Luís Neto Galvão, Sócio, SRS Advogados

Riscos Emergentes do Corporate Governance - oportunidades e ameaças dos Sistemas de Informação – Riscos Legais e Regulatórios

26.03 2015

Riscos Legais e Regulatórios

Global Risks 2015

"The risk of large-scale cyber attacks continues to be considered above average on both dimensions of impact and likelihood (…). This reflects both the growing sophistication of cyber attacks and the rise of hyperconnectivity, with a growing number of physical objects connected to the Internet and more and more sensitive personal data – including about health and finances – being stored by companies in the cloud. In the United States alone, cyber crime already costs an estimated $100 billion each year."

Global Risks 2015
10th Edition

WORLD ECONOMIC FORUM

MARSH & McLENNAN COMPANIES

Riscos Legais e Regulatórios

Global Risks 2015

Main Technology risks

- Breakdown of critical information infrastructure and networks
- Large-scale cyber attacks
- Massive incident of data fraud/theft

Global Risks 2015
10th Edition

Riscos Legais e Regulatórios

Global Risks 2015

"Oversight mechanisms need to more effectively balance likely benefits and commercial demands with a deeper consideration of ethical questions and medium to long-term risks – ranging from economic to environmental and societal.

Mitigating, preparing for and building resilience against global risks is long and complex, something often recognized in theory but difficult in practice."

Global Risks 2015
10th Edition

Riscos Legais e Regulatórios

Ataques

Hacking, spam – Denial of Service – Malware – Cavalos de Troia – Phishing – Perda de Dados – Roubo de Dados

Motivações

Cibercrime, espionagem industrial, crime financeiro, ataques de Estados, terrorismo, Activismo

Riscos Legais e Regulatórios

Fraude (risco financeiro) – Perda de valor accionista – Risco Reputacional – Litígios e pedidos indemnizatórios – Multas e coimas – Perda de Informação Comercialmente Sensível

Proposta de Directiva Segurança das Redes e Informação (SRI)

Principais aspectos

- Datada de 7/2/2013 – está em vias de adopção pelo Parlamento Europeu e Conselho
- Tem o objectivo de garantir um elevado nível comum de segurança das redes e da informação (SRI), melhorando a segurança da Internet e das redes e sistemas informáticos privados em que assenta o funcionamento das nossas sociedades e economias.
- Exige aos Estados-Membros que:
    - aumentem o seu nível de preparação e melhorem a cooperação entre si;
    - exijam aos operadores das infra-estruturas críticas, bem como às administrações públicas, que adoptem medidas adequadas para gerir os riscos de segurança e comunicar os incidentes graves às autoridades nacionais competentes.
- É a primeira tentativa da União Europeia de estabelecer um conjunto mínimo de regras em matéria de cibersegurança em todo o continente

Proposta de Directiva Segurança das Redes e Informação (SRI)

Cada Estado-Membro:

- deve adoptar uma estratégia nacional de SRI
- designa uma autoridade nacional competente em matéria de segurança das redes e dos sistemas informáticos
- cria uma equipa de resposta a emergências informáticas, responsável pelo tratamento de incidentes e riscos de acordo com um processo bem definido
- as autoridades competentes e a Comissão devem constituir uma rede para cooperarem contra os riscos e os incidentes que afectem as redes e os sistemas informáticos

Proposta de Directiva Segurança das Redes e Informação (SRI)

Obrigações para operadores

- Incluem-se os operadores no domínio da energia, banca, saúde, transporte e serviços financeiros – a versão da directiva actualmente em discussão abrange as entidades que gerem infra-estruturas físicas através das quais o tráfego seja transmitido entre operadores de rede,

- devem adoptar medidas técnicas e organizacionais adequadas para gerir os riscos que se colocam à segurança das redes e dos sistemas informáticos que controlam e utilizam na sua actividade

- devem notificar às autoridades competentes os incidentes com impacto significativo na segurança dos serviços essenciais que fornecem.

- As autoridades competentes devem ter todos os poderes necessários, incluindo o de emitir instruções vinculativas, para investigar os casos de incumprimento destas obrigações

Segurança Digital e Privacidade – Introdução

- Regulamento revoga a actual directiva de 1995;
- Aplicabilidade directa nos 28 Estados Membros;
- Pretende remover divergências na implementação da Directiva em cada Estado membro e **diminuir** em **€2,3 mil milhões** os custos administrativos com a implementação do regime de protecção de dados pelas empresas nos vários Estados Membros, em particular por parte das PME;
- Retira o foco da notificação administrativa das operações de tratamento de dados e coloca a ênfase na **responsabilização** dos operadores económicos;

Segurança Digital e Privacidade – Introdução

- Sistema *one stop shop* para as Autoridades de Protecção de Dados. As empresas apenas terão de interagir com a autoridade do país onde têm estabelecimento principal, embora os cidadãos possam sempre queixar-se à autoridade do seu pais;

- Direito amplo de acesso aos seus dados, nomeadamente de portabilidade dos dados de uma empresa para outra (**portabilidade dos dados)**;

- Direito ao **esquecimento** e a obrigação do responsável notificar todos aqueles a que enviou dados da necessidade de proceder ao seu apagamento;

- O regulamento aplica-se a empresas fora da Europa mas cujo mercado que pretendam servir seja o europeu;

Segurança Digital e Privacidade – Introdução

- Cooperação entre autoridades de controlo;
- Reforço do poder das autoridades de protecção de dados;
- Vai incrementar custos dos das empresas com *compliance;*
- Necessária uma especial governance interna para integrar novos procedimentos.

Segurança Digital e Privacidade – Novidades com Impacto em Sectores Sensíveis

Obrigações em destaque:

- Conservar **documentação** relacionada com tratamentos;
- Aplicar os requisitos de **segurança**;
- Notificação de **violação de dados**
- Realizar uma **avaliação de impacto** sobre a protecção de dados
- Designar um **delegado** para a protecção de dados

Segurança Digital e Privacidade – Nível Reforçado de *Compliance*

A - Documentação

- Responsável pelo tratamento e cada subcontratante devem manter documentadas **todas as operações de tratamento de dados** efectuadas sob a sua responsabilidade. Cada empresa terá de implementar procedimentos de reporte interno e registo de operações e identificação das suas características essenciais .

B - Segurança do Tratamento – Principio Geral

- **Responsável pelo tratamento** e **subcontratante** aplicam medidas técnicas e organizativas necessárias para assegurar um nível de segurança adaptado aos **riscos** que o tratamento representa e à **natureza** dos dados pessoais a proteger, atendendo às técnicas mais recentes e aos custos resultantes da sua aplicação.

Segurança Digital e Privacidade – Nível Reforçado de *Compliance*

C - Notificação da violação de dados pessoais à autoridade de controlo

- O responsável pelo tratamento notifica da violação de dados pessoais a autoridade de controlo, **sem demora injustificada** e sempre que possível, o mais tardar **24 horas** após ter tido conhecimento da mesma.

- Deverá nessa notificação:
  (a) **Descrever** a natureza de violação dos dados, incluindo categorias e o número de titulares de dados afectados;
  (b) Comunicar **contactos** do delegado para a protecção de dados ou de outro ponto de contacto onde possam ser obtidas informações adicionais;
  (c) Recomendar **medidas** destinadas a atenuar os eventuais **efeitos adversos**;
  (d) Descrever as **consequências** da violação de dados pessoais;

Segurança Digital e Privacidade – Nível Reforçado de *Compliance*

C - Notificação da violação de dados pessoais à autoridade de controlo

(e) Descrever as medidas propostas ou adoptadas pelo responsável pelo tratamento para **remediar** a violação de dados pessoais. (Artigo 31.º)

- Se o prazo de 24 horas não for cumprido deve ser dada justificação razoável.
- O subcontratante alerta e informa o responsável pelo tratamento **imediatamente** após a detecção de uma violação de dados pessoais.
- O **responsável pelo tratamento** documenta qualquer violação de dados pessoais, incluindo os factos, os respectivos efeitos e a medida de reparação adoptada. A documentação deve permitir à autoridade de controlo verificar o respeito do disposto em matéria de obrigações de reporte.

(Artigo 31.º)

Segurança Digital e Privacidade – Nível Reforçado de *Compliance*

D - Comunicação de uma violação de dados pessoais ao titular dos dados

- Deve ocorrer quando a violação de dados pessoais for **susceptível de afectar negativamente a protecção dos dados pessoais ou a privacidade** do titular dos dados;

- O responsável, após a notificação a autoridade de controlo, **comunica a violação de dados pessoais à pessoa em causa** sem demora injustificada.

- A comunicação descreve a **natureza** da violação dos dados pessoais e incluir, pelo menos, a **identidade** e **contactos** do delegado para a protecção de dados e recomendar **medidas** destinadas a atenuar eventuais efeitos adversos.

- Comunicação não obrigatória se o responsável **demonstrar** cabalmente, a contento da autoridade de controlo, que tomou medidas de protecção tecnológica adequadas e que estas foram aplicadas. (Artigo 32.º)

Segurança Digital e Privacidade – Nível Reforçado de *Compliance*

E - Avaliação de impacto sobre a protecção de dados

- Obrigatória uma avaliação de impacto quando as operações de tratamento apresentem **riscos específicos** para os direitos e liberdades dos titulares de dados em virtude da sua natureza, do seu âmbito ou da sua finalidade.

- O responsável ou o subcontratante devem **avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem** e as medidas devem assegurar um **nível de segurança adequado**.

- Avaliação inclui, pelo menos, uma **descrição geral** das operações de tratamento previstas, a **avaliação dos riscos**, as **medidas previstas para fazer face aos riscos**, as **garantias**, **medidas de segurança** e os mecanismos para assegurar a protecção dos dados e demonstrar a **conformidade** com o regulamento. (Artigo 33.º)

Segurança Digital e Privacidade – Nível Reforçado de *Compliance*

F - Designação do delegado para a protecção de dados

- Designado pelo responsável pelo tratamento e subcontratante com 250 assalariados (ii) ou com actividades principais que constituam operações de tratamento que, pela natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares de dados.

- Escolhido com base no mérito (qualidades profissionais, conhecimentos especializados no domínio da legislação e das práticas a nível da protecção de dados e capacidade para cumprir as suas funções).

- Outras funções profissionais que incumbam ao delegado devem ser **compatíveis** com as atribuições e funções dessa pessoa na qualidade de delegado para a protecção de dados e não impliquem um **conflito de interesses**.

- Designação por período mínimo de **dois anos**, renovável.

(Artigo 35.º)

Coimas Muito Significativas

Actual versão prevê coimas até 100 000 000 EUR ou 5% do volume de negócios mundial anual da empresa infractora, aplicáveis, entre outros casos, a quem, de forma intencional ou negligente:

- Proceda ao tratamento de dados pessoais sem fundamento jurídico ou não respeite uma oposição;

- Não adopte **regras internas** ou não execute medidas adequadas para assegurar e comprovar o respeito de obrigações de **conservação** de documentação, **segurança** no tratamento, **avaliação de impacto**, designação de **delegado** para a protecção de dados, protecção de dados desde a **concepção** e por **defeito**, etc.;

- Não assinale ou não notifique uma violação de dados pessoais, ou não notifique de forma atempada ou completa a violação de dados à autoridade de controlo ou ao titular dos dados;

Coimas Muito Significativas

- Não realize uma **avaliação de impacto** sobre a protecção de dados ou efectue o tratamento de dados pessoais sem autorização prévia ou consulta prévia da autoridade de controlo;

- Não designe um **delegado para a protecção de dados** ou não assegure as condições para o cumprimento das suas funções.

A estas coimas, acresce eventual responsabilidade criminal.

No âmbito de certos sectores como a saúde, banca, seguros, o **risco reputacional** e de **imagem** é muito elevado. Tendo em conta as novas obrigações de reporte em caso de violação de dados pessoais, a sanção para a empresa atingida que representa a perda da confiança dos seus clientes poderá ser muito significativa.

Preparar a Entrada em Vigor do Novo Regulamento

- Envolvimento de vários níveis de decisão no seio da instituição bancaria;

- Avaliar em profundidade como está **estruturado** o negócio em termos de fluxos de dados pessoais e **identificar** bem as **finalidades** para as quais os dados são tratados. É fundamental ter o conhecimento preciso daquilo que se recolhe, como se recolhe, onde se encontra alojado e como é protegido.

- Manter um **registo interno** permanente destes tratamentos, bem como uma lista de tratamentos em outsourcing, e uma cópia dos contratos com prestadores de serviços que envolvam o processamento de dados.

- Estabelecer um grupo interno, incluindo IT, Marketing, Recursos Humanos, Compliance e Legal, de modo a não perder a visão global do negócio e de como o mesmo evolui;

Preparar a Entrada em Vigor do Novo Regulamento

- Nomear um **delegado** para a Protecção de Dados;

- Definição dos termos em que o ***delegado*** para a protecção de dados deverá ser associado a todas as matérias relacionadas com a protecção de dados.

- Realizar outros controles importantes, ao nível da revisão das **políticas de privacidade**, da análise da **adequação** e **proporcionalidade** dos dados tratados às **finalidades** desses tratamentos, procedimentos de **acesso dos titulares dos dados** e de exercício de direitos, definição da **informação** a fornecer as diferentes categorias de titulares dos dados;

- **O novo regime do regulamento determina alterações contratuais** com fornecedores, principalmente em regime de **outsourcing**, determinadas pela entrada em vigor do Regulamento, pelo que deverá existir um registo centralizado;

Autoridade de Controlo

Em Portugal, a Autoridade de controlo é a **Comissão Nacional de Protecção de Dados**;

É importante para os vários sectores sujeitos a uma pressão regulatória importante, como o sector bancário, a existência de uma Autoridade operante, nomeadamente **fornecendo orientações** e contribuindo para um **enquadramento regulatório mais claro e previsível**, estabelecendo uma cooperação com reguladores sectoriais;

O Regulamento permitirá a sujeição das empresas à Autoridade do Estado-Membro onde se localizar o estabelecimento principal.

Obriga a um **nível elevado de cooperação** entre autoridades de protecção de dados e destas com a Comissão Europeia.

Cloud Computing – Protecção de Dados

Membro do Grupo de Peritos da Comissão Sobre Contratos de Cloud Computing

- Lançado pela Comissão Europeia em Outubro de 2013, após processo de selecção ocorrido no Verão de 2013;
- Tem a missão de redigir cláusulas seguras e equitativas para os contratos de computação em nuvem, com base num instrumento opcional;
- O objectivo é identificar as boas práticas utilizadas para responder às preocupações dos consumidores e das pequenas empresas, que frequentemente se mostram relutantes em comprar serviços de computação em nuvem porque os contratos são pouco claros (recomenda-se consulta de materiais no link infra).

URL: http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm

Obrigado | Thank you.

ADVOGADOS

Sociedade Rebelo de Sousa
& Advogados Associados, RL

LISBOA
R. Dom Francisco Manuel de Melo, nº21,
1070-085
T. +351 21 313 2000 | F. +351 21 313 2001

FUNCHAL
Av. Zarco, nº2, 2º,
9000-069
T. +351 291 20 2260 | F. +351 291 20 2261

PORTO (*)
R. Tenente Valadim, nº215,
4100-479
T. +351 22 543 2610 | F. +351 22 543 2611