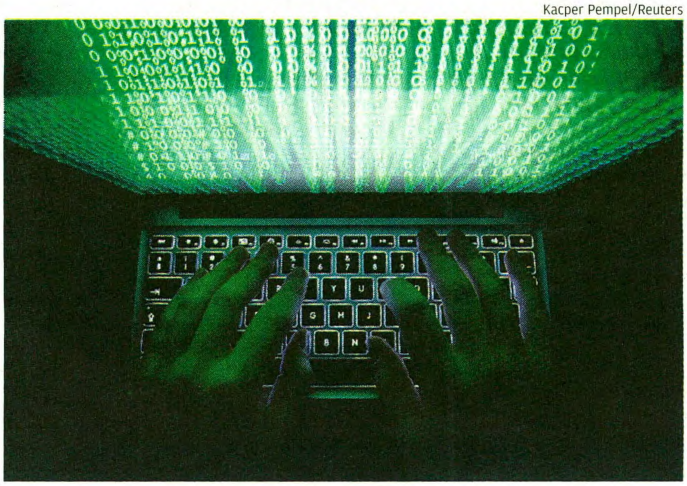
Em alerta. É neste estado que se encontrarão várias empresas depois da sucessão recente de notícias que dão conta do ciberataque recente ao Facebook, que expôs informação de cerca de 50 milhões de utilizadores, ou do encerramento futuro da rede social Google +, envolta em polémica após um incidente de segurança não reportado no passado mês de Março, alegadamente pelo receio das perdas reputacionais associadas, o qual terá desprotegido até 500 mil contas pessoais.

Em situações destas, as empresas têm agora, ao abrigo do Regulamento Geral sobre a Proteção de Dados (ou RGPD), a obrigação de notificar a autoridade competente sempre que uma violação de dados pessoais origine um risco para os direitos e liberdades das pessoas singulares. Desta forma, procedeu aliás o Facebook, que notificou a Comissão de Proteção de Dados irlandesa, tendo esta dado imediatamente início a uma investigação sobre a adoção de medidas técnicas de segurança pelo gigante tecnológico. Caso esta entidade de controlo determine que o Facebook não fez tudo o que devia para prevenir o acesso por hackers às contas dos seus utilizadores, arrisca uma sanção que poderá chegar até 2% do seu volume de negócios anual a nível mundial.

Mas o que é uma violação de dados pessoais? Esta consiste num incidente de segurança que motive, de modo meramente acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados tratados por uma empresa ou um serviço público que permitam a identificação de pessoas singulares.

Imagine que envia um e-mail com conteúdo comum para centenas de destinatários e que, em vez de colocar os respetivos endereços em modo "BCC", estes são descritos em "Para" ou "CC", logo permitindo a sua visualização. Existe aqui um risco para a privacidade destes destinatários que pode motivar uma notificação à Comissão Nacional de Proteção de Dados (ou CNPD).

Kacper Pempel/Reuters



Acrescentemos agora que trabalha como profissional de saúde numa clínica ou num hospital. Ora, um e-mail inócuo que continha apenas informação sobre marcação de consultas permite, de repente, que todos os destinatários saibam quem frequenta uma determinada especialidade, por exemplo quem vai ao psicólogo. O risco para a privacidade acabou de aumentar exponencialmente, pelo que os próprios titulares dos dados pessoais utilizados devem ser notificados.

As empresas ou os serviços públicos têm 72 horas para notificar a CNPD, logo que saibam de uma situação de violação de dados pessoais.

Existem regras a observar. Antes de mais, as empresas ou os serviços públicos têm um prazo de 72 horas para notificar a CNPD, a partir do momento em que tenham conhecimento da violação de dados pessoais. O formulário encontra-se disponível no respetivo sítio de Internet (www.cnpd.pt) e implica que descreva, entre outros aspetos, as medidas que irá adotar para resolver a falha de segurança. Este prazo pode ser manifestamente curto, por exemplo quando o serviço de apoio ao cliente não é assegurado diretamente pela clínica mas por uma entidade terceira, a qual ainda terá que avisar sobre o sucedido de modo a que a notificação possa ocorrer.

Já os destinatários do e-mail devem ser informados sem demora injustificada sobre o ponto de contacto que lhes permita obter mais esclarecimentos (o Encarregado da Proteção de Dados, sempre que exista), quais são consequências prováveis da violação de dados pessoais (como o caráter público das idas ao psicólogo) e as medidas que serão tomadas para reparar a violação de dados pessoais (qualquer contacto, a partir de agora, será efetuado de modo a proteger a sua esfera privada, v.g. por SMS).

Convém que qualquer entidade, como aquela em que trabalha, incorpore algumas preocupações na sua gestão diária. Mesmo que não disponha de um Encarregado da Proteção de Dados, deve ter uma pessoa responsável pela privacidade que se preocupe com estas temáticas.

Igualmente, deve desenvolver um registo, sempre atualizado, em que conteúdo todos os incidentes de segurança, mesmo os que não devam ser notificados, incluindo causas, efeitos e, muito importante, as ações de reparação tomadas.

Recorde-se, sobretudo, que é preciso saber agir com certeza e rapidez. Mal ocorra uma falha, é necessário que exista um processo instalado, o qual determine como é que esta falha de segurança surgiu, se envolveu ou não dados pessoais e, em caso afirmativo, perceber como mitigar sem demora as respetivas consequências, enquanto que as devidas notificações são efetuadas. Tal processo deve ser enquadrado numa política geral de proteção de dados e cibersegurança, com tarefas distribuídas aos diferentes colaboradores.

De algo pode estar certo: apenas será possível articular com sucesso tantos passos a dar se este procedimento estiver consolidado antes da primeira "data breach". Avise a sua organização para que meta mãos à obra. ■

Este artigo foi redigido ao abrigo do novo acordo ortográfico.