CONCLUSÕES DA APDSI

Jantar-Debate "RGPD: Mitos e Realidades"

24 de julho de 2019

A APDSI organizou um Jantar-Debate intitulado "RGPD: Mitos e Realidades" no passado dia 9 de julho, na Ordem dos Engenheiros, em Lisboa. Durante cerca de quatro horas foram discutidas as preocupações, reais e atuais, e o futuro do RGPD.

Um ano após a implementação efetiva da lei, a 25 de maio de 2018, foram debatidos os temas relacionados com a aplicação do Regulamento Geral de Proteção de Dados em Portugal. Neste balanço, foram discutidos os desafios e as dificuldades na implementação do RGPD nas instituições públicas e privadas.

O Parlamento aprovou com os votos favoráveis do PS, PSD e do deputado não inscrito Paulo Trigo Pereira, a lei que assegura a execução em Portugal do Regulamento Geral da Proteção de Dados - RGPD. Os restantes partidos, BE, PCP, CDS-PP, PEV e o deputado do PAN, André Silva, optaram pela abstenção na votação final global deste diploma.

Com a mesma votação foi aprovada a proposta de lei sobre tratamento de dados dos tribunais e do Ministério Público, mantendo-se a exclusão da Comissão Nacional de Proteção de Dados - CNPD - da supervisão dessas operações de tratamento. Estas leis estiveram durante o último ano a ser preparadas no grupo de trabalho criado no âmbito da comissão dos assuntos constitucionais e são, assim, aprovadas mais de um ano depois de o RGPD ter entrado em vigor na União Europeia (UE).

O tratamento de dados em contexto laboral, de saúde e nas seguradoras, é uma das vertentes que mais preocupa o público em geral no contexto do RGPD, e do ponto de vista das instituições a aplicação de coimas ou a sua dispensa por um período de três anos é um dos grandes receios, até pelo "terreno" desconhecido que ainda sentem estar a percorrer.

PRIMEIRO PAINEL: "NOVA LEI DE EXECUÇÃO DO RGPD"

O olhar jurídico sobre a "Nova lei de execução do RGPD" esteve a cargo do Professor Alexandre Sousa Pinheiro, da Faculdade de Direito da Universidade de Lisboa, que apresentou a Lei do RGPD e a sua evolução até chegar a 2019 – fase em que está para aprovação.

Portugal está atrasado na colocação da lei em vigor. As empresas não sabem se têm de ter encarregados de proteção de dados, apesar da Administração Pública ser obrigada a tê-los.

Luís Neto Galvão lembra na sua intervenção enquanto moderador do painel que, desde abril de 2018, tem havido um conjunto de polémicas relacionadas com a aplicação do RGPD no âmbito da saúde – nomeadamente seguradoras e recolha de dados biométricos em contexto laboral para controlo de assiduidade – sendo este um dos aspetos negativos apontados pelo Professor.

Neste contexto é importante sublinhar que, **com a entrada em vigor da lei, a Comissão Nacional de Proteção de Dados (CNPD) é a entidade administrativa, independente e com meios próprios, que atribui competências à proteção de dados e aos DPIAs – *Data Protection Impact Assessments*. A lei também veio alterar o funcionamento da CNPD.**

Houve um grupo de trabalho que adotou um projeto no final de 2017 que não foi, contudo, o que chegou à Assembleia da República.

O regulamento, tal como está, significa a não aplicação de coimas a entidades públicas - sem legislação nacional (resultado do art. 83.º do RGPD). Na Alemanha, por exemplo, não estão previstas coimas a entidades públicas.

Para já está previsto que as entidades públicas sejam isentadas de coimas durante três anos, mas esse pedido tem de ser devidamente justificado e expresso à CNPD – a única entidade que pode conceder essa isenção. Todavia, **para os crimes, não há a possibilidade de "desaplicação" da norma dos três anos.**

As penas a aplicar podem ir até quatro anos de prisão por viciação de dados. O tema volta a ser debatido dada a existência de um acordo político sobre os textos da lei de execução do RGPD e da lei orgânica da Comissão Nacional de Proteção de Dados (CNPD).

Os menores de 13 anos, em matéria de consentimento, têm de ser representados pelos seus tutores.

Ainda na teoria, o Professor Luís Antunes, da Universidade do Porto, começou por pegar na questão das coimas para dizer que, tal como está, **sem transposição nacional, não há coimas a aplicar aos infratores (de acordo com o artigo 83.º do RGPD).** Efetivamente, o Governo não queria aplicar coimas, mas essa decisão fora muito criticada pela CNPD.

"Portugal está atrasado na colocação em vigor da lei", afirma o Professor.

Outra questão levantada por Alexandre Sousa Pinheiro e sobre a qual pairam algumas dúvidas prende-se com os dados pessoais integrados no Diário da República. "Há ali muita informação que não tinha que ser do conhecimento geral e que ali continuam sem que tenham equiparação com a finalidade do concurso em questão e, por isso, deviam ser apagadas",

sustenta. A lei prevê a desconexão da informação sempre que for excessiva em relação à sua finalidade inicial.

Já na opinião de Luís Antunes, o regulador deveria atuar mais ativamente sobre conceitos. Já as tecnologias, à medida que vão evoluindo, rapidamente podem e vão criar vazios legais.

O cargo do Encarregado de Proteção de Dados também está ancorado em dúvidas e incertezas. Se, por um lado, **a Administração Pública sabe que tem de ter um EPD, não há uma concretização profunda sobre esta obrigatoriedade para as empresas**. O Encarregado de Proteção de dados não é um auditor e, no caso da AP, é designado pelo titular do poder político.

Códigos de conduta, portabilidade de dados e saúde

Também não existe concordância na definição da avaliação dos dados e dos códigos de conduta a que recorrer, nomeadamente **na aplicação da lei a pessoas falecidas, vertente na qual a lei é "muito imprecisa"**. Admite-se a existência da herança da matéria relativa a dados pessoais na saúde, mas tal não coloca um filho na posição de herdeiro dessa informação.

Sobre a portabilidade, ficou esclarecido que o direito à mesma abrange os dados fornecidos e, sempre que possível, deve ser feita em formato aberto. A anonimização dos dados não resolve os problemas porque, quando é feita de uma forma superficial, é possível identificar a pessoa.

A gravação do material recolhido pelas câmaras de videovigilância só pode ser feita se constituírem matéria criminal. A lei não prevê o apagamento dos dados pessoais, mas sim uma desconexão da informação quando for tida como excessiva face à sua finalidade.

Na saúde, está contemplado o dever de sigilo a investigadores e estudantes da área. Todavia, não existe qualquer referência na lei dedicada às companhias de seguros.

O Professor da Faculdade de Ciências da Universidade do Porto (FCUP) refere ainda que as organizações não estão capacitadas para a adequação ao RGPD não só em termos de recursos

financeiros, mas mais ainda por falta de **recursos humanos qualificados, que começam agora a ser formados (em 2018 não havia DPOs – *Data Protection Officers* – no mercado).**

As organizações não estão capacitadas em recursos humanos e financiamento para implementar o RGPD porque, até 2016, quem fazia o papel de proteção de dados era o regulador; o mercado não tem este tipo de profissionais.

Luís Antunes quer ver prazos de conservação de dados contemplados na lei para esclarecer, sendo que as instituições são todas diferentes entre si, quanto tempo cada uma pode manter os dados em seu poder. "A proteção de dados é uma gestão de risco e temos que minimizar o risco", conclui, enquanto acrescenta que o risco vai sempre existir, seja em modelos de risco mais avançados ou mais contidos.

O Professor entende que, quando verificável, um *data breach* deve ser comunicado à CNPD e ao Centro Nacional de Cibersegurança assim que haja suspeita de ter ocorrido. Quando um incidente é reportado a mais de um supervisor, o DPO é envolvido. Mensalmente estarão a ser feitos cerca de 450 relatórios.

SEGUNDO PAINEL: "O QUE FIZEMOS E ESTAMOS A FAZER PARA ASSEGURAR A CONFORMIDADE COM O RGPD?"

No segundo painel foram partilhadas questões mais práticas sobre o funcionamento diário, desafios, reestruturação e adaptação das empresas à nova lei.

No Instituto de Informática o RGPD começou a ser preparado com antecedência

Com a moderação de Wilson Lucas, a APDSI contou com João Sequeira, como primeiro interveniente deste painel. Diariamente, o Vive Presidente do Instituto de Informática processa

um volume de dados muito significativo e é também responsável pelo tratamento dos dados pessoais dos cerca de 300 trabalhadores do Instituto.

João Sequeira demonstrou a mudança organizacional que foi implementada no Instituto para receber e compreender o RGPD na instituição e junto dos seus *stakeholders*.

Quanto ao caminho até se chegar à data de hoje, o Instituto de Informática teve de percorrer vários níveis evolutivos neste sentido:

- Foi criado um Plano de Integridade e Transparência;
- Foi feito um protocolo com o Centro Nacional de Cibersegurança;
- Foi ministrado um curso de *e-learning* sobre RGPD a cerca de 400 colaboradores do II, IP e foi feito um trabalho de sensibilização dos dirigentes para esta questão;
- Foi definido um novo modelo de Governação e criada uma área de proteção de dados e segurança de informação;
- Foram realizadas várias análises PIA - *Privacy Impact Analysis*;
- Foi disponibilizada uma página na web com FAQs sobre o que fazer em determinados cenários;
- No RGPD 70% são processos e o restante é tecnologia.

A partir do RGPD tudo na banca passou a estar relacionado com proteção de dados

Cristina Máximo dos Santos, *Data Protection Officer* (DPO) na Caixa Geral de Depósitos (CGD), olha para todo este processo como uma oportunidade de melhoria dos serviços, de levar mais longe as organizações, ganhando a confiança de trabalhadores e parceiros, e lamenta que se tenha generalizado o medo à volta da nova lei.

A DPO relata que, na instituição que representa, os desafios tecnológicos que o RGPD trouxe são enormes e, por isso, a articulação da lei com a componente tecnológica é feita com extremo detalhe e cautela, apesar de, nesta altura e à semelhança do que se passa em todo o setor bancário, afirmar que até têm sido poucos os pedidos de exercício de direitos e os esclarecimentos sobre o RGPD por parte dos clientes. Enquanto DPO, assegura que uma instituição grande só será bem-sucedida neste processo estiverem dotados de uma equipa de apoio exclusiva e dedicada, e se mantiverem uma boa e estreita relação de trabalho e articulação com os profissionais informáticos.

Quanto aos novos poderes que a lei nacional atribui ao *Data Protection Officer* para realizar auditorias, Cristina Máximo dos Santos refere que, sob pena de se tratar de um exercício meramente teórico, o efetivo controlo da conformidade passa por reconhecer e atribuir ao DPO a possibilidade de verificar/auditar, comprovando, se os princípios do RGPD que regem o tratamento dos dados e as recomendações do DPO são efetivamente cumpridas pelo responsável pelo tratamento. À semelhança do que sucede com outros aspetos da atividade bancária, o âmbito das auditorias sobre proteção de dados não deve estar limitado às ISO, que, aliás, neste momento, estão em desenvolvimento no que respeita à proteção de dados.

CONCLUSÕES:

- Para a DPO na CGD o RGPD centra-se no titular dos dados no epicentro das atividades de tratamento de dados, atribuindo-lhe o controlo sobre os seus dados pessoais, mas afirma que, no setor bancário, esses titulares não têm sido particularmente dinâmicos nesta matéria, em linha, aliás, com o que se tem verificado no setor bancário na União Europeia, conforme assinalado pela European Banking Federation.

- A relação institucional com a CNPD enquanto autoridade de controlo tem sido pouco significativa, desejando-se proximidade entre a banca e a CNPD, daí que Cristina Máximo dos Santos defenda soluções colaborativas e de interação, como reuniões temáticas sobre proteção de dados entre a CNPD e os DPOs do setor bancário, que não envolvem nem mais dinheiro nem mais pessoas e lamenta que alguns subcontratantes se estejam a aproveitar do momento e "à boleia" do RGPD para tentar rever e aumentar o valor dos contratos celebrados.

- Na banca é obrigatória a nomeação de um DPO, sendo que a arquitetura da supervisão bancária sofreu, desde 4 de novembro de 2014, uma alteração profunda, tendo sido atribuídas ao Banco Central Europeu competências exclusivas em matéria de supervisão prudencial, cabendo ao Banco de Portugal a supervisão comportamental.

- A regulação da atividade bancária é atualmente assegurada a nível transnacional, designadamente a nível europeu, mas a proteção de dados resulta, em muitos casos, da articulação entre o RGPD e a lei nacional dos Estados, como é o caso da lei nacional em curso de aprovação e os regulamentos emitidos pela CNPD.

- Cristina Máximo dos Santos prevê desafios exigentes no cumprimento de obrigações legais, dificilmente compatíveis, resultantes da legislação sobre proteção de dados e da regulação da atividade bancária.

Como está a funcionar o RGPD nos Serviços partilhados do Ministério da Saúde (SPMS)

Ana Boto (SPMS) refere que existe uma limitação dos recursos financeiros e humanos e que a maioria das organizações não tem ainda maturidade suficiente para conhecer bem e cumprir com o RGPD. Neste sentido, o RGPD deve ser olhado como uma oportunidade para melhorar os processos tecnológicos num esforço de adaptação que a instituição que representa tem feito, nomeadamente junto dos seus subcontratantes e responsáveis de várias áreas.

O Novo Regulamento, diz, é um caminho progressivo necessário e uma oportunidade para mudar mentalidades e culturas.

CONCLUSÕES:

- O trabalho de consciencialização nem sempre tem sido muito informado, daí que a sensibilização dos intervenientes deva ser feita paulatinamente (o caminho faz-se caminhando);

- A nossa atual cultura não é a de proteção de dados, mas as gerações futuras têm muito a ganhar com o RGPD;
- Auditar ou verificar um procedimento é tarefa do encarregado de proteção de dados;
- Um DPO não é um auditor; a tarefa de auditar tem uma especificidade que não é compatível com uma *checklist*.

SOBRE A APDSI

Criada em 2001, a Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI) tem por objetivo a promoção e desenvolvimento da transformação e inclusão digital em Portugal, reunindo com este interesse comum profissionais, académicos, empresas, organismos públicos e cidadãos em geral.

Na linha destes propósitos a APDSI tem vindo a desenvolver diversas atividades em torno de causas tecnológicas e societais, que se traduzem num conjunto de eventos, recomendações e estudos realizados por grupos de trabalho multidisciplinares em diversas áreas de intervenção, como a Segurança, os Serviços Públicos Digitais, a Saúde, a Cidadania e Inovação Social, o Território Inteligente, a Governação das TIC, a Inteligência Digital, a Política Digital e Governança, os Futuros da Sociedade da Informação e as Competências digitais.
Em todos estes trabalhos a APDSI procura identificar as tendências de evolução e também as interações entre as tecnologias e outras dimensões sociais e económicas, contribuindo com uma visão mais aberta para a discussão e tendo como meta a eficaz perceção e implementação destes conceitos na Sociedade Portuguesa. A APDSI tem o Estatuto de Utilidade Pública e foi em 2008 reconhecida como ONGD.

ASSOCIE-SE

URL | www.apdsi.pt
email | secretariado@apdsi.pt

APDSI
ASSOCIAÇÃO
PARA A PROMOÇÃO E DESENVOLVIMENTO
DA SOCIEDADE DA INFORMAÇÃO

Associação de Utilidade Pública
ONG – Organização Não Governamental

Rua Alexandre Cabral, 2C – Loja A
1600-803 Lisboa – Portugal
URL: www.apdsi.pt

Tel.: (+351) 217 510 762
Fax: (+351) 217 570 516
E-mail: secretariado@apdsi.pt