"O NOVO REGULAMENTO DE PROTEÇÃO DE DADOS PESSOAIS"

15 de dezembro de 2016

NOVA DIREITO

COORDENAÇÃO DO OBSERVATÓRIO DE PROTEÇÃO DE DADOS

Francisco Pereira Coutinho

Graça Canto Moniz

MEMBROS DO OBSERVATÓRIO

Afonso Ferreira

Emellin de Oliveira

Graça Canto Moniz

Martinho Lucas Pires

Manuel Melo

Teresa Vale Lopes

CEDIS/NOVA DIREITO

Site: protecaodedadosue.cedis.fd.unl.pt

Secretário Executivo: Afonso Ferreira

“O Novo Regulamento de proteção de dados pessoais”

O Observatório de proteção de dados do CEDIS/FDUNL, promove, no próximo dia 15 de Dezembro, uma discussão sobre **o Regulamento 2016/679, de proteção de dados pessoais** (“Regulamento”), aplicável a partir de Maio de 2018.

O principal objetivo deste primeiro workshop é apresentar o novo quadro normativo da proteção de dados pessoais e discutir os principais desafios que decorrem da sua aplicação. Para esse efeito, foram selecionados um conjunto de temas organizados em três painéis temáticos. No primeiro painel, considerando a aplicação do novo regulamento a um conjunto significativo de organizações do setor público e privado, propomos discutir o princípio da responsabilidade das empresas, uma das principais caraterísticas daquele diploma, bem como as novas obrigações que incidem sobre o responsável pelo tratamento de dados. Igualmente relevantes são as novidades em matéria de direitos específicos do titular dos dados, sobretudo o direito à portabilidade, outro dos tópicos que propomos debater.

Tão relevante quanto a proteção dos dados pessoais é a segurança dos mesmos, cuja discussão será lançada num segundo painel temático. As práticas de cibersegurança, e as novas obrigações e responsabilidades em matéria de segurança da informação e em matéria de gestão de incidentes de violação de dados surgem de forma reforçada no Regulamento, como componente essencial de uma proteção eficaz e completa dos dados pessoais. Por outro lado, a necessidade de um novo regime legal nesta área resultou da constatação da desadequação das soluções legais consagradas na Diretiva 95/46/CE, que o Regulamento vem agora revogar, aprovada numa época em que apenas 1% da população da União Europeia tinha acesso à Internet e o Google ainda não existia enquanto serviço on-line. Considerando que as novidades do Regulamento resultam, sobretudo, da necessidade de responder aos desafios colocados pela “revolução tecnológica” ocorrida nas últimas décadas, as normas aplicáveis ao profiling e aos algoritmos autónomos fazem também parte do nosso programa de trabalho.

Uma importante caraterística da informação, sobretudo da informação digital, é a sua natureza “a-espacial” na medida em que não se encontra circunscrita a um espaço físico,

podendo por isso circular livremente, sem respeito por fronteiras geográficas. O tema das transferências internacionais de dados pessoais, analisado no terceiro painel, tem merecido destaque no debate público da atualidade, sobretudo na sequência da recente jurisprudência do Tribunal de Justiça da União Europeia sobre o caso que ficou conhecido pelo nome do seu promotor, "Schrems". Daí a pertinência em analisar o novo acordo, celebrado entre a União Europeia e os Estados Unidos da América, para regular as transferências internacionais de dados pessoais, bem como as normas sobre as mesmas prescritas pelo novo regulamento. E, sendo os dados dos registos de identificação dos passageiros (PNR), recolhidos e conservados pelas companhias aéreas, considerados dados pessoais, a Diretiva que se aplica a esse tipo de dados, recentemente aprovada no Parlamento Europeu, e a sua relação com o novo Regulamento, constituem um outro ponto de debate.

Programa

9h: Abertura com a apresentação do Observatório: Prof. Dr. Francisco Coutinho

9h30: Painel Temático 1 – Que obrigações para as empresas? Que direitos para os titulares dos dados?

Moderador*:* Dr. João Marques (*Comissão Nacional de proteção de dados*)

Oradores:

- Alberto Souto de Miranda (*Banco Europeu de Investimento*): "O responsável pelo tratamento de dados pessoais no regulamento 2016/679: o que há de novo?"
- Teresa Lopes (*CEDIS*): "Responsabilização e governação das empresas no âmbito do novo Regulamento de Proteção de Dados"
- Graça Canto Moniz (*CEDIS*): "Direitos do titular dos dados pessoais: o direito à portabilidade"

11h15: Coffee Break

11h30: Painel Temático 2 – Que respostas para os novos desafios da revolução tecnológica?

Moderador*:* Dr. Luís Neto Galvão (*SRS Advogados*)

Oradores:

- Manuel Melo (*CEDIS*): "Cibersegurança e Proteção de Dados - Obrigações de Segurança da Informação, Incidentes de Violação de Dados Pessoais e Demonstração de Responsabilidade no Quadro do Regulamento Geral sobre a Proteção de Dados"
- Afonso Ferreira (*CEDIS*): "Profiling e algoritmos autónomos"

13h: Almoço

14h30: Painel Temático 3 – As transferências de dados pessoais, o *Privacy Shield* e a Diretiva PNR

Moderador*:* Dr. João Taborda da Gama (*Gama Glória*)

Oradores:

- Inês Oliveira (*Direção Geral de Políticas Legislativas*): "As transferências de dados internacionais"
- Heraclides Silva (*CEDIS*): "Um novo quadro jurídico para as transferências transatlânticas de dados: o Privacy Shield"
- Martinho Lucas Pires (*CEDIS*): "A compatibilidade do acordo de Privacy Shield face ao direito da União Europeia"
- Emellin de Oliveira (*CEDIS*): "O PNR e a Proteção de Dados: uma análise sobre a transferência da informação dos passageiros dos Estados"

16h: encerramento

Painel Temático 1 – Que obrigações para as empresas? Que direitos para os titulares dos dados?

Moderador: Dr. João Marques (*Comissão nacional de proteção de dados*)

O responsável pelo tratamento de dados pessoais no regulamento 2016/679: o que há de novo?

Alberto Souto de Miranda[1]

O regulamento 2016/679 imputa ao "responsável pelo tratamento de dados pessoais" obrigações que inequivocamente reforçam o seu papel como sujeito determinante na forma como os nossos dados serão efetivamente protegidos. Mas quem é ele e por que é responsável? Apenas por obrigações materiais ou também procedimentais? As empresas estão técnica e financeiramente preparadas para as novas exigências de transparência e segurança? E para lidar com os riscos da "cloud" e de pesadas coimas? Na verdade, o "responsável" responde agora explicitamente pelo cumprimento dos princípios gerais e pela comprovação do mesmo ("accountability"); tem a obrigação específica de proteger os direitos dos titulares "(by design e by default") através da pseudominimização e minimização; a obrigação de segurança e de notificar incidentes de violação de direitos; a responsabilidade pela subcontratação; o dever de proceder à análise do risco, à avaliação de impacto e a consulta prévia; a obrigação de registo das operações; a avaliação da existência de "proteção adequada" nas transferências para países terceiros; enfim, a responsabilidade indemnizatória por danos e a suscetibilidade de coimas e sanções. As empresas têm de interiorizar rapidamente estas mudanças.

[1] Licenciado em Direito (FDUC), pós-graduado em Ciências Jurídicas (FDL) e em Direito Europeu (Universidade Libre de Bruxelles), Mestre, pré-Bolonha, em Direito da União Europeia (FDL). Direção dos Assuntos Jurídicos da CGD, Assistente na FDL, Referendário do Advogado Geral Português Dr. José Luís Cruz Vilaça e do Juiz Português Dr. Moitinho de Almeida, no Tribunal da União Europeia, Jurista do Banco Europeu de Investimento (Departamento Jurídico), Vice-Presidente do Conselho de Administração da ANACOM. Atualmente: Docente da FDL (em licença sem vencimento) e Data Protection Officer no Banco Europeu de Investimento.

Responsabilização e governação das empresas no âmbito do novo Regulamento de Proteção de Dados

Teresa Vale Lopes[2]

O novo Regulamento de Proteção de Dados Pessoais apresenta como uma das suas principais características a consagração do princípio da responsabilidade das empresas, em especial no que concerne à adoção das medidas organizativas adequadas para assegurar e demonstrar o cumprimento das obrigações legais relativamente à proteção de dados pessoais.

Em apreço encontram-se previstas medidas relativas à implementação de políticas internas, ao registo das atividades de tratamento, à realização de uma avaliação de impacto sobre a proteção de dados, bem como à obrigação de nomear um encarregado da proteção de dados, responsável por zelar, de forma independente, pela observância das obrigações legais por parte de cada organização e por ser o ponto de contacto com as autoridades competentes em matéria de proteção de dados pessoais.

Por outro lado, o mencionado Regulamento incentiva a criação de códigos de conduta pelas associações ou outras entidades representativas de categorias de responsáveis pelo tratamento ou de subcontratantes, de forma a tornar mais efetivo o cumprimento das disposições por parte dos diferentes setores, tendo em consideração as suas especificidades, bem como a criação de procedimentos de certificação na área da proteção de dados e de selos e marcas de proteção.

Com a presente comunicação pretende-se analisar algumas das principais obrigações e responsabilidades que o novo Regulamento vem estabelecer para as empresas, assim como o seu impacto a nível organizacional.

Direitos do titular de dados pessoais: o direito à portabilidade dos dados

Graça Canto Moniz[3]

A regulamentação sobre proteção de dados pessoais na qual se insere o novo pacote legal, nomeadamente o Regulamento (UE) 2016/679 ("Regulamento"), parte de um pressuposto geral: a posição de vulnerabilidade e de desvantagem estrutural do titular de

---

[2] *Health Care Compliance Specialist and Data Privacy Liaison* na área da Indústria Farmacêutica; Investigadora no CEDIS – Centro de Investigação e Desenvolvimento sobre Direito e Sociedade, na área de proteção de dados.

[3] Licenciada em Direito (FDUP), Mestre em Ciências Jurídico Políticas (FDUC) e Doutoranda em Direito na FDUNL investigando sobre a extraterritorialidade do Regime Jurídico Europeu de Proteção de Dados Pessoais.

dados pessoais numa sociedade marcada pela circulação de fluxos informacionais sobre as pessoas, de várias origens e para vários destinatários.

O quadro legal da União Europeia, além do direito ao respeito pela vida privada e familiar, previsto no Artigo 7.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE), consagra o direito fundamental à proteção de dados pessoais reconhecido no Artigo 8.º daquele diploma. Estes direitos fundamentais são complementados por um conjunto de direitos específicos do titular dos dados, nomeadamente, o direito de informação, acesso, retificação ou apagamento de dados pessoais. O novo Regulamento, se, por um lado, reafirma essa cartilha de direitos específicos mantendo a sua estrutura, já anteriormente prevista na Diretiva 95/46/CE, por outro, acrescenta novos elementos a essa lista no sentido de reforçar a tutela do titular dos dados. Nesta apresentação propomos um breve excurso sobre este conjunto de direitos, destacando alguns dos aspetos inovadores da nova legislação, em particular o direito à portabilidade dos dados.

Painel Temático 2 – Que respostas para os novos desafios da revolução tecnológica?

Moderador*:* Dr. Luís Neto Galvão (*SRS Advogados*)

Cibersegurança e Proteção de Dados - Obrigações de Segurança da Informação, Incidentes de Violação de Dados Pessoais e Demonstração de Responsabilidade no Quadro do Regulamento Geral sobre a Proteção de Dados

Manuel Melo[4]

O Regulamento 2016/679 do Parlamento Europeu e do Conselho da União Europeia, de 27 de Abril de 2016, designado como Regulamento Geral sobre a Proteção de Dados (RGPD), define o novo regime jurídico da proteção das pessoas singulares no que diz respeita ao tratamento dos dados pessoais e à livre circulação desses dados.

Publicado no dia 4 de Maio de 2016, o RGPD é aplicável a partir de 25 de Maio de 2018, estabelecendo profundas alterações no enquadramento da proteção de dados pessoais dentro de todos os países da União Europeia e sendo diretamente aplicável no ordenamento jurídico português.

Este novo Regulamento tem um grande impacto sobre a atividade das empresas privadas ou instituições públicas e, especificamente, sobre as respetivas práticas de cibersegurança, criando novas obrigações e responsabilidades em matéria de segurança

[4] Licenciado em Direito, Mestre em Ciências Jurídico-Empresariais e Doutorando em Direito e Segurança na FDUNL, desenvolvendo atualmente projetos de investigação em matéria de Proteção de Dados, Ciberilicitude e Cibersegurança. Trabalha atualmente como Formador, como Consultor de Gestão em Proteção de Dados e Cibersegurança e como Encarregado de Proteção de Dados para diversas entidades públicas e privadas em Portugal e outros países da União Europeia. Foi nomeado recentemente Presidente da APCIBER – Associação para a Promoção da Cibersegurança e Proteção de Dados, ficando responsável pelo desenvolvimento de Cursos de Formação, Códigos de Conduta e Programas de Certificação em Cibersegurança e Proteção de Dados. Em Janeiro de 2017 vai assumir o cargo de Diretor do recém-criado Centro de Formação em Protecção de Dados, Cibersegurança e Conformidade Regulatória.

da informação e em matéria de gestão de incidentes de violação de dados e estabelecendo o princípio da demonstração da responsabilidade no domínio das medidas técnicas e organizativas de segurança da informação.

Para garantir a conformidade ("compliance") e a responsabilidade ("accountability") com o RGPD, em termos de cibersegurança, é necessário:

- conhecer as medidas técnicas e organizativas necessárias para assegurar um nível de segurança adequada ao risco;
- compreender a importância da definição de um plano de gestão de incidentes de violação de dados pessoais para cumprimento das obrigações de notificação à autoridade de controlo e de comunicação ao titular dos dados e
- delinear um plano de ação para implementação e desenvolvimento da capacidade de demonstração da responsabilidade no âmbito da segurança da informação e dos incidentes de violação de dados pessoais.

Desta forma será possível delinear uma estratégia e uma prática integrada de cibersegurança e proteção de dados, respondendo aos desafios do novo modelo regulatório definido pelo RGPD.

Profiling e algoritmos autónomos: um verdadeiro direito de oposição?

Afonso José Ferreira[5]

O novo Regulamento Geral de Proteção de Dados introduz alterações na privacidade dos titulares de dados. Estas alterações eram necessárias, tendo em conta o caráter antiquado da Diretiva que o Regulamento substitui. O Regulamento prevê um direito de oposição ao profiling, definido pelo art. 4º, n.º 4 como "tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular".

Este processamento automatizado de dados adquiriu importância nas nossas vidas, especialmente no uso de algoritmos autónomos – que funcionam independentemente da participação de um supervisor, e cujos resultados são desconhecidos do seu criador. O uso de algoritmos autónomos como os motores de busca tem-se tornado crescente nas nossas vidas, com autores como SHIRKY a referirem-se à "autoridade algorítmica", e autores como ZITTRAIN a sugerirem soluções como a "fidúcia de informação", para garantir maior independência e cuidado no resultado destes algoritmos. Sendo estes algoritmos utilizados para prever reincidências criminais, previsões de saúde ou rendimentos para atribuição de seguros e empréstimos, entre outros, torna-se importante o direito previsto no art. 22º, n.º 1, segundo o qual o titular de dados terá a possibilidade de se opor a que uma decisão se funde meramente no resultado do profiling. Este direito

[5] Aluno da Licenciatura em Direito na Faculdade de Direito da Universidade Nova de Lisboa. Bolseiro de Iniciação Científica da Fundação para a Ciência e Tecnologia e do Centro de Investigação & Desenvolvimento em Direito e Sociedade. Este trabalho foi desenvolvido com o apoio de uma Bolsa FCT

é, para MAYER-SCHÖNBERGER, um direito de privacidade de terceira geração, fundado numa utilização dos dados pelo titular.

No entanto, o n.º 2 esclarece que este direito de oposição não é aplicável quando estejam em causa decisões "[necessárias] para a celebração de um contrato". Esta exceção eclipsará o direito de oposição previsto no n.º 1. Adotando uma perspetiva quasi-ciberexcecionalista como a defendida por LESSIG, defenderei que qualquer processamento de dados por algoritmos autónomos, como a utilização de motores de busca, será um contrato entre o titular de dados e o responsável pelo tratamento, devido à justiciabilidade dos termos e condições de websites enquanto contratos de adesão.

Deste modo, sugerirei soluções para o problema, baseadas na visualização simplificada de diferentes perfis de tratamento de dados – uma ideia própria do paternalismo justificado de SUNSTEIN –, que permitirão ao utilizador escolher determinadas categorias de intensidade de processamento de dados por algoritmos autónomos antes de os usar.

Painel Temático 3 – As transferências de dados pessoais, o Privacy Shield e a Diretiva PNR

Moderador: Dr. João Taborda da Gama (Gama Glória)

Transferências internacionais de dados pessoais

Inês Oliveira[6]

O comummente apelidado Pacote de Proteção de Dados, integrado pelo Regulamento (UE) 2016/679 e pela Diretiva (UE) 2016/680, ambos de 27 de abril de 2016, apesar de ter aprovado o novo regime europeu no que à matéria de dados pessoais respeita, não pode ser adjetivado de totalmente inovador, uma vez que são muitas as linhas de continuidade com o regime ainda hoje vigente.

Não obstante, o Regulamento Geral sobre a Proteção de Dados traz-nos algumas novidades no que concerne às transferências de dados pessoais para países terceiros ou organizações internacionais (artigos 44.º a 50.º). A primeira delas é precisamente o alargamento às organizações internacionais, que caminha a par com o alargamento das situações-tipo. Note-se que a partir de maio de 2018 passam a ser admissíveis

[6] 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

transferências quando o tratamento não for repetitivo, para um número limitado de pessoas envolvidas, para fins de interesse legítimo imperioso e mediante garantias adequadas.

O Regulamento, apesar de ser diretamente aplicável e extenso e preciso em muitos dos seus aspetos, permite, no que toca a esta matéria, que os legisladores nacionais prevejam limites à transferência de categorias específicas de dados, mormente quando estão em causa razões importantes de interesse público.
No âmbito da cooperação policial e judiciária em matéria penal (artigos 35.º a 40.º da Diretiva), assistimos igualmente ao alargamento dos mecanismos legitimadores das transferências, que passarão a ser permitidas, nos termos das leis de transposição, também mediante garantias adequadas. Ademais, e como traço inovador, as transferências podem passar a ser feitas diretamente para destinatários estabelecidos em países terceiros.

Um novo quadro jurídico para as transferências transatlânticas de dados: o Privacy Shield

Heraclides Silva[7]

Proferido pelo Tribunal de Justiça da União Europeia a 6 de Outubro de 2015, o acórdão Schrems marcou uma viragem nas relações comerciais entre a União Europeia e os Estados Unidos, ao declarar como inválida a designada Safe Harbour Decision, que até então permitia a livre circulação de dados pessoais da União Europeia para as empresas norte-americanas que subscrevessem os princípios consagrados nessa decisão da Comissão.

Com o objetivo de estabelecer um novo quadro jurídico para os fluxos transatlânticos de dados pessoais que substituísse a Safe Harbour Decision, as autoridades europeias e norte-americanas iniciaram um período de negociações que culminou na adoção, em Agosto de 2016, do intitulado Privacy Shield. Neste novo acordo, partindo das exigências expressas pelo Tribunal de Justiça no acórdão Schrems, procurou-se reforçar a proteção dos dados pessoais dos cidadãos europeus no contexto das transferências transatlânticas, uma vez ter sido este o motivo que levou à declaração de invalidade do mecanismo antecedente.

Composto pela decisão de adequação e por sete anexos, o Privacy Shield contém os princípios que as empresas terão de respeitar, bem como as salvaguardas e os limites em matéria de acesso aos dados por parte das autoridades públicas norte-americanas. Consagra ainda novos mecanismos de reação que estão à disposição dos particulares,

[7] Heraclides Santos Silva – Licenciado em Direito e Mestrando em Ciências Jurídicas Forenses pela Faculdade de Direito da Universidade Nova de Lisboa. Neste momento, encontra-se a preparar a sua dissertação de mestrado sobre o Acórdão Schrems do Tribunal de Justiça da União Europeia.

destacando-se a figura do Provedor de Justiça, à qual poderão recorrer quando entendam que os seus dados tenham sido acedidos ilicitamente pelas instituições norte-americanas. Neste artigo será feita uma apresentação geral do Privacy Shield, o que implica conhecer os pressupostos que justificaram a sua adoção, os critérios pelos quais as empresas e as autoridades terão que se guiar para que a transferência transatlântica de dados seja lícita, os mecanismos de supervisão previstos e os novos meios de reação dos particulares.

A compatibilidade do acordo de Privacy Shield face ao direito da União Europeia

Martinho Lucas Pires[8]

A decisão do Tribunal de Justiça da UE no caso Schrems considerou que o acordo de Safe Harbour celebrado com os EUA, relativo às transferências de dados, não era compatível com o nível de proteção de direitos fundamentais exigido pelo direito europeu. Tal deveu-se, em suma, ao reduzido nível de proteção de dados e da privacidade dos utilizadores garantido pelo acordo, permitindo interferências governamentais e externas, e à falta de meios de reação eficazes ao dispor dos particulares e das agências nacionais de proteção de dados.

Em Agosto de 2016 foi adotado um novo acordo para substituir o Safe Harbour, denominado Privacy Shield. Segundo a Comissão Europeia, este novo acordo cumpre com as exigências estabelecidas na Directiva 95/46/CE e de respeito pelos direitos fundamentais de privacidade, estabelecidos nos artigos 7º e 8º da Carta dos Direitos Fundamentais, reforçando as obrigações das empresas participantes, o mecanismo de controlo e supervisão e a possibilidade de acesso e reação dos particulares.

No entanto, apesar da adesão de várias empresas, foram já anunciadas contestações judiciais ao acordo, devido a dúvidas face à sua real compatibilidade com o direito da união. Existe igualmente um parecer da European Data Protection Supervisor que levanta algumas questões quanto ao facto do Privacy Shield ser um reforço efetivo do Safe Harbour.

Este artigo propõe-se a analisar estas dúvidas sobre o Privacy Shield e a verificar até que ponto é que o mesmo é uma versão fortalecida do Safe Habour, e se a proteção da retenção de dados de interferências externas, das alternativas de reação ao dispor dos particulares em face de qualquer ingerência, e assim a garantia de proteção dos princípios de direito europeu delineados pelo Tribunal de Justiça se encontram ou não, de facto, assegurados.

---

[8] Doutorando em Direito da União Europeia na Universidade Nova de Lisboa. Mestre e LLM em Direito da União Europeia e Direito Internacional pela Faculdade de Direito da Universidade Católica Portuguesa. Principais áreas de investigação: Direito da União Europeia, Direito Constitucional e Direito Económico. Inscrito na Ordem dos Advogado

O PNR e a Proteção de Dados: uma análise sobre a transferência da informação dos passageiros aos Estados

Emellin de Oliveira[9]

De acordo com o artigo 13º da Convenção de Aviação Civil Internacional, as leis e os regulamentos de um Estado contratante devem ser cumpridos pelos passageiros, tripulação e seu representante quando da entrada ou saída de seu território. Diante desta determinação da ICAO (International Civil Aviation Organization) e com o intuito de corroborar com as medidas contra o terrorismo e a criminalidade grave, no dia 14 de abril de 2016, as companhias aéreas foram vinculadas a uma obrigação contida na Resolução Legislativa aprovada pelo Parlamento Europeu, a respeito do tratamento de dados dos registos de identificação dos passageiros, o PNR (Passager Name Record). Mencionada resolução estabelece que as transportadoras aéreas devem fornecer aos Estados-Membros as informações relativas ao registo de seus passageiros nos voos com proveniência e/ou destino países terceiros, extra-UE, podendo estender tal obrigação, se assim entenderem, a voos intra-UE. Assim, tendo em conta a obrigação em transferir dados pessoais contida nos atos legislativos acima citados e a aprovação também em 2016 da Diretiva e do Regulamento sobre a Proteção de Dados de Pessoas Singulares, cuja proposta foi inicialmente rejeitada no Parlamento Europeu por receio de que direitos fundamentais fossem atingidos e violados, é inevitável um estudo comparativo dos documentos relativos aos dois temas: Proteção de Dados e PNR, cujas normas europeias deverão ser transpostas pelos Estados-Membros até 06 e 25 de Maio de 2018, respetivamente. Posto isto, o presente artigo visa analisar o conteúdo da Diretiva UE-PNR, trançando as convergências e incongruências relativamente à Diretiva de Proteção de Dados, a fim de que se possa criticamente averiguar a real aplicabilidade e eficácia dessas legislações comunitárias no combate ao terrorismo e à criminalidade face ao determinado às companhias aéreas.

[9] Advogada especializada em Direito Internacional, Doutoranda em Direito na Universidade Nova de Lisboa (FDUNL) e Investigadora no Centro de I&D em Direito e Sociedade (CEDIS). Como formação, a autora tem o título de Mestre em Migrações Internacionais pelo Instituto Universitário de Lisboa (ISCTE-IUL), Especialista em Estudos da Paz e da Segurança pela Universidade de Coimbra (FEUC) e Bacharel em Direito pela Universidade Federal do Ceará (UFC-CE, Brasil).