



LEGAL

AS STARTUPS E O NOVO REGULAMENTO EUROPEU DE PROTEÇÃO DE DADOS

NO INÍCIO DE 2016 SERÁ ADOPTADO O NOVO REGULAMENTO EUROPEU DE PROTEÇÃO DE DADOS PESSOAIS ("REGULAMENTO").

O que já conhecemos do seu texto (e é quase tudo) permite-nos dizer que este diploma tem a maior importância para cidadãos e empresas e será determinante para o desenvolvimento de novos modelos de negócio de base digital. Vai, por isso, condicionar fortemente a actividade das startups.

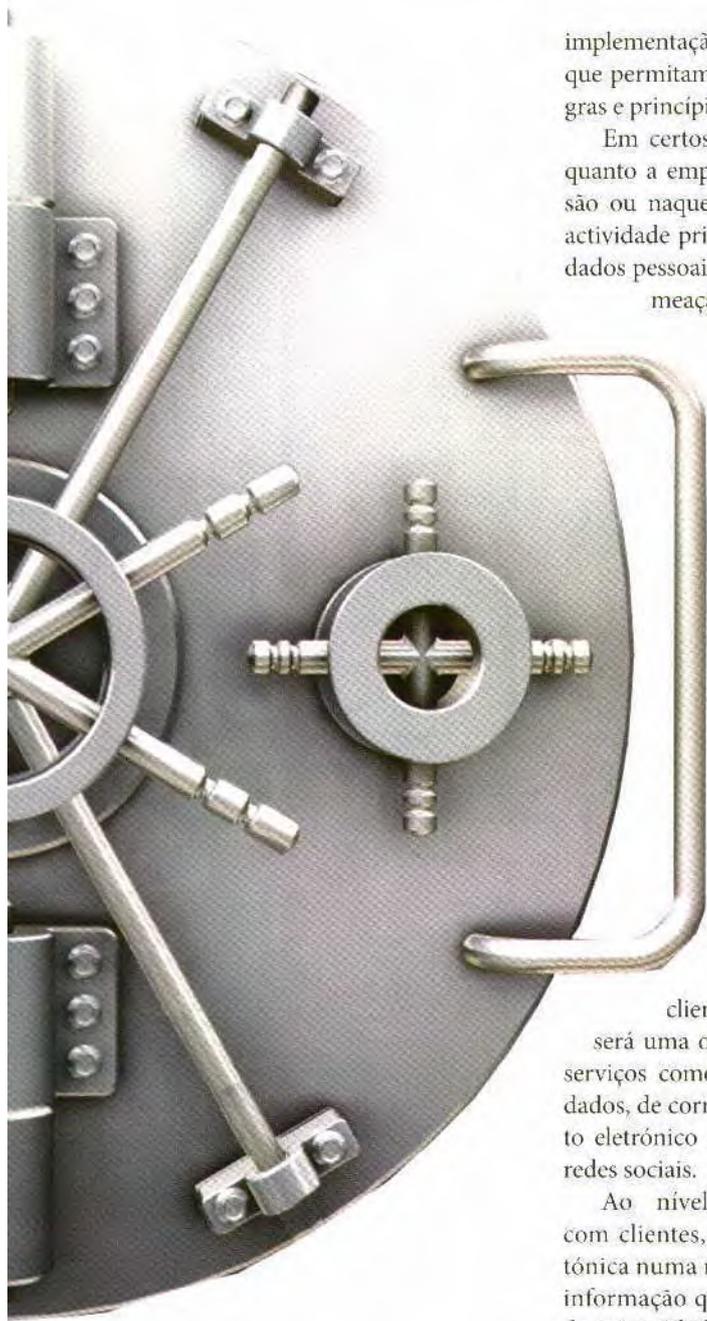
Desde logo, porque impõe de modo muito claro que a conceção de produtos e serviços tenha na sua base preocupações de privacidade.

Ao invés do actual modelo, que coloca muito a tónica nas notificações e pedidos de autorização efectuados à autoridade de protecção de dados (em

Portugal, a CNPD), este novo modelo foca-se muito na responsabilização das empresas quanto à adoção de práticas "privacy friendly", impondo a realização de auditorias regulares às estratégias adotadas quanto a tratamento de dados pessoais.

Introduz ainda o conceito de privacy by design, o que significa que as preocupações com a privacidade passarão a ter de ser partilhadas por todos numa empresa e, em particular, ao nível da conceção de produtos e serviços. Isto requer um período de adaptação prolongado no tempo e a





implementação de práticas de gestão que permitam a interiorização de regras e princípios.

Em certos casos, nomeadamente quanto a empresas de maior dimensão ou naquelas que tenham, como actividade principal, o tratamento de dados pessoais, será obrigatória a nomeação de um “data privacy officer” que, com um estatuto de independência, irá assegurar o cumprimento do regime legal da protecção de dados.

O Regulamento impõe ainda obrigações ao nível da portabilidade dos dados. As empresas serão obrigadas a garantir que a informação pessoal que guardam dos seus clientes pode ser facilmente transferida para um novo prestador de serviços se o seu cliente assim quiser. Esta será uma obrigação desafiante em serviços como os de alojamento de dados, de correio eletrónico, de registo eletrónico de saúde ou ainda nas redes sociais.

Ao nível do relacionamento com clientes, o Regulamento põe a tónica numa maior transparência da informação que consta das políticas de privacidade e que é prestada aos

utilizadores sobre o modo como são tratados os seus dados pessoais (incluindo metadados).

Impõe ainda uma obrigação reforçada de eliminação de dados quando os mesmos deixem de ser necessários, maiores restrições à actividade de profiling, um enquadramento restritivo da anonimização e da pseudoanonimização de dados, bem como um reforço das obrigações de segurança e a introdução da obrigação de as empresas notificarem violações de segurança de dados (data breaches) à CNPD e em certas circunstâncias, aos próprios clientes.

No caso dos negócios de base cloud, desde o data storage até aplicações SaaS (software as a service), o Regulamento passa a impor diretamente às empresas que se limitem a alojar dados dos seus utilizadores ou a processá-los em subcontratação importantes obrigações em matéria de segurança, a necessidade de realização de auditorias periódicas, além da sujeição direta à supervisão/fiscalização da CNPD, o que, até agora não sucedia.

De notar, ainda, que haverá um robustecimento das sanções, que no caso de grupos multinacionais poderão ter um significado muito importante, ascendendo até 4% da sua faturação mundial.

Uma vez adotado, o Regulamento entrará em vigor após dois anos, ou seja, no início de 2018. No entanto, a implementação de estratégias “amigas” da privacidade por uma empresa não é uma tarefa fácil e requer tempo.

Por isso, no caso das start-ups, será aconselhável que, desde já, seja promovido o maior conhecimento das obrigações em matéria de privacidade e do próprio Regulamento, o que se reflectirá de modo muito positivo no sucesso dos seus projetos. ■

Luís Neto Galvão
SÓCIO NA SRS ADVOGADOS

Este novo modelo foca-se muito na responsabilização das empresas quanto à adoção de práticas “privacy friendly”

