Vida Judiciária

Nº 207 - maio/junho 2018 - 7,50 €

OPINIÃO

ANA ALVES LEAL
Assistente da Faculdade de Direito da Universidade de Lisboa
Advogada

ANA RITA PAÍNHO
Sócia da Anselmo Vaz, Aíra & Associados – Sociedade de Advogados

ANDRÉ FILIPE MORAIS
Advogado da CCA Ontier

ARMÉNIO MAXIMINO
Presidente do Sindicato dos Trabalhadores dos Registos e do Notariado

CLÁUDIA MONGE & JANE KIRKBY
Sócias da BAS Sociedade de Advogados, SP RL

DAVID SILVÉRIO
Advogado da Belzus Advogados

DIOGO PEREIRA DUARTE
Professor Auxiliar da Faculdade de Direito da Universidade de Lisboa
General counsel do Banco de Investimento Global

EDUARDO CASTRO MARQUES & TATIANA MARINHO
Advogados
Nuno Cerejeira Namora, Pedro Marinho Falcão & Associados

GRAÇA CANTO MONIZ
Observatório de Proteção de Dados Pessoais/NOVA Direito

INÊS OLIVEIRA
Consultora de Política Legislativa da Direção-Geral da Política de Justiça / Ministério da Justiça

ISA MEIRELES
Assistente Convidada na Escola de Direito da Universidade do Minho
Advogada-Estagiária

JOÃO GABRIEL
Advogado da Gouveia Pereira, Costa Freitas & Associados Sociedade de Advogados

JOSÉ RICARDO GONÇALVES & PEDRO FERREIRA DE SOUSA
Advogados de PLMJ Advogados

MANUEL VERGARA CÉSPEDES & JUAN FRANCISCO BARALLAT LÓPEZ
Advogados da ILOCAD- Baltasar Garzón Abogados (Espanha)

MANUEL DAVID MASSENO
Professor Adjunto e Investigador Sénior do Instituto Politécnico de Beja

MARTIM BOUZA SERRANO & JOANA CUNHA DE MIRANDA
Advogados da CCA ONTIER

RAPHAEL JOSÉ RIBEIRO
Advogado e Sócio de Queiroz Cavalcanti Advocacia (Brasil)

RÚBEN FONSECA
Advogado da Sociedade de Advogados, João Marcelo e Associados

TIAGO MARCELINO MARQUES
Advogado da RSA Advogados

EDIÇÃO TEMÁTICA LUSÓFONA

PROTEÇÃO DE DADOS

ALEXANDRE SOUSA PINHEIRO

Em entrevista, o Professor da Faculdade de Direito da Universidade de Lisboa, com uma tese de Doutoramento sobre "Privacy e Proteção de Dados", esclarece que o Regulamento Geral de Proteção de Dados, que entra em vigor a 25 de maio, "aplica-se a qualquer profissão ou área de atividade em que circule informação pessoal". Critica ainda: "existiu, e existe, muita desinformação"

"O Tratamento de Dados Pessoais é um *Corporate Risk*"

SOFIA BASTOS DOS SANTOS
Sócia da AskBlue

00207
9 772017 002013

SOFIA BASTOS DOS SANTOS

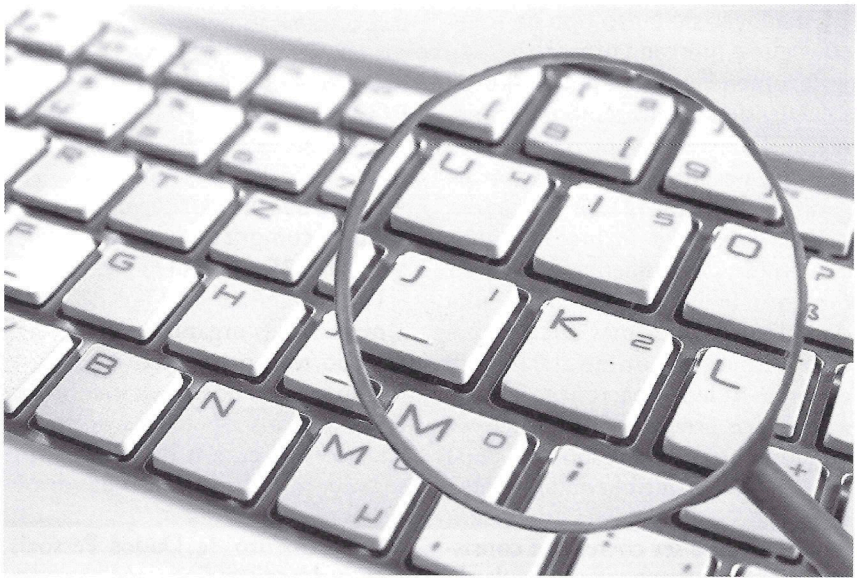
"O Tratamento de Dados Pessoais é um *Corporate Risk*"

A Sócia da AskBlue tem assessorado várias empresas na implementação do Regulamento Geral de Proteção de Dados. Apesar do período transitório de dois anos que as empresas tiveram para efetuarem as necessárias adaptações, Sofia Bastos dos Santos nota que, sensivelmente após o segundo semestre de 2017, começou a haver essa preocupação. Por outro lado, as empresas "perceberam o RGPD somente como um problema de natureza eminentemente jurídico-legal e de segurança informática"

As empresas têm vindo a adaptar-se atempadamente para cumprir com as regras do RGPD?

O Regulamento (UE) 2016/679 do Parlamento e do Conselho Europeu de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, entrou em vigor, de forma simultânea, em 25 de maio de 2016, em todos os Estados-Membros da União Europeia. O Regulamento impõe uma disciplina uniforme entre os vários Estados-Membros a partir de 25 maio de 2018, data em que termina o período transitório de dois anos nele previsto. As empresas e as organizações, privadas e públicas, passam a estar sujeitas a um conjunto de regras de obrigações, cujo incumprimento conduzirá à aplicação de coimas, até ao maior entre € 20 milhões ou 4% do volume de negócios mundial da organização (existem dois níveis de aplicação de coimas cfr. art. 83.º). Na aplicação das coimas serão tidos em consideração diversos fatores, mas a sua amenização dependerá da capacidade das organizações demonstrarem a aplicação das medidas de proteção de dados adequadas. O novo quadro sancionatório eleva a privacidade e a segurança da informação relativa ao tratamento de dados pessoais a um *Corporate Risk*, conduzindo necessariamente a que as organizações considerem esta matéria nas

suas orientações e decisões de gestão. Observamos no mercado português que as organizações começaram de uma forma geral a mobilizar-se para a necessidade de analisar as disposições e implicações do RGPD sensivelmente a partir do final do primeiro semestre de 2017. O período transitório de dois anos não foi de facto aproveitado, na avaliação dos impactos e das necessidades de investimento, na formulação de prioridades e opções e no planeamento das ações a desenvolver. Constatámos, numa primeira fase, que as organizações perceberam o Regulamento somente como um problema de natureza eminentemente jurídico-legal e de segurança informática e, consequentemente, uma matéria a endereçar e resolver através do recurso a competências e meios nestes dois domínios e disciplinas de intervenção.



Quais as principais dúvidas colocadas pelas empresas que vos solicitam assessoria quanto ao novo RGPD?

As dúvidas e as solicitações de assessoria dirigiram-se aos aspetos formais da conformidade legal com as disposições do Regulamento e em paralelo à identificação das opções tecnológicas, ou seja, em termos da recomendação de soluções de software, a adotar em resposta às medidas de segurança no tratamento de dados pessoais. A formulação dos pedidos de assessoria traduziu-se, muito frequentemente, numa consulta ou/e pedido de prestação de serviços profissionais para a "implementação dos requisitos mínimos do RGPD" na organização em causa. Esta abordagem tem implícita a perceção comum às organizações do carácter supostamente prescritivo do Regulamento e também da suposição frequente assumida pelos gestores da existência de "requisitos mínimos" de conformidade. O Regulamento define princípios, estabelece regras e obrigações a observar pelos responsáveis pelo tratamento de dados, pelos seus eventuais subcontratantes e responsáveis conjuntos, mas não é prescritivo quanto às medidas, em especial as de segurança, de natureza técnica e organizativa /processual, ou procedimental (art. 32.º), a implementar pelas organizações. Não o é, nem em rigor o deveria ser. Uma medida de segurança, independentemente da sua natureza, visa a atuação sobre um risco identificado, com um dado objetivo de controlo, a prevenção do risco, a sua eliminação, ou até a transferência para terceiros (exemplo: contrato de seguro). Os riscos decorrem das vulnerabilidades existentes e incidem sobre os ativos de uma organização, neles se incluem os ativos de informação, designadamente a informação que resulta do tratamento de dados pessoais. Os riscos associados às distintas atividades económicas são naturalmente diferentes, não obstante possam existir alguns riscos comuns. Num dado setor de atividade económica, organizações operacionalmente diferentes, ao nível do seu modelo organizativo, dos seus processos de negócio e da tecnologia de suporte (software, bases de dados e infraestrutura de hardware, comunicações, entre outros elementos), terão necessariamente vulnerabilidades distintas. A avaliação integrada de riscos e das vulnerabilidades permite definir os objetivos de controlo e, em função destes, determinar as medidas de segurança necessárias, que poderão ser de distintas naturezas e tipologias (organizativa, processual, tecnológicas), individualmente consideradas ou conjugadas entre si. Dito isto, "a implementação" dos requisitos de conformidade com o RGPD exige um exercício prévio de identificação e avaliação de riscos e de vulnerabilidades e decisões da gestão das organizações quanto aos objetivos de controlo e, consequentemente, às ações a desenvolver para os endereçar.

> **"O período transitório de dois anos não foi de facto aproveitado, na avaliação dos impactos e das necessidades de investimento, na formulação de prioridades e opções e no planeamento das ações a desenvolver"**

E a adoção de outro tipo de soluções que o mercado oferece?

Recomendações e/ou adoções de soluções de software, embora amplamente divulgadas no mercado, sem a adequada avaliação do contexto organizacional em todas as dimensões relevantes para a formação e desconstrução do problema, podem ter o mesmo efeito daquele que resulta do tratamento de uma "infeção viral com antibiótico" ou do tratamento de uma "infeção bacteriana com o antibiótico errado". As medidas de segurança têm que responder ao(s) objetivo(s) de controlo do(s) risco(s), mas a sua escolha e a sua implementação têm que ser coerente e consistente. Coerente, porque o resultado de uma medida de segurança pode depender da implementação prévia de outra medida de segurança ou do desenvolvimento de um conjunto de ações que são por si mesmas um pré-requisito à implementação dessa medida. Estas variáveis têm que ser endereçadas através do planeamento. Consistente, porque gerir e controlar risco é inevitavelmente um exercício de viabilidade económica e financeira para as organizações. Minimizar risco significa também maximizar o controlo, o que pressupõe investimentos e variações nos custos operacionais, presentes e futuros. Assim, da determinação das medidas de segurança necessárias à efetiva conformidade da organização com o RGPD, à adequação das medidas de segurança, para salvaguarda da privacidade e segurança da informação relativa a dados pessoais, emerge um quadro de opções, naturalmente complexo, face à restrição financeira. Os recursos são sempre limitados. A regulação não gera negócio e, como tal, o RGPD será um desafio à gestão das organizações.

Crê na boa preparação das empresas para cumprir com a nova legislação, após 25 de maio?

Penso que, até ao final de 2018, a maioria das organizações do setor privado se concentrarão e trabalharão no sentido de se prepararem para responder aos aspetos de conformidade formal com o RGPD, no que se refere ao cumprimento das disposições relativas aos Princípios Básicos do Tratamento de Dados Pessoais, incluindo as condições de consentimento (artigos 5.º a 11.º), aos Direitos dos Titulares dos Dados (artigos 12.º a 15.º) e ainda ao Registo das Atividades de Tratamento (cfr. Artigo 30.º). Contudo, a complexidade, o esforço e o enorme desafio para todas as organizações, sem exceção, está na conformidade com os princípios e disposições previstos nos artigos 25.º e 32.º do Regulamento, destinados a promover a responsabilização das organizações, respetivamente: proteção de dados desde a conceção e por defeito; segurança do tratamento. A conformidade com estes dois artigos não é uma ação, é sim um processo que exige visão, recursos, planeamento e tempo de execução, pelas razões que procurei explicitar até aqui. É uma realidade incontornável que o período transitório previsto no Regulamento termina a 25 de maio de 2018, data a partir da qual se espera que vigore uma disciplina uniforme entre os vários Estados-Membros da União Europeia. A privacidade e a segurança da informação relativa a dados pessoais são de facto apenas mais duas dimensões de risco a acrescentar ao ecossistema global de uma organização, a contemplar num "Referencial de Gestão Integrada do Risco", que se requer multidisciplinar e parte integrante das disciplinas internas de gestão de uma organização. É esta a mudança no paradigma de gestão que se impõe às organizações em Portugal.

> **"As medidas de segurança têm que responder ao(s) objetivo(s) de controlo do(s) risco(s), mas a sua escolha e a sua implementação têm que ser coerente e consistente"**

Uma questão prática: como é que se exige que um terceiro – sem qualquer relação contratual com o consumidor – seja obrigado a eliminar e a esquecer dados pessoais?

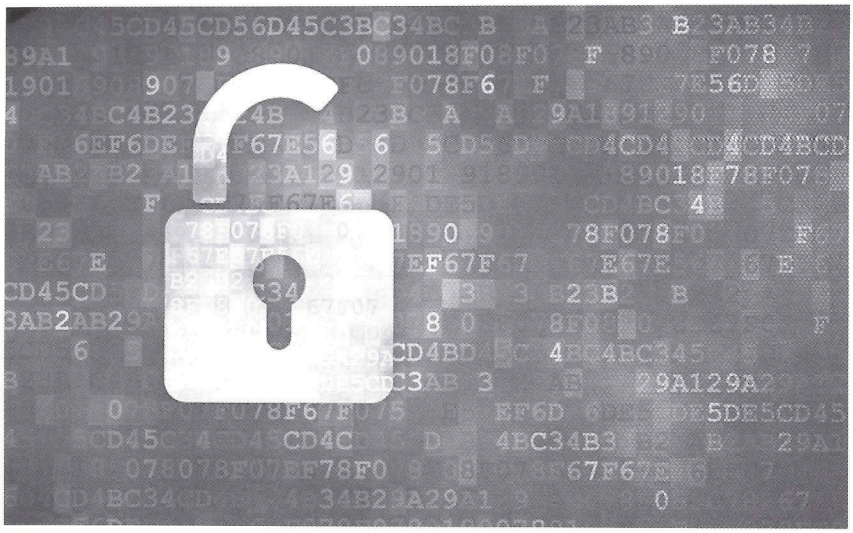
O Regulamento define dois conceitos, o de Responsável pelo tratamento de dados, que "determina as finalidades e os meios de tratamento dos dados pessoais", e o de Subcontratante, que "trata os dados pessoais por conta do Responsável pelo tratamento e de acordo com as suas instruções" (art. 28.º). O Regulamento introduz um novo papel e novas responsabilidades acrescidas para as entidades subcontratadas. Os Subcontratantes devem apresentar garantias de execução de medidas de segurança adequadas a proteger os direitos dos titulares dos dados e não podem contratar subcontratantes sem autorização do Responsável pelo tratamento de dados. O titular dos dados exerce os seus direitos, neles se incluindo o direito ao esquecimento, perante a entidade Responsável pelo tratamento de dados, assumindo obviamente que o tratamento de dados pelo Responsável é lícito nos termos previstos pelo RGPD. Na sociedade atual em que os dados e a informação neles contida é transmitida de forma voluntária pelos titulares, circulando através dos múltiplos canais e repositórios de dados distribuídos, etc., os comportamentos individuais podem conduzir lamentavelmente à abdicação de direitos. Neste ponto, acredito que é a educação a variável que fará a diferença...

Que papel devem ter as autoridades de supervisão?

O papel das autoridades de supervisão é fundamental e será um pilar do sistema. Os níveis de experiência, de organização e de preparação das autoridades de supervisão no quadro dos distintos países da UE é muito díspar. A capacidade e o efetivo exercício da função de supervisão dependem da adequação da estrutura organizativa, das competências internas, necessariamente multidisciplinares e obviamente dos meios financeiros, mas em resposta a um plano de alinhamento estratégico com um dado referencial, isto é, com um "modelo de supervisão alvo", tecnicamente viável, face ao ponto de partida atual, e financeiramente sustentável. Em Portugal não precisamos de "inventar a roda", temos que saber olhar criticamente para outras realidades, ver o que funciona e já deu provas de resultar.

Que desafios vem colocar a tecnologia *blockchain* à legislação de proteção de dados?

A tecnologia *blockchain* é algo ainda muito novo, com um espectro de aplicação potencial vastíssimo. A desintermediação na vida económica e no plano social poderá ser no limite total, com um impacto na sociedade, tal como a conhecemos hoje, ainda não previsível. Não tenho uma opinião formada, tenho apenas reflexões, as mesmas que me fazem pensar que a internet viabilizou as mesmas redes sociais que permitiram a "Primavera Árabe" e a *Cambridge Analytics*. A evolução tecnológica determinará a necessidade de revisão constante da regulação. Face à tecnologia *blockchain*, certamente não estaremos a falar no futuro do RGPD, mas sim de outra qualquer regulação.



E relativamente à inteligência artificial?

Ao contrário, a inteligência artificial já é uma realidade, mas ainda é uma tecnologia muito cara, daí a sua aplicação por enquanto restrita. Com a inteligência artificial, o software tem a capacidade de aprender com o comportamento humano. O exemplo mais fácil e intuitivo é o dos carros com piloto automático. Estes carros existem, porque o software programou-se a partir da leitura do modo de condução de humanos "bons condutores", ou seja, os algoritmos matemáticos na inteligência artificial desenvolvem-se a partir da interação simultânea com o comportamento humano. Dito de outra forma, com a inteligência artificial os algoritmos do software incorporam o comportamento humano. Ora o comportamento é um código único do seu titular, e sendo um "bom comportamento" é um ativo do seu titular, porque passou a ter valor de mercado. Creio que na inteligência artificial o que está em causa em termos do Direito não é a proteção dos dados pessoais dos titulares, mas sim a "incorporação de direitos" na construção do software, pelos proprietários dos "bons comportamentos". Se os proprietários dos "bons comportamentos" são os seres humanos, claramente terá que ser a tributação específica e diferenciada a via de resolução da incorporação de Direitos do Homem no software com inteligência artificial. Para isso a economia desenvolveu no passado a "Teoria das Externalidades". Atividades económicas com externalidades negativas sofrem impostos acrescidos, por outro lado, atividades económicas com externalidades positivas devem ter benefícios ou redução de impostos. A inteligência artificial aplicada à saúde tem valor social, noutros casos causará impactos sociais negativos e o que está em causa é o desemprego. A inteligência artificial obrigará as sociedades a repensar a tributação, a qual terá que cumprir a sua função redistributiva. A teoria económica existe e já é antiga, a sua aplicação será uma questão política.

> **"A necessidade de revisão constante da regulação. Face à tecnologia blockchain certamente não estaremos a falar no futuro do RGPD, mas sim de outra qualquer regulação"**