CRÓNICA VISÃO ELECTRÓNICA
Nº 473 / 2018-02-08
http://www.gestaodefraude.eu
Elisabete Maciel

>> Proteção de Dados: será UM passo maior do que a perna?

Nos dias de hoje, a preocupação com a proteção dos dados pessoais está no centro do debate. Quando falamos em dados pessoais, estamos a referir-nos a toda e qualquer informação, independentemente do suporte, que permite identificar alguém: o nome, o NIF, o número da segurança social, o número de telefone, uma fotografia, o endereço de correio eletrónico, a matrícula de automóvel, a localização, etc. Ademais, há todo um conjunto de dados "sensíveis" que revelam características pessoais, como a origem étnica, a crença religiosa, a opinião política, a orientação sexual, os dados biométricos, genéticos, etc.

Ora, todos estamos cientes da meteórica evolução tecnológica, a qual contribui para que o volume de informação que circula na Internet seja cada vez mais avassalador: em cada minuto, são feitas mais de 3,5 milhões de pesquisas no Google, são visualizados mais de 4 milhões de vídeos no *Youtube* e são enviados mais de 155 milhões de *e-mails*. A informação flui a uma velocidade nunca antes vista. Nesse sentido, é evidente a emergência para a criação de normativos ou protocolos que permitam uma real proteção de dados, nomeadamente online.

Tendo em conta que a proteção de dados de pessoas singulares é um direito fundamental, entende-se que esta encontra-se na génesis da elaboração do Regulamento Geral de Proteção de Dados (RGPD) por parte da Comissão Europeia em 2016 e que irá entrar em vigor em todos os Estados Membros a 25 de Maio do corrente ano[1]. Um dos objetivos fulcrais deste regulamento centra-se na garantia da privacidade e na salvaguarda dos dados pessoais de cidadãos europeus, os quais podem estar na posse de organizações da mais diversa natureza. Este normativo é extensível ao mundo inteiro pois, desde que o tratamento dos dados envolva cidadãos europeus, este terá de ser cumprido.

Se compararmos a legislação em vigor com o atual regulamento, contatamos que, as diferenças não são significativas em relação ao princípio de proteção de dados pessoais. Contudo, já o mesmo não se pode dizer quando falamos das regras a observar para a sua aplicação:

CRÓNICA VISÃO ELECTRÓNICA
Nº 473 / 2018-02-08
http://www.gestaodefraude.eu
Elisabete Maciel

- Há um alargamento do conceito de dados pessoais;
- As organizações são elas próprias responsáveis por garantir a conformidade com o RGPD. Deixam de poder assumir uma postura cómoda de apenas terem de notificar e solicitar autorização à Comissão Nacional de Proteção de Dados (CNPD) sempre que necessitam de efetuar tratamento dos mesmos;
- As organizações são obrigadas a informar a Autoridade de Controlo (AC) da ocorrência de quaisquer incidentes que possam levar ao comprometimento de dados pessoais, como por exemplo uma falha de segurança. Além disso, em algumas situações, essa informação terá de ser fornecido aos próprios titulares;
- As sanções a que as organizações estão sujeitas pelo incumprimento não são de forma alguma insignificantes, podendo mesmo atingir os 20 milhões de euros ou 4% do volume de negócios;

Pelo que foi anteriormente exposto, facilmente se conclui que as organizações, independentemente da sua dimensão, estão perante um enorme desafio:

- Será que têm uma lista exaustiva de todos dados que são da sua responsabilidade e que armazenam dos seus clientes, colaboradores, fornecedores, parceiros, etc? E sabem onde se encontram? Nos servidores internos? Na *cloud*?
- Além disso, têm o consentimento explícito dos envolvidos para o armazenamento/tratamento de dados que efetuam? De acordo com o RGPD, não é de forma alguma suficiente a situação usual de caixas pré-marcadas, ou o inferir o consentimento a partir do silêncio. As empresas têm de ser capazes de demonstrar que o consentimento foi dado e que este foi explícito.
- Mais ainda, um dos direitos estabelecidos no RPGD é o do "esquecimento". Será que as organizações estão preparadas para eliminar os dados a pedido do titular, e que existem em todos os repositórios, sejam estes físicos ou lógicos sem comprometer o seu negócio? E nos *backups*?
- Será que registam e armazenam todos os tratamentos efetuados sobre os dados? Terão de o fazer obrigatoriamente se

CRÓNICA VISÃO ELECTRÓNICA
Nº 473 / 2018-02-08
http://www.gestaodefraude.eu
Elisabete Maciel

empregam mais de 250 trabalhadores.

- E já agora, se tiverem uma falha de segurança, mais frequente do que parece, será que conseguem identificar quais os dados afetados? E será que conseguem identificar os procedimentos a seguir para atalhar o problema e resolvê-lo? Só terão 72 horas para o fazer.

Em Portugal, onde o tecido empresarial é maioritariamente constituído por micro e pequenas empresas, muitas organizações terão certamente grandes dificuldades em estar em conformidade com o RGPD. Mas o desafio não é menor quando nos referimos a empresas de grande dimensão, pois embora eventualmente avançadas do ponto de vista tecnológico, recorrem frequentemente a parceiros, como, por exemplo, a fornecedores de alojamento (*cloud*). A teia é gigantesca.

Se a proteção de dados é algo indispensável e fundamental , e atendendo aos requisitos impostos pelo RGPD, será que houve a ponderação necessária no que diz respeito à sua aplicabilidade por parte das empresas? Qual será o comportamento de empresas como a Google e o Facebook face à obrigatoriedade de estar em conformidade com o RGPD?

Relativamente a esta questão, é pertinente recordar que recentemente a Google recusou apagar da web indexada (o chamado "direito de esquecimento") informação pesquisável pelo seu motor de busca a cerca de 4300 portugueses. E estes tinham solicitado oficialmente que se deixasse de associar as pesquisas feitas pelo seu nome a determinados endereços de internet.

NOTAS

(1) Excelacom 2017