

Opinião: Tempestade Legislativa Perfeita

A legislação aprovada em matéria de segurança e privacidade traz novas exigências às empresas que têm de começar a preparar-se para cumprir as novas regras, defende Ricardo Henriques.



Por **Ricardo Henriques (*)**

Implementar medidas para prevenir falhas de segurança e violações de privacidade é algo de essencial quando falamos de dados pessoais ou de segredos comerciais. Podem prevenir, mitigar ou transferir os eventuais riscos delas resultantes.

Desde logo, em relação aos dados pessoais, o risco de incumprimento pode ter um impacto significativo, traduzindo-se em multas elevadas. Mas os riscos não se reduzem apenas ao aspeto sancionatório. Na verdade, poderão ter um impacto muito superior e, mesmo na ausência de uma efetiva falha ou violação, uma queixa poderá despoletar uma investigação, o que poderá implicar alterações não programadas nas práticas de negócios, exposição mediática negativa e alocação de recursos da entidade para resolver a questão. Se existir efetivamente uma violação de dados pessoais, a este risco acresce o de indemnizações aos titulares dos dados, danos à reputação e imagem da empresa, incumprimento de obrigações contratuais, bem como possível perda de negócios atuais ou futuros. Por último, mas não menos importante, há que ter em conta o risco pessoal dos administradores e gerentes das empresas que podem ser pessoalmente implicados por uma não conformidade ou incumprimento legal, inclusive com sanções penais.

Quanto aos segredos comerciais da empresa, o risco resulta na incapacidade de proteger esse valioso ativo da empresa, de lutar contra a espionagem industrial ou de proteger determinado tipo de inovação e know-how, e assim impedir o aproveitamento do seu valor comercial por terceiros.

Por todos estes riscos, a implementação de um plano e a execução das medidas necessárias para mitigar ou transferir esses riscos torna-se essencial. As medidas a implementar devem ser diretas - relacionadas com a proteção de informações contra uso, acesso ou divulgação não autorizadas (ex.: criptografia de dados,

palavras-passe, perfis de acesso, etc.) - e indiretas (ex.: formação do pessoal).

Em todo o caso, convirá ter presente que, se por um lado a incapacidade de ter em consideração questões de segurança e privacidade em momentos críticos (desenvolvimento de produtos, processo de fusão/aquisição, etc.) pode, em última análise, afetar o valor do negócio ou as vendas, por outro lado uma interpretação errada e demasiado restritiva da lei também poderá colocar entraves desnecessários às práticas de negócios em nome da conformidade, o que pode igualmente resultar na perda de oportunidades e representar uma desvantagem competitiva.

Sobre este assunto, é importante recordar a recente aprovação de três diplomas: a Diretiva de Segurança das Redes e da Informação (SRI), a transpor para o direito interno até 10 de maio de 2018, relativa a obrigações de cibersegurança; a Diretiva relativa à proteção de know-how e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais a transpor para o direito interno até 9 de junho de 2018; e o Regulamento Geral de Proteção de Dados (RGPD) que será diretamente aplicável nos Estados-Membros a partir de 25 de maio de 2018.

Com a aprovação destes três diplomas (e leis nacionais subsequentes) e a sua entrada em vigor em 2018, está criada a tempestade legislativa perfeita para as empresas que, se não prepararem adequadamente para ultrapassar a onda gerada, correm o risco de ficarem esmagadas pelo peso de um esforço de adaptação não planeado.

(*) sócio da sociedade de advogados PBBR