A PROTEÇÃO DE DADOS PESSOAIS E OUTRAS FUNÇÕES DO ESTADO

8 de março de 2018
Observatório de Proteção de Dados Pessoais/NOVA Direito

Coordenação

Francisco Pereira Coutinho
Graça Canto Moniz

Membros

André Inácio
Afonso Ferreira
Emellin de Oliveira
Graça Canto Moniz
Martinho Lucas Pires
Ricardo Rodrigues de Oliveira
Teresa Vale Lopes

“Proteção de dados pessoais e outras funções do Estado”

O Observatório de proteção de dados pessoais do CEDIS/FDUNL promove, no próximo dia 8 de março, uma discussão sobre “Proteção de dados pessoais e outras funções do Estado”.

O principal objetivo deste segundo workshop do Observatório é discutir a proteção de dados pessoais segundo uma perspetiva diferente daquela que tem vindo a vingar na atualidade, marcada pela entrada em vigor do Regulamento 2016/679, aplicável a partir de Maio de 2018. Pretendemos alargar os termos do debate em torno da proteção de dados pessoais a temas novos, nacionais e europeus, suscitados naquele diploma, na reforma, iniciada em 2012 pela Comissão Europeia, que lhe deu corpo e em jurisprudência recente.

No primeiro painel, focado em temas nacionais, propomos discutir as vulnerabilidades do Estado português e as potencialidades de novas tecnologias como o “blockchain” para as mitigar. Mas além de se proteger a si próprio, o Estado tem a função de garantir a segurança e a defesa dos seus cidadãos respeitando os seus direitos fundamentais, designadamente em matéria de dados pessoais. Esse será o debate travado nas duas últimas apresentações do primeiro painel centradas nos poderes dos serviços secretos portugueses e nos seus limites constitucionais.

No segundo painel, centrado em temas europeus, o caso *Digital Rights Ireland* coloca interessantes questões sobre os limites do acesso a dados pessoais, pelas autoridades públicas dos Estados-Membros, com a colaboração de entidades do setor privado, no caso operadoras de telecomunicações. Segue-se uma apresentação sobre as regras que regulam os tratamentos de dados pessoais realizados pelos organismos da União Europeia e, por fim, a perspetiva da polícia judiciária e do Ministério Público sobre a Diretiva 2016/680 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.

Programa para o workshop "Proteção de dados pessoais e outras funções do Estado"

8 de março de 2018

Sala do Conselho Científico da NOVA Direito

9h30 – Receção e abertura: Professor Francisco Pereira Coutinho

10h – Painel temático 1 – Perspetivas nacionais

Moderação: Filipe Pathé Duarte *(VisionWare/UAL/ISCSPI)*

Oradores:

- Lino Santos (*NOVA Direito*) – O Blockchain e o tratamento de dados pessoais por parte do Estado
- Ana Rita Gil *(Tribunal Constitucional/NOVA Direito)* – A decisão do Tribunal Constitucional sobre a anterior lei das secretas
- Sérgio Azevedo (*Deputado PSD/NOVA Direito*) – A nova lei das secretas

11h30 – Painel temático 2 – Perspetivas europeias

Moderação: Helena Lopes Xavier (*HALX advogados)*

Oradores:

- Francisco Pereira Coutinho *(NOVA Direito)* – O caso *Digital Rights Ireland*
- Inês Oliveira Andrade de Jesus *(Observatório de Proteção de Dados Pessoais/DGPJ)* – O tratamento de dados pessoais pelos organismos da União Europeia

13h – Encerramento

10h – Painel temático 1 – Perspetivas nacionais

Moderação: Filipe Pathé Duarte *(VisionWare/UAL/ISCSPI)*

O Blockchain e o tratamento de dados pessoais por parte do Estado

Lino Santos[1]

A 25 de maio de 2018 entra em vigor o novo Regulamento Geral de Proteção de Dados (RGPD). Relativamente à actual Lei n.º 67/98, o Regulamento trás um conjunto de alterações substanciais, de entre as quais se destacam uma maior proteção dos direitos dos titulares on que respeita à recolha e tratamento de informação de passagem na utilização de redes sociais e outras aplicações da internet; regras mais apertadas no tratamento de categorias especiais de dados pessoais; a definição de uma idade a partir da qual deixa de ser necessária autorização parental para utilização de serviços da sociedade da informação; ou ainda, e relevante para o tema em apreço, a necessidade de aplicação de controlos de segurança, quando os dados são maioritariamente tratados em ambiente digital.

Neste contexto a tecnologia de blockchain - tornada conhecida por servir de base às várias implementações de criptomoeda - tem sido apresentada, em diversos setores, como ideal para garantir a privacidade e a proteção de dados pessoais no ciberespaço, e desta forma, cumprir a parte das normas do RGPD relacionada com as boas práticas de segurança da informação, a pseudo-anonimização dos dados ou o princípio do privacy-by-design.

Blockchain, como o nome indica não é mais do que uma cadeia de blocos onde são registadas "transações" - ou acordos entre partes sem a necessidade de uma entidade central - salvaguardadas com mecanismos de cifra forte, de forma a que qualquer alteração num dos elos da cadeia resulta na perda de integridade de toda a cadeia. Cada "transação" é replicada automaticamente em vários nós geograficamente distribuídos, em cópias da mesma cadeia. A introdução de uma transação na cadeia é sujeita a um mecanismo de eleição entre os vários nós participantes que garante a integridade da cadeia.

São vários os países que desenvolveram ou têm preparados pilotos para utilização de blockchain, como forma de mitigar algumas das preocupações e problemas dos governos relativamente à proteção dos dados pessoais dos seus cidadãos. Existem

[1] Mestre em Direito e Segurança pela Faculdade de Direito da Universidade Nova de Lisboa, licenciado em Engenharia de Sistemas e Informática pela Universidade do Minho, foi coordenador de Operações no Centro Nacional de Cibersegurança e Diretor de Segurança e Serviços à Comunidade na Fundação para a Computação Científica Nacional, Diretor do serviço de resposta a incidentes de segurança informática CERT.PT e Oficial de ligação nacional à Agência Europeia de Cibersegurança-ENISA. Membro do European Commission Expert group to support the feasibility study on the implementation of a European-wide Early Warning and Response Systems (EWRS) against cyber-attacks and disruptions in the context of the implementation of the Cyber Security Directive (2013). Membro da Comissão instaladora do Centro Nacional de Cibersegurança.

exemplos de utilização desta tecnologia no registo de propriedade, no registo de dados de saúde, voto electrónico ou cobrança de impostos.

De um ponto de vista arquitetural, o blockchain foi criado com o objetivo de criar uma cadeia de registos mantendo a integridade e disponibilidade dos dados registados e o seu escrutínio por todas os seus participantes. Não foi criada para garantir a confidencialidade dos referidos dados. Para responder a este desiderato, algumas das soluções recorrem a cadeias privadas (onde os participantes ou nós de cada cadeia são o Estado e o cidadão), diminuindo drasticamente a resiliência da cadeia.

Em suma, a arquitectura subjacente ao blockchain apresenta características muito interessantes para mediar a relação entre o cidadão e o Estado e o tratamento de dados pessoais, a maior parte das vezes muito sensíveis, por este último.

O Acórdão n-º 403/15 do Tribunal Constitucional

Ana Rita Gil[2]

No Acórdão n.º 403/15, o Tribunal Constitucional apreciou, em sede de fiscalização preventiva da constitucionalidade, uma norma constante de diploma que aprovava o Regime Jurídico do Sistema de Informações da República Portuguesa, a qual previa que os oficiais de informações do SIS e do SIED podiam aceder a dados de tráfego, de localização ou outros dados conexos das comunicações. No referido acórdão, o Tribunal considerou que o acesso aos referidos dados consubstanciava uma ingerência na vida privada dos cidadãos, e que a lei em causa não dispunha de garantias suficientes para salvaguarda dos direitos fundamentais em causa. Mais considerou que a mesma violava o art. 34.º da Constituição.

Entretanto, foi aprovada a Lei Orgânica n.º 4/2017, que aprova e regula o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do SIS e do SIED. Esta lei visou responder ao primeiro "chumbo" do Tribunal Constitucional com um reforço das garantias de salvaguarda do direito à privacidade dos cidadãos, mas encontra correntemente a ser apreciada pelo Tribunal Constitucional em sede de fiscalização abstrata sucessiva.

[2] Ana Rita Gil é Licenciada em Direito pela Faculdade de Direito da Universidade de Coimbra e Doutora em Direito, na especialidade de Direito Público, pela Faculdade de Direito da Universidade Nova de Lisboa. É Professora Convidada da Faculdade de Direito da Universidade Nova de Lisboa e da Universidade Católica Portuguesa e Assessora do Gabinete de Juízes do Tribunal Constitucional desde 2010.

A nova lei das secretas

Sérgio Azevedo[3]

A produção de informações acompanhou a história da fundação de Portugal. Desde a afirmação da nossa nacionalidade até aos dias presentes, passando por um período negro de perseguição politica. As ameaças globais obrigam a que os serviços de informação respondam às vulnerabilidades trazidas pela globalização dotando o Estado do benefício que o Principiis Obsta pode traduzir não apenas no plano mera segurança interna e externa, mas também na proteção de sectores estratégicos do Estado que garantem igualmente a sobrevivência do Estado de direito democrático. O acesso a metadados pelos serviços de informação encontram tranquilidade jurídica na sua exigível autorização e controlo por autoridade judicial. Este requisito vem suprimir a inconstitucionalidade anteriormente decretada pelo TC. São apenas mais um mecanismo de antecipação. Uma antecipação fiscalizada pela forma judicial e civil, pelo conselho de fiscalização, mas são também novos suportes à cooperação entre serviços e forças de segurança em resposta às crescentes ameaças não tradicionais à segurança nacional e coletiva.

11h30 – Painel temático 2 – Perspetivas europeias

Moderação: Helena Lopes Xavier (*HALX advogados)*

Pode uma lei que transpõe uma diretiva que foi declarada inválida produzir algum tipo de efeitos jurídicos?

Francisco Pereira Coutinho[4]

Esta apresentação tem como propósito discutir a aplicabilidade da Lei 32/2008, de 17 de julho, que transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, à luz, por um lado, das decisões do Tribunal de Justiça *Digital Rights Ireland* (C-293/12 e C-594/12), que declarou a invalidade da Diretiva 2006/24, e *Tele2* (Processos apensos C-203/15 e C-698/15), que veio limitar fortemente a possibilidade de os Estados-Membros adotarem regulamentação nacional que preveja, para efeitos de luta contra a criminalidade, uma

[3] Licenciado em Direito. Doutorando em Direito e Segurança pela Faculdade de Direito da Universidade Nova de Lisboa, investigando sobre "A fiscalização do Sistema de Informações da República Portuguesa e o alcance do Principiis Obsta na segurança do Estado". Deputado à Assembleia da República.

[4] Professor da Faculdade de Direito da Universidade Nova de Lisboa e membro do CEDIS – Centro de I & D sobre Direito e Sociedade da Faculdade de Direito da Universidade Nova de Lisboa.

conservação generalizada e indiferenciada de todos os dados de tráfego e de todos os dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica, e, por outro, do acórdão do Tribunal Constitucional n.º 420/2017, de 13 de julho, que não julgou inconstitucional a norma da Lei 32/2008, de 17 de julho, que estabelece o dever de os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações conservarem pelo período de um ano os chamados "dados de base".

O tratamento de dados pessoais pelos organismos da União Europeia

Inês Oliveira Andrade de Jesus[5]

A aprovação de um novo regime de proteção de dados pessoais aplicável ao setor público dos Estados Membros - entenda-se, a aprovação do Regulamento (UE) 2016/679 ou Regulamento Geral da Proteção de Dados (RGPD) - espoletou a necessidade de rever as normas aplicáveis aos organismos da União Europeia. Recorde-se que o tratamento de dados pessoais pelas instituições e órgãos comunitários é (ainda) disciplinado pelo Regulamento (CE) n.º 45/2001, que, na sequência da aprovação da Diretiva 95/46/CE, veio prever um regime especial para a estrutura institucional da então Comunidade Europeia, tendo por referência, sublinhe-se, o regime geral plasmado na citada Diretiva.

Enquanto no processo legislativo que levou à aprovação do Regulamento (CE) n.º 45/2001 era a Diretiva 95/46/CE que iluminava as regras a prever, agora, na revisão das normas do Regulamento (CE) n.º 45/2001 gizada pela Comunicação COM (2017) 8 final, que acolhe a proposta de novo regulamento, o legislador europeu visa o alinhamento com o RGPD.

Atentando na proposta de novo regulamento a aplicar aos organismos da União, são muitas as continuidades face ao regime ainda em vigor, cumprindo destacar o âmbito de aplicação do futuro regulamento. Com efeito, o regime especial (face à Diretiva 95/46/CE) aplica-se e continuará a aplicar-se às instituições e órgãos da União, não abrangendo, porém, o tratamento de dados operacionais feito pelas agências com competências penais - referimo-nos à Europol e à Eurojust, já criadas, mas também à futura Procuradoria Europeia, ainda a criar, que também não será abrangida, à semelhança das duas agências já referidas.

Uma leitura atenta do que se deixa dito leva-nos à distinção entre dados administrativos (por exemplo, os dados pessoais dos trabalhadores das agências em apreço) e dados operacionais (dados tratados no âmbito das competências das referidas agências). Assim, o tratamento de dados administrativos rege-se pelo regime do (ainda em vigor) Regulamento (CE) n.º 45/2001, enquanto o tratamento de dados operacionais

[5] Licenciada (2008) e Mestre (2010) em Direito pela Faculdade de Direito da Universidade Nova de Lisboa. Doutoranda (desde 2015) em Administração Pública no Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa. Desempenhou funções no Centro Nacional de Informação e Arbitragem de Conflitos de Consumo (2009) e no Gabinete para a Resolução Alternativa de Litígios (GRAL)/Ministério da Justiça (2010) e foi bolseira de investigação no ISCTE – IUL, na área da proteção de dados pessoais (2011). Atualmente é Consultora de Política Legislativa na Direção-Geral da Política de Justiça (DGPJ)/Ministério da Justiça

tem de observar as normas especiais gizadas na legislação especialmente aplicável. Uma especialidade dentro da especialidade. Vejamos.

A Europol (Agência da União Europeia para a Cooperação Policial) encontra regulação no Regulamento (UE) 2016/794, pelo que os dados operacionais tratados no exercício das suas competências estão sujeito ao regime especial aí plasmado. A Agência Europeia para a Cooperação Judiciária Penal (Eurojust) foi criada pela Decisão do Conselho 2002/187/JAI, que se encontra em processo de revisão (cf. COM (2013) 535 final). Note-se que o regulamento proposto para regular esta agência também acolhe um regime especial para os dados operacionais. O mesmo sucede na proposta que visa instituir a Procuradoria Europeia (cf. COM (2013) 534 final).

Em termos gerais, esta dualidade de regimes – coexistem um regime geral e regimes especiais para as agências que se dedicam à cooperação policial e judiciária em matéria penal – espelha a duplicidade de regimes criada pelo RGPD e pela Diretiva (UE) 2016/680, esta que se aplica especificamente ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais. Aliás, esta duplicidade de regimes remonta à legislação transata: já a Diretiva 95/46/CE, aplicável ao mercado interno, era complementada pela Decisão-Quadro 2008/977/JAI, que visou disciplinar o tratamento de dados para fins penais.

Ora, se a crítica à duplicidade de regimes do RGPD e da Diretiva (UE) 2016/680 é pertinente, curial parece também a crítica à dualidades de regimes na estrutura orgânica da União Europeia. Vejamos.

Relativamente ao RGPD e à Diretiva (UE) 2016/680, traga-se à colação o entendimento de Paul De Hert e Vagelis Papakonstantinou ("The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", Computer Law & Security Review 28, 2012, 130-142), que acentuaram que a dualidade de regimes (do RGPD e da Diretiva (UE) 2016/680) foi e está construída sobre uma distinção ilusória entre dados para fins comerciais e dados relativos à segurança. Para os autores, esta distinção provou ser ao longo dos anos artificial, uma vez que dados recolhidos e tratados por entidades privadas para fins comerciais podem ser acedidos por autoridades públicas. E vice-versa. Acresce que o âmbito de aplicação dos instrumentos é extramente difícil, se não mesmo impossível, de delimitar, insistindo-se em dois instrumentos separados e arriscando-se a prolongar a ambiguidade existente.

Na verdade, a consagração de um diploma específico para o tratamento de dados para fins penais redonda em quatro diferenças (sim, quatro). Com efeito, a Diretiva (UE) 2016/680, em comparação com o RGPD, acolhe as seguintes particulares: o único fundamento legitimador do tratamento é a lei; distingue-se entre categorias de titulares e de dados; estão previstas mais limitações aos direitos dos titulares; e é obrigatório um registo cronológico.

Façamos a mesma análise, agora comparando a proposta de regulamento que visa revogar o Regulamento (CE) n.º 45/2001, o regime geral aplicável à generalidade dos organismos da União, e o Regulamento (UE) 2016/794, que regula a Europol.

Com efeito, o regime especialmente gizado no Regulamento (UE) 2016/794 concretiza-se (igualmente) em (apenas) cinco especificidades. São elas: finalidades (específicas) do tratamento; mais restrições ao acesso e utilização dos dados; facilitada transferência e intercâmbio de dados; rigorosa avaliação da fiabilidade e exatidão dos

dados; e atribuição de competências ao Conselho de Cooperação. No entanto, são de destacar as similitudes (muitas) com o regime geral a aprovar – entenda-se, com o regulamento que vai substituir o Regulamento (CE) n.º 45/2001 ainda aplicável: referimo-nos aos princípios, às categorias de dados e de titulares, à segurança do tratamento, aos direitos dos titulares e aos recursos, bem como ao preceituado atinente à proteção de dados desde a conceção, à violação de dados, à consulta prévia, ao registo e à supervisão.

As diferenças elencadas justificaram a dualidade de regimes? Vai bem o legislador europeu a arquitetar uma proteção de dados pessoais dual? Não nos parece. Embrenhado no desenho legal, esquece-se, o legislador, do que se visa tutelar e salvaguardar, o titular dos dados, que pode ficar desprotegido face a tão complexa "proteção".

13h - Encerramento