11/29/2017

Regulamento Geral sobre a Proteção de Redes: Impacto, obrigações e uma grande urgência no setor das empresas dos transportes

Fora de um figurino jurídico, pretende-se alertar as empresas do setor dos transportes para a urgência em identificarem o impacto do novo Regulamento Geral sobre a Proteção de Dados (RGPD), assim como implementarem um Sistema de Gestão da Proteção de Dados (SGPD). Não podemos ignorar a rapidez com que os dias vão passando e a aproximação da data limite para a implementação do RGPD.

O novo RGPD coloca novas exigências e novos desafios às empresas para o seu cumprimento obrigatório, a partir de maio de 2018.
Chegados a essa data, pode admitir-se que o órgão de autoridade nacional, a Comissão Nacional de Proteção de Dados (CNPD) paute a sua intervenção por preocupações mais pedagógicas do que sancionatórias.
No entanto, sugere-se que as empresas que não tenham um SGPD, em conformidade com o regulamento europeu, possam evidenciar o cumprimento dos requisitos mais significativos e, ao mesmo tempo, evidenciar que estão a seguir um plano de ação para o cumprimento integral do RGPD. Quanto mais não seja para evitarem cair no severo quadro sancionatório do novo regime jurídico.

Houve tempo desperdiçado

No dia 4 de maio de 2016 foi publicado o Regulamento (UE) 2016/679 relativo à proteção dos dados das pessoas singulares, ao seu tratamento e à livre circulação.

O referido regulamento, que revoga a Diretiva 95/46/CE - Regulamento Geral sobre a Proteção de Dados [Cf. art.º 94 - Revogação da Diretiva 95/46/CE], é da responsabilidade do Conselho e do Parlamento Europeu. Datado de 27 de abril de 2016, entrou em vigor no dia 24 de maio de 2016 e será aplicável na ordem jurídica da UE a partir de 25 de maio de 2018 [Cf. art.º. 99 - Entrada em vigor e aplicação].

Este período de dois anos de "vacatio legis", entre as datas da entrada em vigor e da sua aplicação na ordem jurídica nacional de cada membro da União Europeia, tem como objetivo permitir às empresas uma adaptação adequada e atempada às novas exigências.

Assim, as empresas deveriam: (1) identificar e avaliar a significância dos impactos do novo RGPD na vida das organizações; (2) conceber e implementar um SGPD em conformidade ("compliance") com os requisitos legais aí especificados; (3) garantir a consequente demonstração da responsabilidade ("accountability") no âmbito da proteção de dados das pessoas singulares.

Pelas informações obtidas em contactos com algumas empresas, em especial do setor dos transportes, conclui-se que, e salvo algumas exceções, este período foi e continua a ser desperdiçado. Agora, e sob o peso da consciência tardia das responsabilidades impostas pelo RGPD, começa a sentir-se um certo ambiente de preocupação nas direções das empresas, com as eventuais medidas sancionatórias, num quadro de reforço dos poderes de fiscalização da CNPD.

Em vez de uma adaptação tranquila aos novos paradigmas da proteção de dados, algumas empresas, neste quadro de enorme pressão, poderão ser tentadas a aceitar "soluções rápidas e generalistas" que o mercado sempre oferece, apresentando atalhos metodológicos para a implementação, quanto antes, de sistemas "fast food".

A elaboração de diagnósticos com a inventariação e o mapeamento superficiais dos dados existentes e das respetivas operações de tratamento poderão gerar um sistema de gestão com lacunas de conformidades de todo indesejáveis.

A complexidade do RGPD exige seriedade na conceção e na implementação de um plano

de ação que não queime etapas, que defina o perfil dos recursos humanos a mobilizar, sejam eles internos e/ou externos, e dinamize os esforços coletivos a desenvolver para se deitar “mãos à obra”.
Particular importância deve ser dada à formação sobre o RGPD, orientada para os quadros superiores e para todos os envolvidos nas operações de tratamento de dados. Só assim será possível garantir um ambiente de responsabilidade e de envolvimento positivo de todos quantos terão que garantir uma gestão adequada da mudança da cultura organizativa, para um novo ambiente em conformidade com o regulamento.
A título de exemplo, e quanto à urgência na adequação das empresas ao novo RGPD, pode referir-se o agravamento dos custos administrativos com a revisão de todos os contratos celebrados com clientes, trabalhadores, etc, assim como dos modelos de impressos para a recolha de dados pessoais em utilização durante o atual período de adaptação, sem incluírem as cláusulas que evidenciem o cumprimento do RGPD.

A passagem para um sistema auto regulado de gestão dos dados pessoais, com responsabilidade demonstrada

No exemplo, a seguir apresentado, pode ver-se o que significa a passagem do atual sistema “hetero-regulado” para um sistema “auto regulado”.
Atualmente, e de acordo com a lei 67/98 – Lei da Proteção de Dados Pessoais, quando uma empresa precisa de adotar medidas de controlo, como sejam os sistemas de videovigilância, de geolocalização, de controlo biométrico de acessos ou da assiduidade, é obrigada a notificar a CNPD destas operações de tratamento de dados, com um pedido expresso de registo ou de autorização prévia para a sua implementação.
Com o novo RGPD, cessa o regime de notificação prévia por defeito, sendo os responsáveis pelo tratamento e também todas as entidades que atuem em nome e por conta daqueles, obrigados a implementar um sistema de registo das operações de tratamento de dados, devendo disponibilizar, a pedido da CNPD, os registos respetivos, estabelecendo obrigações específicas de “responsabilidade demonstrada”.
Assim, esta alteração do paradigma atual permite que a CNPD deixe de estar atolada em milhares de processos administrativos de notificações com registos ou autorizações, focando-se no processo de fiscalização da conformidade legal das empresas face ao novo RGPD.
Na sequência dos processos de fiscalização, e caso sejam levantados autos de contraordenação às empresas detentoras dos dados, e por isso responsáveis pelo seu tratamento, o novo quadro sancionatório prevê as seguintes sanções normais ou graves, a saber:
- As sanções consideradas normais podem atingir 10 milhões de euros ou até 2% do seu volume de negócios anual a nível mundial, correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado;
- As sanções consideradas graves podem atingir 20 milhões de euros ou até 4% do seu

volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.
Com este quadro sancionatório deixa de ser rentável a pouca vergonha da traficância dos dados das pessoas singulares, num processo comercial de venda em mão das bases de dados – veja-se o caso recente, do "toma lá, dá cá" entre empresas dos ramos elétrico e de telecomunicações, com subcontratados para as campanhas de telemarketing, como tem sido divulgado em vários órgãos de informação.
Com o novo RGPD a responsabilidade pelo tratamento dos dados envolve toda a cadeia de empresas, incluindo as subcontratadas. Estas passam também a ser responsáveis pela avaliação da legalidade das bases de dados que os seus clientes entregam para as campanhas comerciais que solicitam. Assim, terminará o cinismo comercial de se refugiarem no argumento de que "trabalham com os dados que os clientes lhes entregam".
Antes de terminar e sem querer cansar os leitores com termos e definições, entende-se necessário referir, de forma breve, três conceitos fundamentais do RGPD, a saber: dados de pessoas singulares, responsável pelo tratamento dos dados e tratamento de dados.

Dados, quais dados?

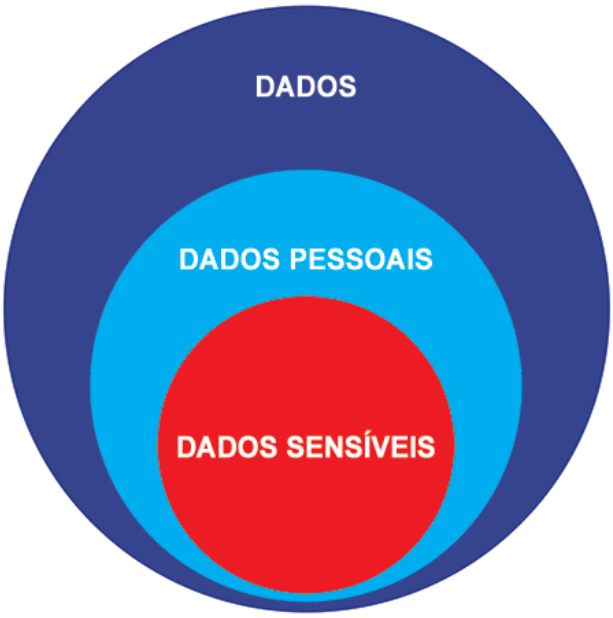

FIGURA 1 - **ILUSTRAÇÃO DA RELAÇÃO ENTRE OS DIVERSOS TIPOS DE DADOS**

Os dados, objeto do RGPD em apreço, são os dados das pessoas singulares. No seu art.º 4 – 1, o regulamento define o conceito de dados pessoais como a "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social

dessa pessoa singular."
Para uma melhor compreensão do tipo de dados a tratar, o regulamento distingue, os dados pessoais normais dos dados pessoais sensíveis, como se apresentam na figura 1.
As operações de tratamento de dados sensíveis podem definir-se como operações de "tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa", sendo os «dados relativos à saúde», os "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde", conforme o Art.º 4º - 15.
As empresas realizam este tipo de operações de tratamento de dados sensíveis quer no âmbito do seu relacionamento com clientes ou utentes, quer no âmbito do seu relacionamento com os trabalhadores.
Outras definições a ter em consideração são as definições de dados genéticos (Art.º 4 – 13) e de dados biométricos (Art.º 4 – 14).

Há sempre um responsável pelo tratamento dos dados pessoais...

Se as pessoas singulares são os titulares dos dados, importa clarificar quem é o responsável pelo tratamento dos seus dados.
No Art.º 4 – 7 define-se o responsável pelo tratamento dos dados como sendo "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-membro."
De um modo geral pode dizer-se que qualquer empresa que, para o desenvolvimento da sua atividade, precise de utilizar dados pessoais, obtidos diretamente ou por intermédio de empresas subcontratadas, são sempre os responsáveis pelo tratamento dos dados em conformidade com os requisitos do regulamento.

... e o que é o tratamento de dados?

O tratamento de dados é definido (Art.º4-2) como sendo "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição."

por Sílvio Gomes

Por:
Fonte: